

G&D ControlCenter-IP 2.0

EN Web Application»Config Panel« Configuring the matrix switch



G& AND KVM FEELS RIGHT.		G&D Config Panel 21 EN 🔗 🚑							
Tools	* 	Home /	Home / Matrix systems / Matrix switches						
៹ڷۣ} System		IP I	IP matrix						
Configuration									
ှင့် Matrix systems 🗸 🗸		Sea	rch	X			\$	•	
နိုငCIP2.0 🗸			Name 📤	-	Device type	Monitoring ov	erview	•	
MTX Matrix	<		CCIP2.0 (j)		ControlCenter-IP 2.0	ок			
Console modules									
CPU Computer modules									
↔ RemoteGateways									
Con RemoteTargets									
Computer module groups									
	-	Add e	nd devices Serv	vice tools		ර දරූව	Configuration	Delete	

About this manual

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

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

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

Caveat Emptor

G&D will not provide warranty for devices that:

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

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

Proof of trademark

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

© Guntermann & Drunck GmbH 2025. All rights reserved.

Version 1.60 – 04/03/2025 Config Panel 21 version: 1.6.000

Guntermann & Drunck GmbH Obere Leimbach 9 57074 Siegen

Germany

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

www.gdsys.com sales@gdsys.com

Table of contents

Chapter 1: Basic functions

Introduction	. 1
System requirements	. 2
Supported operating systems	. 2
Recommended resolutions	. 2
Initial configuration of the network settings	. 3
(De)Activating the integrated DHCP server	. 4
Overview of the assigned IP addresses	4
Step 1: Select device	4
Step 2: Configure DHCP server	4
Step 3: Configuration completed	5
Getting started	. 6
Starting the web application	. 6
Operating the web application	. 8
User interface	8
Frequently used buttons	10
Configuring table columns	10
Language settings	12
Selecting the language of the web application	12
Selecting the system language	12
Selecting the language for a specific user account	13
Automatic logout	14
Snowing terms of use	15
Password complexity	16
Login options	18
Showing the version number of the web application	19
Closing the web application	19
Basic configuration of the web application	20
Network settings	20
Configuring the network interfaces	20
Configuring global network settings	22
Increasing the reliability of network connections by link aggregation	23
Reading out the status of the network interfaces	25
Creating and administrating netfilter rules	26
Creating new netfilter rules	26
Editing existing netfilter rules	28
Deleting existing netfilter rules	29
Changing the order or priority of existing netfilter rules	30

Creating an SSL certificate	30
Special features for complex KVM systems	. 31
Creating a Certificate Authority	. 31
Creating any certificate	. 33
Creating and signing an X509 certificate	. 34
Creating a PEM file	. 35
Selecting an SSL certificate	36
Firmware update	38
Firmware update of a single device	. 38
Firmware update of multiple KVM system devices	. 39
Restoring the system defaults	40
Restarting the device	40
Network functions of the devices	41
NTP server	41
Time sync with an NTP server	41
Manual setting of time and date	43
Logging systog messages	44
Local logging of systog messages	45
Sending systog messages to a server	46
Viewing and saving local syslog messages	47
User authentication with directory services	47
Setting up two-factor authentication on the device (optional)	50
KVM connection	52
Defining the ports of the KVM-over-IP connection	52
Classifying IP packets (DiffServ)	53
Determination of the type of video transmission	53
Restricting KVM-over-IP counterparts (UID locking)	55
Used network ports and protocols	56
Database mode	58
Monitoring functions	59
Viewing all monitoring values	59
Enabling/disabling monitoring values	60
Advanced features for managing critical devices	61
Displaying the list of critical monitoring values	. 61
Confirm the alarm of a critical device	.61
Monitoring devices via SNMP	62
Practical use of the SNMP protocol	62
Configuring an SNMP agent	62
Adding and Configuring SNMP traps	65
Harro and erround	20
Users and groups	68
Efficient rights administration	68
I ne effective right	.68
Endend user group administration	.09

Administrating user accounts	70
Creating a new user account	. 71
Activating two-factor authentication (optional)	. 72
Renaming a user account	. 75
Changing the password of a user account	. 76
Changing the user account rights	. 77
Changing a user account's group membership	. 79
Enabling or disabling a user account	. 80
Deleting a user account	. 80
Administrating user groups	81
Creating a new user group	. 81
Renaming a user group	. 82
Changing the user group rights	. 83
Administrating user group members	. 85
(De)activating a user group	. 85
Deleting a user group	. 85
System rights	86
Rights for unrestricted access to the system (Superuser)	. 86
Changing the login right to the web application	. 86
Rights to access the EasyControl tool	. 87
Rights to change your own password	. 87
Authorization to confirm a monitoring alarm	. 87
Authorisation to execute the »Replace device« function	. 88
Advanced functions of the KVM system	89
Identifying a device by activating the Identification LED	89
Saving the configurations	80
Saving the configurations with oute health function	00
Deste sing the configurations with auto backup function	90
Restoring the configurations	92
Activating premium functions	93

Chapter 2: Matrix system

Computer modules	94
Adjusting access and configuration rights	94
Access rights to a computer module	94
Access rights to a computer module group	96
Access mode for simultaneous access to computer modules	. 97
Access to USB devices	100
Rights to configure computer modules1	103
Basic configuration of computer modules 1	103
Changing the name of a computer module1	03
Changing the comment of a computer module1	04
Deleting a computer module from a KVM matrix system1	04
Copying configuration settings to a new computer module1	05
Copying the configuration settings of a computer module1	105

Settings for special hardware	106
(De)Activating an USB keyboard mode the Generic USB mode	106
Adjusting the operating mode of the RS232 interface	109
Defining the EDID profile to be used	110
Reducing the colour depth of image data to be transmitted	111
Advanced features	112
Wake On LAN	112
Sending a key combination after disconnecting all users	113
Enabling/disabling the keyboard signal	113
Multi-user information	114
Configure Mouse mode CrossDisplay-Switching	115
Extended settings of KVM-over-IP connection	118
Limiting the bandwidth	118
Classifying IP packets (DiffServ)	119
De)Activating signals	119
Determination of the type of video transmission	120
Viewing status information of a computer module	121
Restarting a computer module	122
Updating the firmware of computer modules	123
	120
Console modules	124
Operating modes of console modules	124
Standard operating mode	124
OpenAccess operating mode	124
Video operating mode	125
Selecting the console module's operating mode	125
Basic configuration of console modules	126
Changing names or comments of console modules	126
Enabling or disabling console modules	126
Copying configuration settings to a new console module	127
Copying the configuration settings of a console module	127
Deleting a console module from the KVM matrix system	128
(De)Activating access to exclusive signals	128
Rights for access to exclusive signals	129
Settings for special hardware	132
Support of any USB devices	132
Reinitialising USB input devices	133
Advanced functions	134
Automatic user logout	134
Configuring default execution after a user logon	134
Return to the last computer module	136
Restore the last FreeSeating session	137
Deactivation of the Restore last session function	137
Automatically disconnecting access to computer modules	138
Remembering a username in the login box	139
Setting the hold time for the screensaver	140
Setting the hold time for the login screensaver	140
Enabling or disabling DDC/CI support	141
Adjusting the operating mode of the RS232 interface	143

Restarting a console module	144
Updating the firmware of a console module	145
Viewing status information of a console module	146
Domoto gatawaya and remoto targeta	147
Conforming and remote targets	14/
Configuring remote gateways	148
Changing the name of a remote gateway	148
Changing the comment of a remote gateway	148
Configuring the network interface	149
Configuring global network settings	150
Assigning a remote pool	151
Extended settings of KVM-over-IP connection	151
Limiting the bandwidth	151
Classifying IP packets (DiffServ)	152
(De)Activating signals	152
Determination of the type of video transmission	153
Viewing monitoring values	154
Viewing status information of a remote gateway	155
Configuring remote targets	156
Changing the name of a remote target	156
Changing the comment of a remote target	156
Saving the resolution of a virtual machine	157
Reducing the colour depth of the image data to be transmitted	158
Holding a connection	158
Connection repeats	159
Defining the connection parameters for a remote target	160
Saving login data or use the matrix credentials for login	162
Assigning a remote pool	163
Viewing monitoring values	163
Viewing status information of a remote target.	164
Computer module groups and view filters	165
Intended use of computer module groups	165
Intended use of view filters	165
Administrating computer module groups	165
The »New IP targets« computer module group	165
Creating a new computer module group	166
Changing the name or comment of a computer module group	166
Administrating computer module group members	167
Deleting a computer module group	167
Administrating view filters	168
Creating a new view filter	168
Changing the name of a view filter	168
Deleting a view filter.	168
Adding a computer module to a view filter	169
Deleting a computer module from a view filter	169
Assigning a view filter as default in the OSD	170

Accessing computer modules via select keys	171
Changing select key modifier or valid key type	171
Administrating select key sets	172
Step 1: Select a matrix switch	172
Step 2: Select a user	173
Step 3: Select key sets	173
Step 4: Configure a select key set	173
Automatic or manual switching between computer modules	174
Auto scanning all computer modules (Autoscan)	174
Applying the Autoscan function	175
Configuring the scantime of the <i>Autoscan</i> function	175
Auto scanning all active computer modules (Autoskip)	176
Applying the Autoskip function	176
Configuring the scantime of the Autoskip function	176
Scanning computer modules manually (Stepscan)	177
Starting and stopping the Stepscan function	177
Configuring keys for manually scan	177
Administrating scan mode sets	178
Step 1: Select a user	178
Step 2: Scan mode sets	178
Step 3: Configure scan mode set	178
Configuring the on-screen display	179
Configuration	179
Changing the hotkey to open the OSD	179
Opening the OSD via double keypress	181
Automatic closing of the OSD after inactivity	182
Adjusting the OSD transparency	183
Adjusting the information display	184
Changing the colour of the information display	185
Defining a default view filter	186
Selecting a keyboard layout for OSD entries	187
Operating the OSD by mouse	188
Enabling/disabling the OSD	188
Adjusting the OSD resolution	189
Expanding switchable signals	191
Expanding the system through channel grouping	192
Creating a new channel group	193
Adding or deleting modules from a channel group	194
Deleting a channel group	195
Advanced functions of the KVM matrix switch	196
Copying the config settings of a matrix switch	196
Restoring the connection status after a restart	197
Restarting the matrix switch	108
Destoring the connection state after a restart	100
Conving and confidential and a new matrix multiple	199
Copying counting settings to a new matrix switch	200

Freeze mode	201
Changing push event key modifiers and valid keymodes	204
Rights administration	205
Right to change the personal profile	.205
Optional functions	206
Viewing the status information of matrix switches	.210
Push-get function (optional)	211
Changing the right to execute the Push-get function	211
Changing push-get key modifiers and valid keys	212
Administrating push-get key sets	213
Step 1: Select a matrix switch	213
Step 2: Select a user	213
Step 3: Select push-get key set	.214
Step 4: Configure push-get key set	214
IP-Control-API (ontional)	215
Supported functions via text-based control	215
Configuring access for taxt based control	215
Configuring access for text-based control	210
Scripting function (optional)	217
Configuring scripts	217
Step 1: Select the option »Scripts«	.217
Steps 2 and 3: Create, edit, merge or delete scripts	.218
Step 4: Define owner	.220
Step 5: Script availability	.220
Step 6: Target device	.221
Configuring script groups	222
Step 1: Select the option »Scripts groups«	.222
Steps 2 and 3: Create, edit or delete script groups	.222
Step 4: Add scripts to group or delete them from group	.223
Step 5: Define order of script execution	.223
Step 6: Script group availability	.223
Assigning rights to execute scripts and script groups	224
Defining the right to execute a script	.224
Defining the right to execute a script group	.225
Assigning and configuring script keys	226
Using script keys at a console module	.226
Changing the script key modifier and the valid keys	.226
Administrating script key sets	227
Step 1: Select a device	.227
Step 2: Select a user	.228
Step 3: Add or select script key sets	.228
Step 4: Assign scripts and edit script key sets	.228
OSD settings fo the Scripting function	228
Editing the default menu mode	.228
Switching threshold to switch the menu mode by mouse	.229

Tradeswitch function (ontional)	230
Changing tradeguitch key and valid key type	230
A dministrating tradequitab workplace	230
Step 1: Salact a matrix switch	232
Step 1. Select a main Switch workplace	232
Step 2. Configure tradeswitch workplace	232
Step 9: Configure tradeswitch workplace	232
Advanced functions	232
Configure Tradeswitch visualization	233
Customizing the appearance of the tradeswitch frame	234
	201
CrossDisplay-Switching (optional)	236
Using »CrossDisplay-Switching«	237
Requirements for »CrossDisplay-Switching«	238
Order and proportions of monitors	239
Implementing multi-head monitors	240
The »CrossDisplay-Switching« view	241
List of modules	. 241
Workspace	. 242
Basic configuration	243
Enabling CrossDisplay-Switching for the entire system	. 243
Adjusting the general CDS mouse speed	. 244
CDS mouse positioning	, 244
Enabling CrossDisplay-Switching for a specific computer module	. 246
Configuring the CrossDisplay-Switching function	247
Step 5: Position displays	, 247
Step 6: Configure CDS settings of computer modules	, 249
Messages	252
CDS multihead groups	253
Differences between CDS modes	253
Example of use	255
CDS with channel groups	233
CDS with mulithead groups	254
Dequirements	255
The Member configuration view	250
I ne »iviember comiguration« view	257
List of computer modules	.231
Configuring CDC multihead groups	250
Stan 1: Administrate CDS multiheed groups	239
Step 2: Configure CDS multihead groups	259
Saving order and resolutions of workspaces	260
ouving order and resolutions of workspaces	. 200

MatrixGuard (optional)	263
Rules for the assignment of the leader role	263
Example 1: Restart of all components	.263
Example 2: Failure of the current database leader	.264
Example 3: Recognition of another database leader	.264
Example 4: Failure of a network component	.264
Important notes	265
Requirements	265
Configuring a MatrixGuard member	266
Overview: Configuration of a MatrixGuard member	.266
Step 1: Set system time	.266
Step 2: Set certificate	.269
Step 3: Configure members	.270
DirectRedundancyShield (ontional)	272
The DRS status	272
Rules for the assignment of the DRS status	272
Example 1: Restart of all KVM components	273
Example 1: Restart of an R vivi components	273
Example 3: Failure of a network component	273
Important notes	273
Requirements	274
Configuring the DRS function	274
Step 1: Initial setup and definition of the target system	274
Step 7: Adjust configuration	276
Step 2: DRS configuration completed	270
Step 5. Divo comigutation completed	.277
EasyControl (optional)	278
Starting the »EasyControl« tool	278
Establishing and disconnecting a connection	279
Switching functions	.280
Hiding modules on the user interface	.280
Executing scripts	281
Configuring the interface	.282
Operating the user interface	.283
General configuration settings	284
Showing all notifications or only errors	.284
Changing the colour scheme of the tool	.284
Closing the tool	284
Possible messages and their meanings	285

1 Basic functions

Introduction

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

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

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

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

System requirements

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

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

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

- Apple Safari 18
- Google Chrome 133
- Microsoft Edge 133
- Mozilla Firefox 135

Supported operating systems

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

Recommended resolutions

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

Initial configuration of the network settings

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

- IP address of network interface A: 192.168.0.1
- IP address of network interface B: address obtained using DHCP
- Global network settings: settings obtained using DHCP

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

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

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

NOTE: Use the IP address *192.168.0.100*, for example.

- 3. Switch on the device.
- 4. Start the computer's web browser and enter **192.168.0.1** in the address bar.
- 5. Configure the network interface(s) and the global network settings as described in the paragraph *Network settings* on page 20 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.

(De)Activating the integrated DHCP server

If required, you can activate the DHCP server integrated in the matrix switch. The DHCP server is *deactivated* by default.

The DHCP server provides basic functionalities for the automatic integration of clients (this also includes the computer and console modules) into a network.

IMPORTANT: Activation and use of the integrated DHCP server *is not* possible when using the **MatrixGuard** function (see page 263) or when using the **DirectRedundancyShield** function (see page 272)!

Overview of the assigned IP addresses

If you have already activated the integrated DHCP server, the wizard starts with the overview of the assigned IP addresses.

The table lists the MAC address of each client and the assigned IP address.

You can (de)activate the DHCP server comfortably with a wizard. Click on the menu **Advanced features** and select the entry **DHCP-Server**. Click on **Configure** to start the wizard.

The following paragraphs briefly summarise the wizard's configuration options.

Step 1: Select device

IMPORTANT: The integrated DHCP server may only be activated on *one* matrix switch of a matrix system.

NOTE: This step is automatically skipped if a matrix switch is operated standalone.

- Click the matrix switch on which the integrated DHCP server is to be activated.
- Click Save and continue.

Step 2: Configure DHCP server

Configure the DHCP server in this step according to your requirements.

How to configure the DHCP server:

1. Enable or disable the DHCP server:

Enable DHCP server:	Switch DHCP	the serve	slider er.	to	the	right	(enabled)	to	enable	the
	Switch DHCP	the serve	slider er.	to	the	left	(disabled)	to	disable	the

2. If the DHCP server is enabled, you can configure the following settings::

IP address range from:	Enter the first IP address to be assigned by the DHCP server.
IP address range to:	Enter the last IP address to be assigned by the DHCP server.
Netmask:	Specify the netmask of the network.
Lease time:	Enter the amount of time in days that a client is allowed to keep the assigned IP address.
Gateway:	Specify the IP address of the gateway (optional).

3. Click Save and continue.

Step 3: Configuration completed

- The wizard confirms the successful setup of the DHCP server.
- 4. Click Finish.

Getting started

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

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

Starting the web application

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

How to start the web application

1. Enter the following URL in the address line:

https://[IP address of the device]

2. Enter the following data in the login mask:

Agree to the terms of use:		Click on the text to read the terms of use. Click on the checkbox to accept the terms of use.
NOTE: The terms of use only appear if a corresponding configuration has be made (see <i>Showing terms of use</i> on page 15 ff.).		s of use only appear if a corresponding configuration has been <i>ng terms of use</i> on page 15 ff.).
U	sername:	Enter a username.
P	assword:	Enter a password for your user account.
2. (1	Factor Auth Code OTP):	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.
NOTE: The 2-Factor Auth Code (TOTP) is only requested if two-factor authentication has been configured (see page 50 f.) and activated (see page 72 ff.).		

IMPORTANT: Change the administrator account's default password.

To do this, log into the web application with the administrator account and then change the password (see page 76).

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

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

NOTE: The default *admin* password for devices manufactured before June 2020 is **4658**.

- 3. Click on Login.
- 4. Click on the Config Panel 21 icon.

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancy-Shield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

NOTE: As an alternative to the **Config Panel 21** you can open the **EasyControl** (see page 278) tool after login, if you have activated the **IP-Control-API** feature for a fee.

Operating the web application

User interface

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

G& AND KVM FEELS RIGHT.	G&D Config Panel 21	5 en 2 🚍
Tools	Home / Matrix systems	
رژن system	IP matrix	
Configuration	Search 3 X	•
ېچ mank systems پ کې د دراوی	Name A Device type	Monitoring overview
Matrix <	CCIP2.0 ① ControlCenter-IP 2.0	ок
Con Console modules	(4)	
RemoteGateways		
Com RemoteTargets		
Computer module groups		
© User groups	Add end devices Service tools •	

Figure 1: User interface of the web application

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

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

Shortcuts (5)	Language selection: The language identifier (for example EN for <i>English</i>) shows the currently active language in the web application.
	To switch the language, click the language identifier. This opens a submenu that shows the supported languages and the corresponding identifiers.
	Switch the language by clicking on the desired language.
	User: A click on the user icon opens a submenu:
	 The name of the active user is displayed in the submenu. Click on <i>User</i> to access the user settings of the active user. Click on <i>Logout</i> to exit the active session.
	Monitoring status: This icon shows you at a glance whether all monitoring values are within the normal range (green icon) or if at least one monitoring value is outside the nor- mal range (yellow or red icon).
	The <i>Monitoring status</i> icon always takes the colour of the <i>most critical</i> monitoring value
	If the icon is displayed in yellow or red, you can access the <i>Active alarms</i> dialog by clicking on the icon.
Buttons 6	Depending on the dialog shown, different buttons are displayed in this area.

Frequently used buttons

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

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

Configuring table columns

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

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

IP	IP matrix				
Sea	rch X			\$	
	Name 🗕		Device type	Monitoring overview	•
	CCIP2.0		ControlCenter-IP 2.0	ОК	

Figure 2: Table columns (selection) of a matrix switch

NOTE: Click the chain icon in the **Name** column to display grouped devices as a unit or list each device individually.

How to change the columns to be displayed:

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

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

Table configuration

Columns:	Status	\$	Add column
Visible columns:	. 4		\$
Device	e type	Comment	Monitoring overview
		* *	* *

Figure 3: Table configuration

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

How to change the column order:

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

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

How to reset the table configuration to the default settings

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

Language settings

Selecting the language of the web application

How to change the language of the web application:

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

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

EN

Selecting the system language

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

If required, you can permanently assign a (different) language to each user account.

NOTE: All language settings apply to the web application as well as to the on-screen display (OSD) of the device . . If the OSD does *not* support the selected language, the OSD will be displayed in English.

How to set the system language:

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

Selecting the language for a specific user account

How to set the language of a specific user account:

- 1. On the menu, click Users.
- 2. Click the user account you want to configure, and then click **Configuration**.
- 3. Click the KVM matrix systems tab, and then click the Personal profile area selection.
- 4. In the Language field, choose between the following options:

System:	Use the system language (see above).
[Selection]	Use the selected language.

5. Click Save.

Automatic logout

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

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

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

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

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

How to (de)activate the Auto logout function:

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

NOTE: If user activity is detected, the timer is reset.

When an update process is started via the web application, the timer is also reset and only runs again once the update process has been completed.

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

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

5. Click Save.

Showing terms of use

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

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

How to configure the display of terms of use:

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

Off:	No terms of use are displayed during log in (default).
User defined:	Individual terms of use are displayed during log in.
DoD Notice and Consent Banner:	The terms of use of the <i>US Department of Defense</i> are used dur- ing log in (can only be selected if the optional <i>SecureCert fea-</i> <i>ture</i> is activated).

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

Password complexity

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

IMPORTANT: Changes in the section of password complexity have **no** effect on existing passwords, but are only taken into account when a password is changed (see *Changing the password of a user account* on page 76 ff.) and a new user account is created (see *Creating a new user account* on page 71). You should therefore configure the password complexity as early as possible.

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

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

How to configure the password complexity:

- 1. Click **System** on the menu.
- 2. Click Password complexity.
- 3. In the **Minimum password length** field, enter the desired minimum password lenght (*Default*: 3 or 15 with activated *SecureCert-Feature*)
- 4. In the **Minimum number of capital letters (e.g. ABCDEF)** field, enter the desired minimum number of capital letters within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
- 5. In the **Minimum number of lowercase letters (e.g. abcdef)** field, enter the desired minimum number of lowercases within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
- 6. In the **Minimum number of digits (e.g. 012345)** field, enter the desired minimum number of digits within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
- 7. In the **Minimum number of special characters (e.g. !#%&?@)** field, enter the desired minimum number of special characters within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)

8. In the **Minimum number of characters of the previous password to be changed** field, enter the desired minimum number of characters that must be differnt compared with the previous password (*Default:* 0 or 8 with activated *SecureCert-Feature*)

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

9. Click Save.

Login options

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

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

In this area, you can also specify how many simultaneous superuser sessions are permitted.

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

How to configure the Login options:

- 1. Click **System** on the menu.
- 2. Click Login optionsy.
- 3. In the **Number of consecutive invalid login attempts up to the time of blocking (0=off)** field, enter the desired maximum number of failed attempts when entering the password (*Default*: 0 = off/unlimited number of failed attempts or. 3 with activated *SecureCert-Feature*, max. 1,000)
- 4. In the Locking time (in minutes) field, enter the desired locking time in minutes for which a user is locked after exceeding the maximum number of failed password entry attempts (*Default*: 1 (if max. failed attempts > 0) or 15 with activated *Secure-Cert-Feature*, max. 1,440 minutes)
- 5. In the Limit the number of simultaneous sessions with superuser rights field, enter the desired number of maximum simultaneous superuser sessions
 (*Default*: 0 = off/unlimited number of superuser sessions, max. 1,024)

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

6. Click Save.

0

Showing the version number of the web application

How to show the version number of the web application:

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

Closing the web application

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

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

How to close the web application:

- 1. Click on the user icon at the top right.
- 2. Click on **Logout** to exit the active session.

Basic configuration of the web application

Network settings

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

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

Configuring the network interfaces

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

NOTE: These are the default settings:

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

How to configure the settings of a network interface:

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

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph **Interfaces**.

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

0	perating mode:	 Select the operational mode of Interface A or Interface B: Off: Disable network interface. Static: A static IP address is assigned. DHCP: Obtain IP address from a DHCP server
	The drop-dow been added to In this case, co	n list shows the text Link aggregation active if the interface has a network interface group. onfigure the network interfaces under »Link aggregation«.
IF	o address:	Enter the IP address of the interface (only when operating mode <i>Static</i> is selected)
	IMPORTANT: Vision IP series. network mana may otherwis address in a di	The IP address <i>192.168.0.1</i> should not be used on the As this IP address is also used as standard IP address for the gement interfaces of the KVM-over-IP end devices, conflicts e occur during communication. If possible, select an IP fferent subnet.
N	etmask:	Enter the netmask of the network (only when operating mode <i>Static</i> is selected).

6. Click on Save.

Configuring global network settings

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

How to configure global network settings:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Now go to Global network settings.
- 5. Enter the following values:

Operating mode:	Enter the desired operating mode:	
	Static: Use of static settings.DHCP: Obtain settings from a DHCP server.	
Hostname:	Enter the hostname of the device.	
	IMPORTANT: If the DHCP server itself does not assign a host- name when DHCP is enabled, the hostname entered here is used. Otherwise the hostname obtained from the DHCP server is used.	
In the <i>DHCP</i> operating mode the following settings are obtained automatically. Making entries is not possible.		
Domain:	Enter the domain to which the device should belong.	
Gateway:	Enter the IP address of the gateway.	
DNS server 1:	Enter the IP address of the DNS server.	
DNS server 2:	Optionally, enter the IP address of another DNS server.	

6. Click on Save.

Increasing the reliability of network connections by link aggregation

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

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

Two different modes are available for monitoring the interfaces:

• **MII mode:** The carrier status of the network interface is monitored via the *media independent interface*. In this mode, only the functionality of the network is tested.

• **ARP mode:** Using the *address resolution protocol*, requests are sent to an ARP target on the network. The response from the ARP target confirms both the functionality of the network interface and a proper network connection to the ARP target.

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

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

How to configure the settings of grouped network interfaces:

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph Link aggregation.

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

Name:	Enter the name of the network interface group.
Operating mode:	 Select the operating mode for grouped network interfaces: Off: Disable link aggregation. <i>Go to »Interfaces« to configure the network interfaces.</i> Static: A static IP address is assigned. DHCP: Obtain IP address from a DHCP server.
IP address:	Enter the IP address of the interface (only when operating mode <i>Static</i> is selected).
Netmask:	Enter the netmask of the network (only when operating mode <i>Static</i> is selected).

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

Primary Follower:	Select whether data traffic should preferably be transmitted via the interface $Network A$ (Interface A) or the interface $Network B$ (Interface B). As soon as the selected interface is available, this interface is used for data traffic.
	If you select the option None , the data traffic is sent via any interface. A switch-over occurs only if the active interface fails.
Link monitoring:	Select whether you want to use the MII or the ARP mode (see explanation above) to monitor the interface.
MII down delay:	Waiting period in milliseconds before a failed network interface is disabled.
	The entered value must be a multiple of 100 ms (the MII link monitoring frequency).
MII up delay:	Waiting period in milliseconds before a reset network inter- face is activated.
	The entered value must be a multiple of 100 ms (the MII link monitoring frequency).
ARP interval:	Enter the interval (100 to 10,000 milliseconds) after which the system checks for incoming ARP packets of the network interfaces.

ARP validate:	The validation ensures that the ARP packet for a particular network interface has been generated by one of the specified ARP targets.
	Select whether or which of the incoming ARP packets should be validated:
	• None: ARP packets are not validated (default).
	• Active: Only the ARP packets of the active network inter- face are validated.
	• Backup: Only the ARP packets of the inactive network interface are validated
	• All: The ARP packets of all network interfaces of the group are validated.
ARP target:	The table contains a list of all configured ARP targets.
	Use the buttons New, Edit and Delete to manage the ARP targets.

7. Click on Save.

Reading out the status of the network interfaces

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

How to detect the status of the network interfaces:

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

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

6. Click on Save.
Creating and administrating netfilter rules

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

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

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

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

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

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

Creating new netfilter rules

How to create a new netfilter rule:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph Netfilter.
- 5. Enter the following values:

Interface:	In the pull-down menu, select on which network interfaces the data packets are to be intercepted and manipulated:
	 All Interface A Interface B Link-Aggregation group

Option:	In the pull-down menu, select how to interpret the sender information of the rule:
	 Normal: The rule applies to data packets whose sender information corresponds to the IP address or MAC address specified in the rule. Inverted: The rule applies to data packets whose sender information does <i>not</i> correspond to the IP address or MAC address specified in the rule.
IP address/	Enter the IP address of the data packets or - by using the Net -
Netmask:	mask field - the address space of the IP addresses.
	Examples:
	192.168.150.187: for IP address 192.168.150.187
	 192.108.100.0/24: 1P 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 <i>IP</i>	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 <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.	
Filter rule: Drop: Data packets whose sender information ma IP address or MAC address are not processed.	
	 Accept: Data packets whose sender information matches the IP address or MAC address are processed.
Service:	Select a specific service for which this rule is used exclusively, or choose (AII).

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

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

7. Click on Save.

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

Editing existing netfilter rules

How to edit an existing netfilter rule:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph **Netfilter**.
- 5. In the list of existing netfilter rules, select the rule you want to change.
- 6. The current rule settings are displayed in the upper part of the dialog. Check and change the following settings.

Interface:	In the pull-down menu, select on which network interfaces the data packets are to be intercepted and manipulated: • All • Interface A • Interface B • Link-Aggregation group
Option:	In the pull-down menu, select how to interpret the sender information of the rule:
	 Normal: The rule applies to data packets whose sender information corresponds to the IP address or MAC address specified in the rule.
	• Inverted : The rule applies to data packets whose sender information does <i>not</i> correspond to the IP address or MAC address specified in the rule.
IP address/ Netmask::	Enter the IP address of the data packets or - by using the Net-mask field - the address space of the IP addresses.
	Examples:
	 192.100.100.101.101 IP addresses of section 102.168 150 v
	 192.168.10/16: 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 <i>IP</i> a	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 a	address and/or a MAC address can be specified within a rule.

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

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

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

Deleting existing netfilter rules

How to delete existing netfilter rules:

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

Changing the order or priority of existing netfilter rules

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

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

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

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

Creating an SSL certificate

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

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

The following websites provide detailed information about operating OpenSSL:

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

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

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

Special features for complex KVM systems

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

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

Creating a Certificate Authority

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

How to create a key for the Certificate Authority:

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

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

openssi genrsa -out ca.key 4096

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

How to create the Certificate Authority:

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

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

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

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

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

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

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

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

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

Creating any certificate

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

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

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

openssl genrsa -out server.key 4096

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

How to create the certificate request:

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

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

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

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

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

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

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

- 3. If desired, the *Challenge Password* can be defined. This password is needed if you have lost the secret key and the certificate needs to be recalled.
- 4. Now, the certificate is created and stored in a file named server.csr.

Creating and signing an X509 certificate

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

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

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

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

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

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

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

openssl x509 -text -in ca.crt

Creating a PEM file

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

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

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

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

a. Linux

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

b. Windows

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

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

Selecting an SSL certificate

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

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

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

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

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

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

How to select the SSL certificate you want to use:

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph **Certificate**.

5. Select the certificate you want to use:

G&D certificate #1:		This certificate is enabled for <i>new</i> devices.	
	NOTE: Make sur KVM system.	e that you use the same certificate for all devices within the	
G٤	&D certificate #2:	This certificate is supported by some older G&D devices with integrated web application.	
User certificate:		Select this option if you want to use a certificate purchased from a certificate authority or if you want to use a user cer- tificate.	
		Now you can import and upload the certificate:	
		• Click on Import certificate from file and use the file dialog to select the .pem file you want to import.	
		You can also copy the plain text of the server certificate, the server's private key and the certificate of the certifi- cate authority to the text box.	
		 Click on Upload and activate to store and activate the imported certificate for the device. 	

6. Click on Save.

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

Firmware update

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

Firmware update of a single device

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

How to execute a firmware update of a single device:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to update.
- 3. Open the menu Service tools and select the entry Firmware update.
- 4. Click on Supply firmware image files.

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

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

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

The firmware file is transferred to the internal storage and can then be selected for the update.

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

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

Firmware update of multiple KVM system devices

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

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

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

4. Click on Supply firmware image files.

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

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

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

The firmware file is transferred to the internal storage and can then be selected for the update.

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

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

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

Restoring the system defaults

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

How to restore the system defaults:

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

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

4. Click on Set system defaults.

Restarting the device

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

How to restart the device using the web application:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the desired device.
- 3. Open the menu Service tools and select the entry Restart.
- 4. Confirm the confirmation prompt with Restart.

Network functions of the devices

The devices within the KVM system provide separate network functions.

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

- Authentication against directory services (LDAP, Active Directory, RADIUS, 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 62 ff.)

NTP server

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

Time sync with an NTP server

How to change the NTP time sync settings:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **Network**.

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

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

5. Click on Save.

Manual setting of time and date

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph **NTP server**.

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

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

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

7. Click on Save.

Logging syslog messages

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

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

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

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

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

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

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

Local logging of syslog messages

How to locally log syslog messages:

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

Syslog local:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the local logging of syslog messa- ges: • Disabled • Enabled (<i>default</i>)
Log level:	In this pull-down menu, select the severity from which a log message is to be logged (<i>Default</i> : 6 - Info).
	The selected severity and all lower severity levels are logged.
If you select th severity levels	e severity 2 - <i>Critical</i> , messages for this code as well as for the 1 - <i>Alert</i> and 0 - <i>Emergency</i> are logged.

5. Click on Save.

Sending syslog messages to a server

How to send syslog messages to a server:

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

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

5. Click on Save.

Viewing and saving local syslog messages

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

How to view and store local syslog messages:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure.
- 3. Open the menu **Service tools** and select the entry **Syslog**.
- 4. Click on Retrieve syslog.

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

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

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

User authentication with directory services

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

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

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

The user account exists in the directory service and in the KVM system

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

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

• The user account exists in the directory service, but not in the KVM system

A user who has been successfully authenticated against the directory service but does not have an account of the same name in the KVM system's database will be granted the rights of a *RemoteAuth* user.

If required, change the rights of this particular user account to set the rights for users without a user account.

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

• The user account exists in the KVM system, but not in the directory service

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

If the server is not available but the fallback mechanism is activated, the user can log on with the password stored in the KVM system.

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

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

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

How to configure the authentication of user accounts:

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph Authentication.

5. Enter the following values under Authentication service:

Authentication server:	Select the Local option if the user administration is to be carried out by the KVM system.				
	If you want to use a certain external directory service, select the corresponding entry from the pull-down menu:				
	 LDAP Active Directory Radius TACACS + 				
	After selecting a external directory service, enter the settings of the directory service server in the corresponding dialog box.				
NOTE: User na nal directory se	ames can be subject to a naming convention when using exter- ervices (see <i>Creating a new user account</i> on page 71).				
ADVICE: When using <i>LDAP</i> or <i>Active Directory</i> , enter the path from which the respective search should be started in the Base DN/SearchScope field. This saves time and prevents an unnecessarily long search.					
Fallback: Activate this option if you want to use the local user a istration of the KVM system if the directory service is to rarily unavailable.					
IMPORTANT: In order to prevent the logon of a user locked or deactivated in the directory service when the connection to the directory service fails, please observe the following security rules:					
 If a user acc action must Activate the	ount is deactivated or deleted in the directory service, this also be carried out in the user database of the KVM system! e fallback mechanism only in exceptional cases.				
IMPORTANT: When using two-factor authentication, the fallback mechanism cannot be used					

(see Setting up two-factor authentication on the device (optional) on page 50).

6. Click on Save.

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

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

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

IMPORTANT: If you no longer have access to your possession-based factor or if it is broken, you will lose access to the system. Take precautions by, for example, keeping the emergency codes in a safe place if you are using the internal OTP server and configuring settings that will minimise the risk of losing access (see *Activating two-factor authentication (optional)* on page 72).

How to activate 2FA on the device:

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

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

2FA support:	Disabled (<i>default</i>)Enabled				
OTP server:	Select the option Internal (<i>default</i>), if you will be using an authentication server that is provided in the device.				
	If you want to use a specific external directory service, select the corresponding entry from the pull-down menu:				
	 LDAP Active Directory Radius TACACS+ 				
	Once you have selected a directory service, enter the settings for the directory service server in the dialogue screen that opens.				
NOTE: Note t tory service is	hat usernames may be subject to a naming convention if a direc- s used (see <i>Creating a new user account</i> on page 71).				
Login only for users with configured 2FA:	If the internal OTP server is used, you can specify whether login for users without activated 2FA will permitted (<i>default</i>) or prevented. This option can be used to set up a transition period for setting up the OTPs, for example.				
	 No (default) Yes 				
IMPORTANT: required for e	If an external directory service is used, the second factor will be every user profile on login.				

6. Click on Save.

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

Information on activating two-factor authentication is provided on page 72.

KVM connection

Defining the ports of the KVM-over-IP connection

To establish the KVM-over-IP connection, the control port and the communication port must be defined.

How to configure the ports of the KVM-over-IP connection:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **KVM connection**.
- 4. Go to the paragraph Local and enter the following values:

Control Port:	Enter the number of the port to be used (<i>default</i> : 18246).
Communication Port (K, M, misc):	Enter the number of the port to be used (<i>default</i> : 18245).

5. In the line **Establish connection via own certificate**, select whether the connection setup to the remote station is to be protected with a certificate:

IMPORTANT: A connection can only be established if the counterpart uses a certificate by the same Certificate Authority!

Deactivated:	The connection establishment <i>is not</i> protected by a certificate.		
Activated, network certificate:	The network certificate is used to establish the connection (see <i>Selecting an SSL certificate</i> on page 36).		
Activated, separate certificate:	A purchased certificate from a certificate authority or a self- created certificate are used to establish the connection (see <i>Creating an SSL certificate</i> on page 30).		
	Click Upload certificate and select the .pem file to import in the file dialog. Click Upload and activate to save and activate the certificate.		

6. Click on Save.

IMPORTANT: For security reasons, network certificates for the web application (see page 30 ff.) and, if used, additional user certificates for the KVM connection (see page 52) are **not** included in a backup and may have to be stored again after a restore.

Classifying IP packets (DiffServ)

For QoS purposes (Quality of Service) you have the possibility to use **Differentiated Services Codepoints** (DSCP) to classify the IP packets.

Through this classification, you can prioritize the data packets, for example, through a switch.

How to configure the DSCPs of the IP data packets:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **KVM connection**.
- 4. Go to the paragraph **Connection settings** and enter the following values:

DiffServ Communication (K, M, misc): Define the Differentiated Services Codepoint (DSCP) to be used for the classification of the IP packets of the Communication data packets.

NOTE: Take. into consideration that some network switches automatically assign the server class **Network Control** (DSCP name: **CS6**) for *all* data packets.

In such environments, the **DSCP 48** option must not be selected!

5. Click on Save.

Determination of the type of video transmission

In the default setting, the computer modules (IP-CPU) send the video streams via multicast to the console modules (IP-CON).

This option allows users with »Target multi access« right to connect to a computer module to which *another* user is already connected.

IMPORTANT: The multicast streams are controlled by the network switches and enable efficient distribution of the streams to multiple recipients at the same time.

Please note the requirements for the *network switch* for sending the video streams via multicast. Refer to the Installation Guide for detailed information.

Alternatively, you can specify that the computer modules (IP-CPU) send the video streams via *unicast* to the console modules (IP-CON).

The connection of a user to a computer module to which another user is already connected is *not* possible in this mode!

NOTE: This option places significantly less demands on the network switch.

You can define the type of video transmission system-wide. The system-wide setting is applied by default by all computer modules. In addition, you can specify the type of video transmission individually for each computer module (see page 120).

How to configure the system-wide multicast or unicast video transmission setting:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab KVM connection.
- 4. Enter your setting in the paragraph Multicast:

IP adress range:	Preset based on the UID
Netmask:	Preset
Multicast video:	Select On (default) to enable Mulitcast video. Select Off to disable Multicast video.
Multicast group- management:	Select Early re-use (default) or Deleyed re-use.
Group standby- time:	Enter the desired standby-time in seconds (<i>default</i> : 130 seconds).

NOTE: The *default* settings in the **Multicast** section cover most applications. Only in a few exceptional cases, you need to make adjustments in this area.

If you have any questions, please contact our support team.

5. Click on Save.

Restricting KVM-over-IP counterparts (UID locking)

By default, *each* IP matrix, *each* console module and *each* computer module is allowed to establish a KVM-over-IP connection to the matrix switch.

ADVICE: Activate the function **UID locking** if you want to *specify* which counterparts should be able to connect to the matrix switch.

How to enable/disable UID locking:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM connection**.
- 4. Enter your setting in the paragraph **UID locking**:

UID locking:	Only the counterparts specified in the list may establish a KVM-over-IP connection (Enabled), or all counterparts may establish a connection (Disabled).
Connected device UIDs:	If UID locking is switched on, activate the Permitted slider in the line of each device that is allowed to establish a connection to the matrix switch.
Add computer module:	Click this button and enter the UID of the computer module that is allowed to connect to this matrix switch. Click on Save .
Add console module:	Click this button and enter the UID of the console module that is allowed to connect to this matrix switch. Click on Save .
Add RemoteAccess- IP-CPU:	Click this button and enter the UID of the computer module that is allowed to connect to this matrix switch. Click on Save .
Add IP matrix:	Click this button and enter the UID of the IP matrix that is allowed to connect to this matrix switch. Click on Save .
Remove:	Click on a permitted counterpart and then on Remove to revoke the permission.

5. Click on Save.

Used network ports and protocols

The following network ports and protocols can be used by G&D KVM-over-IP.

IMPORTANT: Make sure that these ports and protocols are not blocked in your network.

Port	Service	Туре	Description	Note
-	IPSec	ESP	IPSec Encapsulating Security Payload	not changeable
-	IPSec	AH	IPSec Authentication Header	not changeable
22	SSH	ТСР	optional communication RemoteAccess-IP-CPU and RemoteTargets	changeable (see page 160)
49	TACACS+	UDP/ TCP	optional communication authentication service	not changeable (see page 47)
67	DHCP	UDP	DHCP server	not changeable (see page 4)
68	DHCP	UDP	DHCP client	not changeable (see page 4)
80	http	ТСР	for opening the web application (forwarding to https)	deactivatable, if forwarding is not required or desired
123	NTP	UDP	for time sync	not changeable (see page 41)
161	SNMP	UDP	optional SNMP agent	changeable (see page 62)
162	SNMP-Traps	UDP/ TCP	optional SNMP agent	changeable (see page 65)
389	LDAP	UDP/ TCP	optional communication authentication service	not changeable (see page 47)
443	https	SSL/ TCP	for opening the web application	not changeable (see page 26)
445	CIFS	ТСР	for auto-backup function	changeable (see page 90)
514	Syslog	UDP/ TCP	optional Syslog server 1/ Syslog server 2	changeable (see page 44)

636Active DirectoryUDP/ TCPoptional communication authentication servicenot changeable (see page 47)1812RadiusUDP/ TCPoptional communication authentication servicenot changeable (see page 47)2049NFSUDP/ TCPfor auto-backup function RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and (see page 160)3389RDPTCPoptional communication RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and (see page 160)5900VNCTCPoptional communication RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and (see page 160)6137U2-LANUDPoptional communication RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and (see page 160)18244KMV-over-IPUDPoptional communication RemoteAccess-IP-CPU and RemoteAccess-IP-CPU and (see page 160)18245KVM-over-IPUDPKVM-over-IP: Communication NPS or Ind device Communicationchangeable (see page 52)18246KVM-over-IPUDPKVM-over-IP: Communication Port (K, M, misc)changeable (see page 52)18246KVM-over-IPUDPStyle-Over-IP: Control Port and IPSec Internet Key Exchange (IKE)changeable (see page 52)27994Remote-PortTCPOptional Remote control for example IP Control Aprchangeable (see page 216)27995Database communica- tionTCPinternal communication, for example MatrixGuardchangeable (see pag					
1812RadiusUDP/ TCPoptional communication authentication servicenot changeable (see page 47)2049NFSUDP/ TCPfor auto-backup function for auto-backup function RemoteAccess-IP-CPUand RemoteAccess-IP-CPUand RemoteAccess-IP-CPU (see page 160)changeable (see page 160)3389RDPTCPoptional communication RemoteAccess-IP-CPU Optional communication RemoteAccess-IP-CPUchangeable (see page 160)5900VNCTCPoptional communication RemoteAccess-IP-CPUchangeable (see page 160)6137U2-LANUDPoptional communication U2-LANnot changeable (OSD)18244KMV-over-IP UDPData-Port (video, only for end device communication)changeable (OSD)18245KVM-over-IP UDPUDPKVM-over-IP: Communication Port (K, M, misc)changeable (see page 52)18246KVM-over-IP UDPUDPKVM-over-IP: Control Port and IPSec Internet Key Exchange (IKE)changeable (see page 52)27994Remote-PortTCPoptional Remote control access, for example IP Control APIchangeable (see page 216)27995Database communicationTCPinternal communication, for example MatrixGuardchangeable (see page 270)	636	Active Directory	UDP/ TCP	optional communication authentication service	not changeable (see page 47)
2049NFSUDP/ TCPfor auto-backup function (see page 90)3389RDPTCPoptional communication RemoteAccess-IP-CPU and RemoteCargetschangeable (see page 160)5900VNCTCPoptional communication RemoteAccess-IP-CPUchangeable (see page 160)6137U2-LANUDPoptional communication U2-LANnot changeable (see page 160)18244KMV-over-IPUDPKVM-over-IP: Data-Port (video, only for end device communication)changeable 	1812	Radius	UDP/ TCP	optional communication authentication service	not changeable (see page 47)
3389RDPTCPoptional communication RemoteAccess-IP-CPU and RemoteTargetschangeable (see page 160)5900VNCTCPoptional communication RemoteAccess-IP-CPUchangeable (see page 160)6137U2-LANUDPoptional communication U2-LANnot changeable 	2049	NFS	UDP/ TCP	for auto-backup function	changeable (see page 90)
5900 VNCTCPoptional communication RemoteAccess-IP-CPUchangeable (see page 160) 6137 U2-LANUDPoptional communication U2-LANnot changeable (see page 160) 18244 KMV-over-IPUDPKVM-over-IP: Data-Port (video, only for end device 	3389	RDP	ТСР	optional communication RemoteAccess-IP-CPU and RemoteTargets	changeable (see page 160)
6137U2-LANUDPoptional communication U2-LANnot changeable (OSD)18244KMV-over-IPUDPKVM-over-IP: Data-Port (video, only for end device communication)changeable (OSD)18245KVM-over-IPUDPKVM-over-IP: Communication Port (K, M, misc)changeable (see page 52)18246KVM-over-IPUDPKVM-over-IP: 	5900	VNC	ТСР	optional communication RemoteAccess-IP-CPU	changeable (see page 160)
18244KMV-over-IPUDPKVM-over-IP: Data-Port (video, only for end device communication)changeable (OSD)18245KVM-over-IPUDPKVM-over-IP: Communication Port (K, M, misc)changeable 	6137	U2-LAN	UDP	optional communication U2-LAN	not changeable
 18245 KVM-over-IP UDP KVM-over-IP: Communication Port (K, M, misc) 18246 KVM-over-IP UDP KVM-over-IP: Control Port and IPSec Internet Key Exchange (IKE) 27994 Remote-Port TCP optional Remote control access, for example IP Control API 27996 Database communica- tion TCP internal communication, for exsample MatrixGuard changeable (see page 216) changeable (see page 270) 	18244	KMV-over-IP	UDP	KVM-over-IP: Data-Port (video, only for end device communication)	changeable (OSD)
18246KVM-over-IPUDPKVM-over-IP: Control Port and IPSec Internet Key Exchange (IKE)changeable (see page 52)27994Remote-PortTCPoptional Remote control access, for example IP Control APIchangeable (see page 216)27996Database communica- tionTCPinternal communication, for exsample MatrixGuardchangeable (see page 270)	18245	KVM-over-IP	UDP	KVM-over-IP: Communication Port (K, M, misc)	changeable (see page 52)
 27994 Remote-Port TCP optional Remote control access, for example IP Control API 27996 Database communication, for example MatrixGuard (see page 216) (see page 216) 	18246	KVM-over-IP	UDP	KVM-over-IP: Control Port and IPSec Internet Key Exchange (IKE)	changeable (see page 52)
27996 Database TCP internal communication, changeable communication for exsample MatrixGuard (see page 270)	27994	Remote-Port	ТСР	optional Remote control access, for example IP Control API	changeable (see page 216)
	27996	Database communica- tion	ТСР	internal communication, for exsample MatrixGuard	changeable (see page 270)

NOTE: It is possible that additional ports are used, e.g. when using the optional *RemoteAccess-Streaming-Features* (see *Remote gateways and remote targets* on page 147 ff.).

Database mode

In the default setting, each matrix switch has the database mode **Leader** and administers its own database.

IMPORTANT: It is *not* possible to edit the database mode when using the **DirectRedundancyShield** function (see page 272 ff.).

How to edit the database mode:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Database mode.
- 4. Enter your setting in the paragraph Edit database mode:

Database mode:	Select Leader (<i>default</i>) if the matrix switch is to assume the role of the database leader and should store the database in this device. Select Follower if the matrix switch should take over the settings of another matrix switch.			
Database port (local):	Enter the number of the port to be used (<i>default</i> : 27996).			
Database IP (remote):	If you have selected the database mode Follower , enter the IP address of the matrix switch that has the database role Leader .			
Database port (remote):	If you have selected the database mode Follower , enter the database port of the matrix switch that has the database role Leader .			
NOTE: In general, no manual adjustments need to be made in the Database mode				

NOTE: In general, no manual adjustments need to be made in the **Database mode** section. The settings are controlled via the wizards of the **Advanced features**.

If you have any questions, please contact our support team.

5. Click on Save.

Click on **Test database connection** to check, if the set database is available.

Monitoring functions

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

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

IP matrix							
Sea	rch	Х			\$		
	Name 🕈	-	Status	Main power	Temperature	•	
	CCIP2.0		Online	On	40.5 °C		

Figure 4: Detailed view of an exemplary monitoring table

The values configured for the table view (see *Configuring table columns* on page 10) are listed in the table.

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

Viewing all monitoring values

You can see the list of all monitoring values under Matrix systems.

NOTE: Matrix switches with firmware version 1.1.000 or higher additionally support monitoring of the computer and console modules.

How to show a list of all monitoring values:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to check and then click on Configuration.
- 3. Click on the tab **Monitoring**.

The displayed table contains a list of all available monitoring values.

4. Click on Close.

Enabling/disabling monitoring values

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

Deactivated monitoring values are not displayed in the web application.

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

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

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

How to enable/disable all monitoring values:

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

Advanced features for managing critical devices

The **Monitoring status** icon (see *User interface* on page 8) shows you at a glance whether all monitoring values are within the normal range (green icon) or if at least one monitoring value is outside the normal range (yellow or red icon).

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

Displaying the list of critical monitoring values

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

The Active alarms dialog shows any critical values.

Confirm the alarm of a critical device

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

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

How to acknowledge the monitoring message of a device:

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

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

Practical use of the SNMP protocol

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

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

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

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

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

Configuring an SNMP agent

How to configure an SNMP agent:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Go to the paragraph **SNMP agent**.

5. Enter the following values under *Global*:

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

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

Access:	Activate read access (View), write access (Full) or deny access (No) via the <i>SNMPv2c</i> 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 <i>Community</i> which has also been selected in the <i>Network Management System</i> .

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

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

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

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

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

8. Click on Save.

Adding and Configuring SNMP traps

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the tab Network.
- 3. Go to the paragraph **SNMP trap**.
- 4. Click on Add or on Edit.
- 5. Enter the followng values under **Global**:

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

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

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

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

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

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

Username:	Enter the username for the communication with the <i>Network Management System</i> .
Authentication protocol:	Select the authentication protocol which has been activated in the <i>Network Management System</i> :
	■ SHA-1
	■ SHA-224
	■ SHA-256
	■ SHA-384
	■ SHA-512
	- MD5 (defende)
	• MD5 (dejaut)
NOTE: As it is now known that MD5 does not offer collision resistance it recommended to use it.	
Authentication passphrase:	Enter the authentication passphrase for secure communica- tion with the <i>Network Management System</i> .

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

8. Click on Save.

How to delete an existing trap:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the tab Network.
- 3. Go to the paragraph **SNMP trap**.
- 4. In the row of the receiver you want to delete, click on Delete.
- 5. Click on Save.

Users and groups

Efficient rights administration

The web application administrates up to 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.

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

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

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

The effective right

The effective right determines the right for a particular operation.

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

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

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

Right	User JDoe	Group Office	Group Computer- ModuleConfig	Effective right
Computer module config	No	No	Yes	Yes
Change own password	No	Yes	No	Yes
(Computer module) Access	Yes	View	No	Yes

The settings of the *Computer module config* and *Change own password* rights result from the rights assigned to the user groups. The *(Computer module) Access* right is given directly in the user account.

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

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

Efficient user group administration

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

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

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

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

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

In both cases, the user is provided with the Yes effective right for Change device configuration.

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

Administrating user accounts

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

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

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

Creating a new user account

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

IMPORTANT: If an individual password policy is to be taken into account, you must configure the password complexity (see *Password complexity* on page 16) before creating a new user account.

How to create a new user account:

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

Name:		Enter a user name.
	NOTE: User name external directory (see <i>User authentice</i>)	s can be subject to a naming convention when using services <i>ation with directory services</i> on page 47 ff.).
Ρ	assword:	Enter the user account password.
Confirm password:		Repeat the password.
C	lear text:	If necessary, mark this entry to view and check both passwords.
F	ull name:	If desired, enter the user's full name.
Comment:		If desired, enter a comment regarding the user account.
Enabled:		Mark this checkbox to activate the user account.
	NOTE: If the user KVM system.	account is deactivated, the user is not able to access the

4. Click on Save.

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

5. If two-factor authentication is activated on the device (see page 50), the settings for the user account must be made in the next step (see page 72).

Activating two-factor authentication (optional)

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

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

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

IMPORTANT: To activate or deactivate 2FA for a user profile, the user needs superuser rights (see page 86), or the user must be logged in with the corresponding user profile (see page 86) and have the right *Change own password* (see page 87).

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

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

How to activate 2FA in the user account:

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

E	ncryption key:	When the parameter 2FA for this user is changed from Disabled to Enabled , a encryption key is generated and displayed automatically.
	IMPORTANT: B	ase32 format must be used for the entry.
		Click on Generate to obtain a new encryption key.
Hash algorithm: • SHA1 • SHA256 (<i>default</i>) • SHA512		 SHA1 SHA256 (<i>default</i>) SHA512
Validity period (secs):		Enter how long the 2-Factor Auth Code (TOTP) should remain valid. The value entered must be between 10 and 200 seconds (<i>default</i> : 30 seconds).
	ADVICE: It is a as access proble rectly.	good idea to avoid selecting a validity period that is too short, ems could otherwise occur if the time is not synchronised cor-
Length of = 6 digits (<i>default</i>) 2-Factor Auth Code (TOTP): • 8 digits		6 digits (<i>default</i>)8 digits
2-Factor Auth Code (TOTP) window width:		The window width specifies how many previous 2-Factor Auth Codes (TOTP) are valid in addition to the current one. It is not possible to allow future 2-Factor Auth Codes (TOTP). The value entered must be between 1 and 20 (<i>default</i> : 1).
	ADVICE: To av being synchron 2-Factor Auth	oid access problems from occurring as the result of the time not ised correctly, it can be a good idea to permit several previous Codes (TOTP).
Show QR code & copy security key: Clickin A secu contain scan in to the c		Clicking the button validates the entries that have been made. A security key is generated and a QR code is displayed that contains the generated security key and that can be used to scan in with an authenticator app. The security key is copied to the clipboard.
V	erification code:	Enter a verification code here that you receive from a hardware token or an authenticator app that you are using. Only numbers can be entered in this field.

6. Click on Save.

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

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

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

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

Change the rights of this special user account to configure the rights of users without their own account (see *Changing the user account rights* on page 77).

Deactivate the user *RemoteAuth* to prevent users from logging in to the KVM system without their own user account (see *Enabling or disabling a user account* on page 80).

Once 2FA has been activated in the user acoount, the 2-Factor Auth Code (TOTP) will be queried in addition to the username and password on login (see *Starting the web application* on page 6).

Renaming a user account

How to change the name of a user account:

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

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

Changing the password of a user account

NOTE: The activated *Superuser* right

(see Rights for unrestricted access to the system (Superuser) on page 86 ff.)

or the right Change own password

(see Rights to change your own password on page 87 ff.)

are prerequisite for changing the password of a user account.

NOTE: When changing the password, any defined password policies (see *Password complexity* on page 16) are taken into account.

How to change the password of a user account:

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

Current password:	Enter the current password.
NOTE: No entry is rights (see page 86	required in this field for users with activated superuser ff.).
New password:	Enter the new password.
Confirm password:	Repeat the new password.
Clear text:	Mark this entry to view and check entered passwords.
Verification code:	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.
NOTE: The 2-Fa two-factor auther and activated (see p	actor Auth Code (TOTP) is only requested if ntication has been configured (see page 50 f.) age 72 ff.).

Changing the user account rights

Any user account can be assigned with different rights.

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

System rights

Name	Right	Page
Superuser right	Unrestricted access to the configuration of the system	page 86
Config Panel Login	Login to the ConfigPanel web application	page 86
EasyControl Login	Access to EasyControl tool	page 87
Change own password	Change own password	page 87
Confirm monitoring alert	Confirmation of a monitoring alarm	page 87

Global device rights

Name	Right	Page
Edit personal profile	Change personal user settings	page 205
Computer module config	Configuration of computer modules	page 103
Permission to replace device	Execution of the "Replace device"-function	page 88
MultiAccess	Access type when a computer module is simultaneously accessed	page 97
Access to exclusive signals	Access to exclusive signals	page 128
Access to USB devices	Access USB devices	page 100

Computer module rights and device group rights

Name	Right	Page
Access	Access to a computer module or a target group	page 94
MultiAccess	Access type when a computer module is simultaneously accessed	page 97
Access to exclusive signals	Access to exclusive signals	page 128
Access to USB devices	Access USB devices	page 100

Console module rights

Name	Right	Page
Push-Get	Carry out Push-Get function	page 213

Scripting rights and scripting group rights

Name	Right	Page
Execution	Execute scripts and script groups	page 224

Changing a user account's group membership

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

How to change a user account's group membership:

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

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

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

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

Enabling or disabling a user account

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

How to enable or disable a user account:

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

If you want to block access to the system with this user account, unmark the checkbox.

4. Click on Save.

Deleting a user account

How to delete a user account:

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

Administrating user groups

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

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

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

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

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

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

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

4. Click on Save.

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

Renaming a user group

How to rename a user group:

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

Changing the user group rights

The various user groups can be assigned with different rights.

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

System rights

Name	Right	Page
Superuser right	Unrestricted access to the configuration of the system	page 86
Config Panel Login	Login to the ConfigPanel web application	page 86
EasyControl Login	Access to EasyControl tool	page 87
Change own password	Change own password	page 87
Confirm monitoring alert	Confirmation of a monitoring alarm	page 87

Global device rights

Name	Right	Page
Edit personal profile	Change personal user settings	page 205
Computer module config	Configuration of computer modules	page 103
Permission to replace device	Execution of the "Replace device"-function	page 88
MultiAccess	Access type when a computer module is simultaneously accessed	page 97
Access to exclusive signals	Access to exclusive signals	page 128
Access to USB devices	Access USB devices	page 100

Computer module rights and device group rights

Name	Right	Page
Access	Access to a computer module or a target group	page 94
MultiAccess	Access type when a computer module is simultaneously accessed	page 97
Access to exclusive signals	Access to exclusive signals	page 128
Access to USB devices	Access USB devices	page 100

Console module rights

Name	Right	Page
Push-Get	Carry out Push-Get function	page 213

Scripting rights and scripting group rights

Name	Right	Page
Execution	Execute scripts and script groups	page 224

Administrating user group members

How to administrate user group members:

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

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

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

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

6. Click on Save.

(De)activating a user group

How to (de)activate a user group:

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

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

4. Click on Save.

Deleting a user group

How to delete a user group:

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

System rights

Rights for unrestricted access to the system (Superuser)

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

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

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

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

Activated:	Allow full access to the KVM system and the connected devices $% \mathcal{A}^{(n)}$
Deactivated:	Deny full access to the KVM system and the connected devices

5. Click on Save.

Changing the login right to the web application

How to change the login right to the web application:

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

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

Rights to access the EasyControl tool

How to change the rights to access the *EasyControl* tool:

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

Yes: Allow access to the *EasyControl* tool

No: Deny access to the *EasyControl* tool

5. Click on Save.

Rights to change your own password

How to change the right to change your own password:

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

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

5. Click on Save.

Authorization to confirm a monitoring alarm

How to change the authorization to confirm a monitoring alarm:

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

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

Authorisation to execute the »Replace device« function

If a computer or a console module is replaced by new 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.

In the default settings, the authorisation to execute the function is limited to the administrator and all users with activated superuser rights.

If desired, the authorization can be granted to other users.

How to change the right to change your own password:

- 1. In the menu, click on User or User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems**.
- 4. Go to the Global device rights section.
- 5. Under **Permission to replace device**, select between the following options:

Activated:	Allow users to execute the function
Deactivated:	Deny users to execute the function

Advanced functions of the KVM system

Identifying a device by activating the Identification LED

Some devices provide an *Identification* LED.

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

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

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

Saving the configurations

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

How to save the configuration of the KVM system:

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

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

Saving the configurations with auto backup function

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

How to use the auto backup function:

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

Auto Backup:	 By selecting the corresponding entry in the pull-down menu, you can enable or disable the auto backup function: Disabled (<i>default</i>) Enabled
Filename profiv:	Entor the filename prefix
r nename prenx.	ADVICE: When the auto backup function is enabled, the file- name prefix field is automatically filled with the UID of the device. You can change this entry.
	IMPORTANT: Only letters (upper and lower case), numbers (<i>0</i> to <i>9</i>) and the characters - and _ are permitted. The prefix may contain a maximum of 25 characters.
Backup password:	Optional: Enter a password to secure the backup file.
	IMPORTANT: Double inverted commas (" and ") cannot be used here.
Backup scope:	Select the scope of data you want to back up: You can back up either the network settings and/or the application settings .
Path:	Enter the path for the backup files.
	IMPORTANT: The syntax of the path specification differs depending on the selected protocol.
	Examples:
	• NFS: name:/directory1/directory2
	CIFS: //name/directory1/directory2
Protocol:	Choose between the following protocols:
	NFS (default)CIFS
Port:	Enter the port. This field is filled automatically depending on the selection in the <i>protocol</i> field:
	2049 (when selected <i>NFS</i>)445 (when selected <i>CIFS</i>)

User:	Optional: Enter the name of the user.
Password:	Optional: Enter a password to secure the share.
Time:	Enter the following data:
	• Hour (numbers 0 to 23)
	• Minute (numbers 0 to 59)
Selection of the day:	You can choose between the following options:
	 1. to 31. day of the month Select all (avery day of the month)
	• Select all (every day of the month)

4. Click on Save & Test or Save.

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

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

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

Restoring the configurations

How to restore the configuration of the KVM system:

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

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

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

7. Click Restore.

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

Activating premium functions

With every purchase of a premium function (see *Optional functions* on page 206 ff.), you receive a feature key. This file contains a key to activate the purchased function(s).

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

IMPORTANT: The *SecureCert feature* is only available with the order of new devices. After sales implementation is **not** possible!

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

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

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

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

5. Click on Save.

ADVICE: You can display the activated functions in the respective overview table. For this, add the Active features column (see *Configuring table columns* on page 10 ff.)

2 Matrix system

In the *Matrix systems* menu of the web application, you can configure various settings of the matrix switches and the devices connected.

IMPORTANT: If optional DirectRedundancyShield (see page 272) is activated, on the passive matrix switch, configuration is only possible to a limited extend. Switch to the web application of the device with active DRS status. Carry out the configuration there and then simply transfer it from there using the "DirectRedundancyShield (DRS)" wizard (see *Step 2: Adjust configuration* on page 276 ff.).

The following pages provide a detailed description of these settings.

Computer modules

Computer modules connect computers to the KVM matrix system and can be accessed with console modules.

Adjusting access and configuration rights

Access rights to a computer module

ADVICE: We recommend using computer module groups to help assign all computer module access rights (see page 165).

This makes it easier to keep an overview of the KVM matrix system. It also benefits the operating performance of the system's on-screen display (OSD).

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

How to change computer module access rights:

- 1. In the menu, click on **User** or on **User groups**.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Individual rights** in the selection area on the right-hand side.
- 4. In the **Individual computer module rights** field, you can select the desired computer module on the left-hand side.

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

5. In the **Access** field on the right-hand side of the dialogue, you can select between the following options:

Yes:	Allow full access to the computer connected to the computer module.
No:	Deny access to the computer connected to the computer module.
View:	View screen contents of the computer connected to the computer module

- 6. Repeat steps 5 and 6 if you want to change the access rights for other computer modules.
- 7. Click on Save.

Access rights to a computer module group

How to change the computer module group access rights:

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Device group rights** in the selection area on the right-hand side.
- 4. In the **Device group rights** field, you can select the desired computer module group on the left-hand side.

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

5. In the **Access** field on the right-hand side of the dialogue, you can select between the following options:

Yes:	Allow full access to the computer modules of the group.
No:	Deny access the computer modules of the group.
View:	View screen contents of a computer module of a group

- 6. Repeat steps 5 and 6 if you want to change the access rights for other computer modules.
- 7. Click on Save.

Access mode for simultaneous access to computer modules

In the default settings of the KVM matrix system only one user can access a computer module.

This restriction can be lifted by changing the *MultiAccess* right for a user account or a user group.

After being assigned with *MultiAccess right*, a user or a user group can access computer modules even if they are already accessed by another user.

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

NOTE: The right for simultaneous access to computer modules depends on the user's effective right (see page 68). The effective right is the highest right and results from the individual right of a user account and the rights of the assigned group(s).

How to change the MultiAccess right for *all* computer modules:

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Global device rights** in the selection area on the right-hand side.
- 4. Select one of the options given under MultiAccess:

Yes:	Allow access to a computer module already accessed by another user
No:	Deny access to a computer module already accessed by another user
View:	When connecting to a computer module with an already active connection, only the monitor image is displayed. no inputs possible
How to change the MultiAccess right for a *particular* computer module:

NOTE: MultiAccess rights can be configured and used only if a user or a user group is assigned with the required rights to access the computer module (see page 94 f.).

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Individual rights** in the selection area on the right-hand side.
- 4. In the **Individual computer module rights** field, you can select the desired computer module on the left-hand side.

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

5. Select one of the options given under MultiAccess on the right-hand side:

Yes:	Allow access to a computer module already accessed by another user
No:	Deny access to a computer module already accessed by another user
View:	When connecting to a computer module with an already active connection, only the monitor image is displayed. no inputs possible

How to change the MultiAccess right for *a particular* computer module group:

NOTE: MultiAccess rights can be configured and used only if a user or a user group is assigned with the required rights to access the computer module (see page 94 f.).

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Device group rights** in the selection area on the right-hand side.
- 4. In the **Device group rights** field, you can select the desired computer module group on the left-hand side.

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

5. Select one of the options given under MultiAccess on the right-hand side:

Yes:	Allow access to a computer module of a computer module group already accessed by another user
No:	Allow access to a computer module of a computer module group already accessed by another user
View:	When connecting to a computer module with an already active connection, only the monitor image is displayed. no inputs possible

Access to USB devices

In the defaults of the matrix system, users have access to the USB devices of a channel group.

If required, this right can be denied by changing the right »Access to USB devices« of a user account or a user group.

You can either deny users the right to access USB devices of a particular computer module globally (for all computer modules to which a user or a user group has access) *or* you can change the rights for particular computer modules or computer module groups only.

NOTE: The access right depends on the user's effective right (see page 68). The effective right is the highest right and results from the individual right of a user account and the rights of the assigned group(s).

How to change the right to access USB devices for *all* computer modules:

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Global device rights** in the selection area on the right-hand side.
- 4. Select one of the options given in the Access to USB devices field:

Yes:	Allow access to USB devices.
No:	Deny access to USB devices.

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

NOTE: USB access rights can be configured and used only if a user or a user group is assigned with the required rights to access the computer module (see page 94 f.).

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Individual rights** in the selection area on the right-hand side.
- 4. In the **Individual computer module rights** field, you can select the desired computer module on the left-hand side.

IMPORTANT: Configure USB access rights for the computer module that provides the main KVM channel of the channel group. The USB channel is assigned to the same channel group.

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

5. Select one of the options given in the **Access to USB devices** field:

Yes:	Allow access to USB devices.
No:	Deny access to USB devices.

6. Click on Save to save your settings.

How to change the right to access USB devices for *a particular* computer module group:

NOTE: USB access rights can be configured and used only if a user or a user group is assigned with the required rights to access the computer module (see page 94 f.).

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Device group rights** in the selection area on the right-hand side.
- 4. In the **Device group rights** field, you can select the desired computer module group on the left-hand side.

IMPORTANT: Configure USB access rights for the computer module that provides the main KVM channel of the channel group. The USB channel is assigned to the same channel group.

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

5. Select one of the options given in the **Access to USB devices** field:

Yes:	Allow access to USB devices of computer module group.
No:	Deny access to USB devices of computer module group.

Rights to configure computer modules

How to change the right to view and edit the configuration of a computer module:

- 1. In the menu, click on **User** or on **User groups**.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Global device rights** in the selection area on the right-hand side.
- 4. Select one of the options given under Computer module config:

Yes:	Allow user or user group to view and edit the computer module configuration.
No:	Deny user or user group to view and edit the computer module configuration.

5. Click on Save.

Basic configuration of computer modules

Changing the name of a computer module

During the start-up of the KVM matrix system any computer modules are named automatically.

How to change the name of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Enter the name of the computer module in the **Name** field of the *Device* section.
- 4. Click on Save.

Changing the comment of a computer module

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

ADVICE: For example, use the comment field to note where the computer module is placed.

How to change the comment of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Enter any comment in the **Comment** field of the *Device* section.
- 4. Click on Save.

Deleting a computer module from a KVM matrix system

If the system is not able to find a computer module that has previously been integrated in the KVM system, the system assumes that the device is switched off. If a computer module has been permanently removed from the system, you can manually delete it from the list of computer modules.

NOTE: You can delete only computer modules that are switched off.

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

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to delete and then click on Delete.
- 3. Confirm the confirmation prompt by clicking on **Yes** or cancel the process by clicking on **No**.

Copying configuration settings to a new computer module

If a computer module of the KVM matrix system is replaced by another device, you can copy the configuration settings of the device to be replaced to the new device. After you copied the configuration settings to the new device, you can operate it immediately.

IMPORTANT: The computer module whose settings you copy to a new device will then be deleted from the KVM matrix system.

How to copy configuration settings to a new computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the new device.
- 3. Open the Service tools menu and select the item Replace device.
- 4. Select the device whose configuration settings you want to copy.
- 5. Click on Save.

Copying the configuration settings of a computer module

You can copy the configuration settings **General**, **KVM connection**, **Channels**, **GPIO** (if supported by the device) and/or **Monitoring**) of a computer module to the settings of one or multiple other computer modules.

NOTE: The name of and the comment about the computer module are not copied.

How to copy the configuration settings of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module whose configuration you want to copy.
- 3. Click on Service tools and then click on Copy configuration.
- 4. In the upper area, you can select which settings of the computer module you want to copy (General, KVM connection and/or Monitoring).
- 5. In the lower area, select the computer modules to which you want to copy the data.
- 6. Click on **Copy configuration**.

Settings for special hardware

(De)Activating an USB keyboard mode the Generic USB mode

USB computer modules support different USB input devices. You can use the special features of a USB input device after selecting the specific USB keyboard mode.

As an alternative to the specific USB keyboard modes, you can also use the **generic USB** mode. In this mode, the data from the USB devices connected to the interface of the console module is transmitted to the active computer module.

IMPORTANT: The **generic USB** mode supports USB mass storage devices and many available HID device. However, being able to operate particular USB device in generic USB mode can not be guaranteed.

• USB keyboards: In addition to the keys of standard keyboard layouts, the default USB keymode PC Multimedia supports several multimedia keys like Loud and Quiet.

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

The following table lists the supported USB keyboards:

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

• **Displays and tablets:** You can operate computers connected to the computer module with one of the supported *displays* or *tablets* (depending on model):

INPUT DEVICE	SETTING
HP 2310tk	→ HP 2310t
iiyama T1931	∙iiyama T1931
iiyama TF2415	∙ iiyama TF2415
NOTTROT N170 KGE	 NOTTROT N170 KGE
Wacom Cintiq 21UX Gen 1	 Wacom Cintiq 21UX
Wacom Cintiq 21UX Gen 2	• Wacom Cintiq 21UX Gen2
Wacom Cintiq Pro 24 Pen	 Wacom Cintiq Pro 24 Pen
Wacom Cintiq Pro 27	• Wacom Cintiq Pro 27
Wacom Cintiq Pro 32 Pen	 Wacom Cintiq Pro 32 Pen
Wacom Cintiq Pro 32 Touch	• Wacom Cintiq Pro 32 Touch
Wacom DTK-2451	• Wacom DTK-2451
Wacom Intuos3	• Wacom Intuos 3
Wacom Intuos4 S	 Wacom Intuos 4 S
Wacom Intuos4 M	 Wacom Intuos 4 M
Wacom Intuos4 L	• Wacom Intuos 4 L
Wacom Intuos4 XL	 Wacom Intuos 4 XL
Wacom Intuos5 S	 Wacom Intuos 5 S
Wacom Intuos5 M	• Wacom Intuos 5 M
Wacom Intuos5 L	• Wacom Intuos 5 L
Wacom Intuos Pro L	• Wacom Intuos Pro L

• **Generic-USB mode:** In this mode, data of the USB device connected to the interface of the console module is transmitted to the computer module without being altered.

INPUT DEVICE	SETTING	
any USB mass storage or USB HID device	 Generic USB 	

IMPORTANT: The **generic USB** mode supports many available USB mass storage devices and HID devices. However, being able to operate particular device in generic USB mode can not be guaranteed.

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

INPUT DEVICE	SETTING
Contour ShuttlePRO v2	 Contour Shuttle Pro 2

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

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

INPUT DEVICE	SETTING
LK463-compatible keyboard	→ LK463

How to select a USB keyboard mode:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Select the desired option in the **USB HID mode** field of the *Configuration* paragraph (see table on page 106):.

NOTE: Update the firmware of both the matrix switch and the computer module if the web application does not show all keyboard modes.

Adjusting the operating mode of the RS232 interface

In the default setting of the computer module, you can connect any RS232-compatible device to the RS232 interface of the computer module (depending on model). The RS232 data stream is transmitted unchanged to the console module.

For transmitting RS422 signals, you can use two **G&D RS232-422 adapters**. Each of the adapters converts the RS232 interface of the console module and the computer module into **RS422** interfaces.

IMPORTANT: If you want to transmit **RS422** signals, in addition to using adapters, you also need to change the operating mode of the *RS232* interfaces of both the console *and* the computer module.

How to set the operating mode of the RS232 interface of the computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab **General**.
- 4. Select one of the options of the **Serial communication** field under the paragraph **Configuration**:

R\$232:	The data stream of an RS232 device is transmitted from the computer module to the console module (<i>default</i>).
RS422:	The data stream of an RS422 device is transmitted from the computer module to the console module via separately available G&D RS232-422 adapters.

Defining the EDID profile to be used

The EDID information (*Extended Display Identification Data*) of a monitor inform the graphics card of the connected computer about various technical features of the device.

The EDID profile of the monitor connected to the console module is not available at the computer module. Therefore, the computer module transmits a standard profile to the computer. The EDID information of this profile is optimised for most graphics cards.

We provide additional profiles for special resolutions.

ADVICE: In some cases it is recommended to read out the EDID profile of the console monitor and activate the configuration of the computer module afterwards.

How to choose the EDID profile to be transmitted to the computer:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. In the **EDID profile** field of the *Configuration* section, you can select either the default profile (**Device specific default profile**) or another profile from the list.

NOTE: The names of G&D profiles provide information on the profile's resolution and refresh rate.

For example, the profile **GUD DVI1024D4 060 1280×1024/60** is provided for a resolution of 1280×1024 pixels at a 60 Hz refresh rate.

Reducing the colour depth of image data to be transmitted

By default, the computer module transmits image information with a maximum colour depth of 24 bit to the console module.

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

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

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

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

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. In the **Colour depth** field of the *Configuration* section, you can select one of the following options:

24 Bit: Transmit image data with a maximum colour depth of 24 bits.18 Bit: Reduce colour depth of image data to 18 bits.

Advanced features

Wake On LAN

Wake on LAN (WoL) is a standardized method to start a computer that is powered off or in sleep mode via a network command. If a WoL-compatible and accordingly configured computer receives a so-called magic packet on the LAN connection, the network card and BIOS initiate the startup process. In addition to the network card and the BIOS, the computer's operating system also needs to be configured accordingly.

The matrix switch also supports this function to use WoL in a KVM installation.

How to configure WoL function:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. In the section *Wake On LAN*, enter the following data:

Wake On LAN:	Enable or disable the <i>WoL</i> function.
MAC-Adresse:	Enter the MAC address of the WoL-compatible and configured computer connected to the selected computer module.
Password:	Enter a password if a password has been stored on the computer at the WoL setup.
Automatic Wake On LAN on connection:	Enable or disable the automatic Wake On LAN when connection to the defined computer module.

4. Click on Save.

How to send a WoL command to the defined computer:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure.
- 3. Öpen the **Service tools** menu and click on **Wake On LAN** to send the WoL command to the defined computer.

Sending a key combination after disconnecting all users

Use the **Key Macros** function to send a key combination to the computer connected to the computer module after having disconnected all users.

NOTE: For example, send the key combination Win+L to lock a Windows computer after disconnecting all users.

How to configure a key macro:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Under Key-Macros, select one of the following options:

Send a key combination after disconnecting all users:	Enable or disable the <i>Key Macro</i> function.
Key combination:	Select up to three of the listed keys that are sent to the computer together as a key combination.

4. Click on Save.

Enabling/disabling the keyboard signal

In the default settings, the signals of keyboard and mouse connected to the console are transmitted to a computer module.

In the settings of the computer modules of the VisionXS-IP series, you can enable or disable the transmission of the keyboard signal.

How to enable/disable the transmission of the keyboard signal:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. In the **Keyboard activated** field of the *Configuration* section, select one of the following options:

Enabled:	Transmit keyboard signals to the computer module of this channel (<i>default</i>).
Disabled:	Do not transmit keyboard signals to the computer module.

Multi-user information

If multiple users are accessing a computer module (multi-user mode), *multi-user* information can be activated. This way, all users accessing a computer module are provided at the console module with the information that *at least* one other user is currently accessing the same computer module.

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 enable or disable multi-user information for the entire system:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on Configuration.
- 3. Select one of the options given under Multi-user display:

On:	Enables the display of <i>multi-user</i> information
Off:	Disables the display of <i>multi-user</i> information

4. Click on Save.

How to enable or disable the display of *multi-user* information for a *particular* user account:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. Select one of the options given under Multi-user OSD info:

Off:	Disables the display of <i>multi-user</i> information
On:	Enables the display of <i>multi-user</i> information
System:	Apply global system settings (see above)

Configure Mouse mode | CrossDisplay-Switching

If you want to use the *CrossDisplay-Switching* function, we recommend that you activate the function for the entire system (see *Enabling CrossDisplay-Switching for the entire system* on page 243 ff.). This affects all computer modules that use the system-wide setting *(default).*

You can override the system-wide settings for each computer module and enable or disable *CrossDisplay-Switching* for certain computer modules only.

ADVICE: You can also disable the system settings and enable *CrossDisplay-Switching* only in the settings of computer modules on which you want to use the function.

ADVICE: You can also configure the CDS settings of computer modules comfortably with a wizard (see *Step 6: Configure CDS settings of computer modules* on page 249 ff.).

How the change CDS settings of a specific computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. In the field **Mouse mode | CrossDisplay-Switching**, you can select between the following options:

System:	Apply global system settings (default)
Relative mouse coordingates CDS disabled:	Disable CrossDisplay-Switching.
Absolute mouse coordinates CDS activatedt:	Enable CrossDisplay-Switching.

How to change the mouse speed for a specific computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. Move the **CDS mouse speed** slider to the desired value.
- 5. Click on Save.

How to adjust the CrossDisplay resolution of a specific computer module:

NOTE: With active *CrossDisplay-Switching*, the mouse speed is not controlled by the operating system of the computer but by the matrix switch.

If the cursor speed changes between horizontal and vertical mouse movements, the monitor resolution could not be auto detected.

In such cases, a resolution of 1680×1050 pixels applies. If the monitor's resolution differs from this resolution, the mouse moves as described above.

In this case, you can adjust the monitor resolution manually.

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the General tab.
- 4. Disable the Auto option in the CDS resolution field.
- 5. Enter the vertical and horizontal resolution in the input boxes.
- 6. Click on Save.

How to change the mouse position for a specific computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. In the **CDS mouse positioning** field, you can select between the following options:

System:	Apply global system settings (default)
Off:	The mouse cursor remains at the position at which the switching to the module of the next monitor takes place.
On:	According to the CDS mouse hideout setting the mouse cursor is positioned so that it is barely visible.
	Only during <i>multi-user access</i> , the cursor remains at the position at which the switching to the next monitor takes place.
On (multi access:	According to the CDS mouse hideout setting, even during <i>multi-user access</i> , the mouse cursor is positioned so that it is barely visible.

ADVICE: You can enable or disable this function for particular modules independently from the selected system setting (see below).

5. With activated CDS mouse positioning, you can select between the following options in the **CDS mouse hideout** field:

Right:	The mouse cursor is placed on the right edge of the monitor so that it is barely visible.
Bottom:	The mouse cursor is placed on the bottom edge of the monitor so that it is barely visible.

Extended settings of KVM-over-IP connection

Limiting the bandwidth

By default, the KVM extender uses the maximum available bandwidth of a Gigabit Ethernet. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

EXAMPLE: Typical bandwidth requirements for KVM-over-IP:

- 3840 × 2160 = 800-900 Mbit/s (office application with approx. 40% of changes)
- 2560 × 1440 = 600-500 Mbit/s (office application with approx. 40% of changes)
- 1920 × 1080 = 300-400 Mbit/s (office application with approx. 40% of changes)
- Window maximization: 900 Mbit/s at 3840 × 2160
- Still image: 20 Mbit/s at 3840 × 2160

How to set a limit for the bandwidth of a KVM-over-IP connection:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM connection**.
- 4. In the section **Connection settings** you can set the bandwidth limit in Mb/s under **Max. bandwidth**.

NOTE: Entering the value **0** deactivates the limit.

Classifying IP packets (DiffServ)

For QoS purposes (Quality of Service) you have the possibility to use **Differentiated Services Codepoints** (DSCP) to classify the IP packets.

Through this classification, you can prioritize the data packets, for example, through a switch.

How to configure the DSCPs of the IP data packets:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM connection**.
- 4. Go to the paragraph **Connection settings** and enter the following values:

 DiffServ
 Define the Differentiated Services Codepoint (DSCP) to be used for the classification of the IP packets of the Data data packets.

 NOTE:
 Take. into consideration that some network switches automatically assign the server class Network Control (DSCP name: CS6) for *all* data packets.

 In such environments, the DSCP 48 option must not be selected!

5. Click on Save.(

De)Activating signals

By default, not only keyboard, video and mouse data but also audio data are transmitted.

In addition, you can enable the transmission of RS232 data and, alternatively, disable the transmission of audio data.

How to (de)activate the transmission of audio or RS232 signals:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM connection**.
- 4. Under **Deactivatable signals** select the desired option in the line **Audio**. Select the desired option in the line **Serial communication**.
- 5. Click on Save.

Determination of the type of video transmission

In the default setting, the computer modules (IP-CPU) send the video streams via multicast to the console modules (IP-CON).

This option allows users with »Target multi access« right to connect to a computer module to which *another* user is already connected.

IMPORTANT: The multicast streams are controlled by the network switches and enable efficient distribution of the streams to multiple recipients at the same time.

Please note the requirements for the *network switch* for sending the video streams via multicast. Refer to the Installation Guide for detailed information.

Alternatively, you can specify that the computer modules (IP-CPU) send the video streams via *unicast* to the console modules (IP-CON).

The connection of a user to a computer module to which another user is already connected is *not* possible in this mode!

NOTE: This option places significantly *less* demands on the network switch.

You can define the type of video transmission system-wide (see page 53). The system-wide setting is applied by default by all computer modules. In addition, you can specify the type of video transmission individually for each computer module.

How to configure the individual multicast or unicast video transmission settings of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab KVM connection.
- 4. Enter your setting in the paragraph Multicast in the line Multicast video:

System:	Apply global system settings (see page 53).
Disabled:	Multicast video disabled.
Enabled:	Multicast video enabled.

Viewing status information of a computer module

How to view the status information of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the tab **Information**.
- 4. The following information is displayed in the dialog box that opens now (depending on model):

Name:	Name of computer module
Device ID:	Unique ID of computer module
Status:	Current status (Online or Offline) of computer module
Class:	Device class
Firmware name:	Firmware name
Firmware rev.:	Firmware version
Hardware rev.:	Hardware version
IP address Netzwork:	IP address of Network interface(s)
IP address Transmission:	IP address of Transmission interface
MAC Network:	MAC addres of Network interface(s)
MAC Transmission:	MAC address of Transmission interface
Serial number:	Serial number of the module

NOTE: In addition, *Active features* and the *Monitoring* information of the device are displayed.

5. Click on Close.

Restarting a computer module

Use this function to restart a computer module. Before restarting you will be prompted for confirmation to prevent an accidental restart.

How to restart a computer module using the web application:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to restart.
- 3. Open the Service tools menu and select the item Restart.
- 4. Confirm the security prompt by clicking on Yes.

Updating the firmware of computer modules

You can update the firmware of computer modules comfortably via web application.

How to update the firmware of computer modules:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to update.
- 3. Click on **Service tools** and then click on **Firmware update**.
- 4. Click on Supply firmware image files.

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

Select the firmware file on your local data carrier and click on Open.

NOTE: Press the Shift key to select multiple firmware files using the left mouse key.

The firmware file is transferred to the internal device memory and can then be selected for the update.

- 5. Select the firmware files to be used from the internal device memory and click on **Continue**.
- 6. If required, select the **Target version** of the devices if you have selected several firmware files for one device in step 5.
- 7. Click on the Update slider of all devices you want to update.
- 8. Click Run update.

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

Console modules

The computers connected to the system are operated via the console modules of the KVM matrix system.

Operating modes of console modules

Depending on the intended use, you can select the console module's operating mode from the following options:

Standard operating mode

NOTE: The standard operating mode is the default operating mode.

The standard operating mode only permits the access to the KVM matrix system after users are authenticated with their username, password and optional 2-factor authentication (see page 72) if set up.

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

OpenAccess operating mode

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

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

IMPORTANT: For the configuration of access rights, a user account is created for each console mdoule with activated *OpenAccess* mode.

The user account of an *OpenAccess* console applies to all users at this console module.

ADVICE: The user accounts of the *OpenAccess* console modules are marked with a *OAC* symbol.

The color of the symbol indicates whether the corresponding console is currently operating in *OpenAccess* mode (green) or is operating neither in *OpenAccess* mode nor in *video* mode (gray, the console module has been switched back to *standard* operating mode).

Video operating mode

A video console is only possible when combined with the optional *Push-get function* (see page 211). It 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, entires can be made on the on-screen display only.

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

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

NOTE: A video console *does not* create an occupancy state.

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

Selecting the console module's operating mode

How to select the console module's operating mode:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the **Operating mode** field, you can select between the following options:

Standard:	Standard operating mode
OpenAccess console:	OpenAccess operating mode
Video:	Video operating mode

NOTE: Selecting the *OpenAccess* or *Video* options activates further submenus to configure the access rights.

Basic configuration of console modules

Changing names or comments of console modules

How to change names or comments of console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the Name field, you can rename the console module.
- 5. In the **Comment** field, you can change or enter comments about the console module.
- 6. Click on Save.

Enabling or disabling console modules

You can disable a console module if you want to deny its access to the KVM matrix system.

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

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

How to enable or disable a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab
- 4. In the **Enabled** field, you can choose between the following options:

Enabled:	Console module is enabled.	
Disabled:	Console module is disabled.	

Copying configuration settings to a new console module

If a console module of the KVM matrix system is replaced by another device, you can copy the configuration settings of the device to be replaced to the new device.

After you copied the configuration settings to the new device, you can operate it immediately.

IMPORTANT: The console module whose settings you copied to a new device will be deleted from the KVM matrix system.

How to copy configuration settings to a new console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the *new* device.
- 3. Open the Service tools menu and select the item Replace device.
- 4. Select the device whose configuration settings you want to copy.
- 5. Click on Save.

Copying the configuration settings of a console module

You can copy the configuration settings **General**, **KVM connection**, **Channels**, **GPIO** (if supported by the device) and/or **Monitoring** of a console module to the settings of one or multiple other console modules.

NOTE: The name of and the comment about the console module are not copied.

How to copy the configuration settings of a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module whose configuration you want to copy.
- 3. Click on Service tools and then click on Copy configuration.
- 4. In the upper area, you can select which settings of the console module you want to copy (General and/or Monitoring).
- 5. In the lower area, select the console modules to which you want to copy the data.
- 6. Click on **Copy configuration**.

Deleting a console module from the KVM matrix system

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

Manually delete the console module you want to permanently remove from the system from the list of console modules.

NOTE: Only administrators and users with the *superuser* right can delete inactive console modules.

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

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to delete and click on Delete.
- 3. Confirm the confirmation prompt by clicking on **Yes** or cancel the process by clicking on **No**.

(De)Activating access to exclusive signals

There are signals that cannot be connected to several console modules at the same time (e.g. Generic-HID, RS232, GPIO). In the default setting, the console module that connects to computer module first is given access to these exclusive signals.

It may be that the exclusive signals are not needed at this console module or that certain users should not have access to them. Therefore, access to the exclusive signals can be deactivated for console modules as well as users and user groups.

How to (de)activate access to exclusive signals for a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 1. Click on the console module you want to configure and then click on **Configuration**.
- 2. Click on the tab **General**.
- 3. Select one of the options of the **Access to exclusive signals** field under the paragraph **Configuratio**

Enabled:	Basically access to the exclusive signals (default)
Disabled:	No access to the exclusive signals

IMPORTANT: The user only has access to the exclusive signals if the access is enabled at the corresponding console module **and** the user has the corresponding right (*default*).

Rights for access to exclusive signals

You can either change the global settings to allow access to exclusive signals (for all computer modules to which a user or a user group has access) *or* you can change the rights for particular computer modules or computer module groups only.

NOTE: The right for access to exclusive signals depends on the user's effective right (see page 68). The effective right is the highest right and results from the individual right of a user account and the rights of the assigned group(s).

How to change the rights to access exclusive signals for *all* computer modules:

- 1. In the menu, click on User or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Global device rights** in the selection area on the right-hand side.
- 4. Select one of the options given under Access to exclusive signals:

Enabled:	Basically access to the exclusive signals (default)
Disabled:	No access to the exclusive signals

IMPORTANT: The user only has access to the exclusive signals if the user has the corresponding right **and** the access is enabled at the corresponding console module (*Standard*).

How to change the rights to access exclusive signals for a particular computer module:

- 1. In the menu, click on Users or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Individual rights** in the selection on the right-hand-side.
- 4. In the **Individual computer module rights** field, you can select the desired computer module on the left-hand side.

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

5. Select one of the options given in the Access to exclusive signals field:

Enabled:	Basically access to the exclusive signals (default)
Disabled:	No access to the exclusive signals

IMPORTANT: The user only has access to the exclusive signals if the user has the corresponding right **and** the access is enabled at the corresponding console module (*Standard*).

How to change the rights to access exclusive signals for a *particular* computer module group:

- 1. In the menu, click on Users or on User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Device group rights** in the selection on the right-hand-side.
- 4. In the **Device group rights** field, you can select the desired computer module group on the left-hand side.

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

5. Select one of the options given in the Access to exclusive signals field:

Enabled:	Basically access to the exclusive signals (default)
Disabled:	No access to the exclusive signals

IMPORTANT: The user only has access to the exclusive signals if the user has the corresponding right **and** the access is enabled at the corresponding console module (*Standard*).

Settings for special hardware

Support of any USB devices

In **Generic USB** mode, the data from the USB devices connected to the interface of the console module is transmitted to the active computer module.

NOTE: When the **Generic USB** mode is enabled, it is *not possible* to operate the OSD with a keyboard connected to the **Generic** interface.

IMPORTANT: The **Generic USB** mode supports many available HID devices (including FIDO security keys, for example). However, the operation of a particular HID device in **Generic USB** mode can not be guaranteed.

In **Generic USB** mode, you can connect USB hubs or USB composite devices to the **Generic** interface of the console module.

NOTE: In *multiuser* mode, the generic USB device is available on the first active console module. Once this console module logs off and another console module logs in, the generic USB device of the other console module is available.

How to enable/disable the Generic USB mode of a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the Generic USB field, you can select between the following options:

Disabled:	You can connect either a USB keyboard or a USB mouse to the Generic interface of the console module.
Enabled:	Data from any USB device connected to the Generic interface is transmitted to the active computer module.

IMPORTANT: To use a generic USB device, enable the USB HID mode **Generic USB** of the computer modules you want to access (see page 106).

Reinitialising USB input devices

After connecting a USB keyboard or mouse to the console module, the input devices are initialised and can be used immediately.

Some USB input devices require a reinitialisation of the USB connection. Enable the automatic reinitialisation of USB devices if a USB keyboard or mouse does not respond to your inputs during operation.

How to enable/disable the reinitialisation of USB devices:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. Under USB Auto Refresh, you can choose between the following options:

Off:	The status of the USB devices is not monitored. If communication to a USB device is interrupted, the device is not reinitialised.
All devices:	The status of the USB devices is monitored. If communication to one USB device is interrupted, all devices are reinitialised.
Only faulty devices:	The status of USB devices is monitored. If the communication with a USB devices is interrupted, this device is reinitialised (<i>recommended setting</i>).
Advanced functions

Automatic user logout

A console module can be configured in a way that the access to the computer 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. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the General tab.
- 4. In the **Auto logout (minutes)** field, you can set the time (between **1** to **999** minutes) for the automatic logout.

NOTE: Entering the value »0« disables the automatic user logout.

5. Click on Save.

Configuring default execution after a user logon

After a user has logged on to a console module, the OSD usually opens on the screen of said console module.

The configuration setting **Default execution** allows you to define a computer module that is automatically accessed after a user logs on. As an alternative, you can also define a script that runs automatically.

IMPORTANT: If the **Return to last computer module** function (see page 136 f.) or the **Restore last FreeSeating session** function (see page 137 f.) is activated, the user's configured default action is ignored.

How to select a default computer module that is automatically executed after a user logon:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. In the **Default execution** field, select the option **Default computer module**.
- 5. Scroll down to the **Default target** area.

6. Click on the slider of the desired default computer module in the column **Default** computer module (enabled).

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

7. Click on Save.

How to select a default script or a script group that is automatically executed after a user logon:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on Configuration.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. In the **Default execution** field, select the option **Default script/script group**.
- 5. Scroll down to Default script/script group.
- Click on the slider of the desired default script/script group in the column Default script/script group.

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

7. Click on Save.

How to disable the configured default action:

- 1. In the menu, click on User.
- 2. Click on the user account you want to configure and then click on Configuration.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. In the **Default execution** field, select the option **None**.
- 5. Click on Save.

Return to the last computer module

Enable the **Return to last computer module** function in your personal profile to remember the computer module you accessed before logging out of the system. After the next login, you will automatically be switched to this computer module.

NOTE: Turning off the console module on which the user is logged in is treated like a logout.

IMPORTANT: If the **Return to last computer module** function is activated, the user's configured default execution (see page 134 f.) isignored.

How to enable automatic access to the last accessed computer module:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. Select the option Return to last computer module under Restore last session.
- 5. Click on Save.

Restore the last FreeSeating session

Enable the **Restore last FreeSeating session** function in the personal profile to save the connection status of FreeSeating members. With this function, the last connection state can be restored when logging in again at the same workplace or another workplace that is set up and configured accordingly. By logging in or logging out to the Tradeswitch leader, all other FreeSeating members are automatically logged in with the same user (if no other user is logged in yet) or logged out (if the same user is logged in).

IMPORTANT: The prerequisite for this is the activation and configuration of the premium *Tradeswitch* function (see page 230 ff.).

NOTE: Turning off the console module on which the user is logged in is treated like a logout.

IMPORTANT: If the **Restore last FreeSeating session** function is activated, the user's configured default execution (see page 134 f.) isignored.

How to enable the restore last FreeSeating session function:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on Configuration.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. Select the option Restore last FreeSeating session under Restore last session.
- 5. Click on Save.

Deactivation of the Restore last session function

How to disable the Restore last session function:

- 1. In the menu, click on User.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tab **KVM matrix systems** and click on **Personal profile** in the selection area on the right-hand side.
- 4. Select the option Off under Restore last session.
- 5. Click on Save.

Automatically disconnecting access to computer modules

Console modules can be configured in a way that the active access to a computer module is automatically disconnected after a 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 displayed on the right-hand side is shown on the screen of the console module.

How to automatically disconnect the access to a computer module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the **Auto disconnect (minutes)** field, you can set the time (between **1** to **999** minutes) for automatically disconnecting the access to a computer module.

NOTE: The value 0 disables the automatic disconnection when a computer module is accessed.

Remembering a username in the login box

If the same users often works at a certain console module, their 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. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the **Remember last user** field, you can select between the following options:

 Yes:
 The system remembers the last user.

 No:
 The system does not remember the last user.

Setting the hold time for the screensaver

The screensaver deactivates the screen display at the console module 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 computer.

How to set the hold time of the screensaver:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. In the **Screensaver (minutes)** field, you can set the holding time (**1** to **999** minutes) for activating the screensaver.

NOTE: Entering the value 0 disables the screensaver of the console module.

5. Click on Save.

Setting the hold time for the login screensaver

The screensaver deactivates the screen display at the console module 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 computer.

How to set the hold time of the screensaver:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. In the **Login screensaver (minutes)** field, you can set the holding time (**1** to **999** minutes) for activating the screensaver.

NOTE: Entering the value 0 disables the screensaver of the console module.

Enabling or disabling DDC/CI support

Most of the computer and console modules supported by the *Vision IP series* system are ready to support monitors with **DDC/CI** functionality.

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

You can set the **DDC/CI** support for the entire system. The system-wide setting is used by all console modules. In addition, you can define these settings for each console module individually.

How to configure the sytem-wide setting of the DDC/CI support:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. In the DDC/Cl field, you can select between the following options:

Disabled:	Disable transmission of DDC/CI signals (default).
CPU > monitor:	Carry out transmission of DDC/CI signals exclusively from computer module to monitor.
Bidirectional:	Carry out transmission of DDC/CI signals bidirectionally.

How to configure the individual settings of the DDC/CI support of a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the General tab.
- 4. In the **DDC/Cl support** field, you can select between the following options:

System:	Use system-wide setting (see above).
Disabled:	Disable transmission of DDC/CI signals (default).
CPU > monitor:	Carry out transmission of DDC/CI signals exclusively from computer module to monitor.
Bidirectional:	Carry out transmission of DDC/CI signals bidirectionally.

Adjusting the operating mode of the RS232 interface

In the default setting of the console module, you can connect any RS232-compatible device to the RS232 interface of the console module (depending on model). The RS232 data stream is transmitted unchanged to the computer module.

Fro transmitting RS422 signals, you can use two **G&D RS232-422 adapters**. Each of the adapters converts the RS232 interface of the console module and the computer module into **RS422** interfaces.

IMPORTANT: If you want to transmit **RS422** signals, in addition to using adapters, you also need to change the operating mode of the *RS232* interfaces of both the console *and* the computer module.

How to set the operating mode of the RS232 interface:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration.
- 3. Click on the General tab.
- 4. Select one of the options of the **Serial communication** field under the paragraph **Configuration**:

RS232:	The data stream of an RS232 device is transmitted from the console module to the computer module (<i>default</i>).
RS422:	The data stream of an RS422 device is transmitted from the console module to the computer module via separately available G&D RS232-422 adapters.
Tradeswitch:	With the tradeswitch mode you can use optional LED sets. This facilitates locating the monitor (computer) to which the keyboard/mouse focus is switched to (see page 230).

Restarting a console module

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

How to restart a console module via web application:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to restart.
- 3. Click on Service tools and then click on Restart.
- 4. Confirm the security prompt with Yes.

Updating the firmware of a console module

You can use the web application to update the firmware of a console module.

How to update the firmware of a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to update.
- 3. Click on Service tools and then click on Firmware update.
- 4. Click on Supply firmware image files.

ADVICE: If the firmware file is already stored in the internal device memory, you can skip this step.

Select the firmware file on your local data carrier and click on Open.

ADVICE: Press the Shift key to select multiple firmware files using the left mouse key.

The firmware file is transferred to the internal device memory and can then be selected for the update.

- 5. Select the firmware files to be used from the internal device memory and click on **Continue**.
- 6. If required, select the **Target version** of the devices if you have selected several firmware files for one device in step 5.
- 7. Click on the Update slider of all devices you want to update.
- 8. Click on Run update.

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

Viewing status information of a console module

How to view the status information of a console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the **Information** tab.
- 4. Now you are provided with the following information:

Name:	Name of the console module
Device ID:	Unique ID of the console module
Status:	Current status (Online or Offline) of the console module
Klasse:	Device class
Firmware name:	Firmware name
Firmware rev:	Firmware version
Hardware rev.:	Hardware version
IP address Transmission:	IP address of the <i>Transmission</i> interface(s)
MAC Transmission:	MAC address of the Transmission interface(s)
Serial number:	Serial number of the module

NOTE: In addition, *Active features* and the *Monitoring* information of the device are displayed.

5. Click on Close.

Remote gateways and remote targets

The computer modules of the **RemoteAccess-IP-CPU** series let you integrate virtual machines into the IP matrix switch. You can access these virtual machines via network.

NOTE: To establish a network connection to virtual machines, you can use the **SSH**, **VNC** or **RDP** protocol.

With the fee-based **RemoteAccess Streaming Feature**, streams can also be received via **RTP/TCP**, **RTSP/TCP** and **MMSH** transport protocols. The **H.264**, **VP8** and **VP9** codecs for decoding video data and **MPGA**, **MP3** and **AC3** for decoding audio data are supported.

Like other computer modules, the virtual machines connected via these computer modules are integrated into the OSD and the operating concept of the matrix switch:

As usual, you connect to a virtual machine (*remote target*) via the **Select** menu in the OSD and can also use functions such as *push-get*, *multi-user access* or *CrossDisplay-Switching* with these virtual machines.

The instructions and functions provided in the chapter *Computer modules* on page 94 ff. also apply for remote targets (apart from marked exceptions).

To connect a *remote target*, you need to configure the *remote gateway*, the different *remote targets* and the *remote pools*.

NOTE: The following terms are important to distinguish in connection with remote targets:

• **Remote gateway:** Each connected computer module of the **RemoteAccess-IP-CPU** series is listed under *Remote Gateways* in the web application.

Remote gateways establish a connection between a KVM matrix system and virtual machines

• **Remote targets:** Configured virtual machines are called remote targets within a KVM matrix system. They are listed under *Remote targets* in the web application

• **Remote pools:** A remote pool groups all remote targets that are accessible via the remote gateways included in the pool.

NOTE: You can adjust the mouse speed of a *remote target*. Further information on this topic are provided on page 249 of this manual and in the separate OSD manual.

Configuring remote gateways

Changing the name of a remote gateway

How to change the name of a remote gateway:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the remote gateway/computer module you want to configure and then click on **Configuration**.
- 3. Enter the name in the **Name** field of the *Device* section.
- 4. Click on Save.

Changing the comment of a remote gateway

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

How to change the comment of a remote gateway:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the remote gateway/computer module you want to configure and then click on **Configuration**.
- 3. Enter any comment in the **Comment** field of the *Device* section.
- 4. Click on Save.

Configuring the network interface

The device provides a network interface. This interface is used to connect to one of the virtual machines and allows direct access to the web application.

By default, the following settings of the Network interface are preselected:

- IP address of the *Network* interface: Obtain address via **DHCP** (Fallback: IP address:192.168.0.1)
- Global network settings: Obtain settings via DHCP

How to configure the settings of a network interface:

NOTE: The *Link Local* address space 169.254.0.0.0/16 is reserved for internal communication between devices according to RFC 3330. It is not possible to assign an IP address of this address space!

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **Network**.
- 4. Enter the following values under Network:

Operating mode:	Select the operating mode of Network :
	Static: A static IP address is assigned.DHCP: Obtain IP address from a DHCP server.
IP address:	Enter the IP address of the interface if the operating mode <i>Static</i> is selected.
Netmask:	Enter the netmask of the network if the operating mode <i>Static</i> is selected.

Configuring global network settings

Global network settings ensure that the web application is accessible from all subnetworks, even in complex networks.

How to configure global network settings:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network.
- 4. Select the section Global settings.
- 5. Enter the following values:

Operating mode:	Enter the desired operating mode:
	• Static: Use of static settings.
	• DHCP : Obtain settings from a DHCP server.
Hostname:	Enter the hostname of the device.
	IMPORTANT: If the DHCP server itself does not assign a host- name when DHCP is enabled, the hostname entered here is used. Otherwise the hostname obtained from the DHCP server is used.
In the <i>DHCP</i> of cally. Making	perating mode the following settings are obtained automati- entries is not possible.
Domain:	Enter the domain to which the device should belong.
Gateway:	Enter the IP address of the gateway.
DNS server 1:	Enter the IP address of the DNS server.
DNS server 2:	Optionally, enter the IP address of another DNS server.

Assigning a remote pool

A *remote pool* groups all remote targets that are accessible via the existing remote gateways included in the pool.

All *remote targets* and *remote gateways* are automatically assigned to the default pool. If you want to limit the accessibility, you can do so at any time by assigning a pool that you have defined.

How to change the pool assignment of a remote gateway:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **Remote pool**.
- 4. In the Assigned column, click on the slider of the pool (enabled) to which you

NOTE: Each remote gateway belongs to exactly *one* remote pool.

If you don't select a *specific* pool, the remote gateway automatically belongs to the default pool.

want to assign the remote gateway.

5. Click on Save.

Extended settings of KVM-over-IP connection

Limiting the bandwidth

By default, the maximum available bandwidth of a Gigabit Ethernet is used. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

How to set a limit for the bandwidth of a KVM-over-IP connection:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **KVM connection**.
- 4. In the section **Connection settings** you can set the bandwidth limit in Mb/s under **Max. bandwidth**.

NOTE: Entering the value **0** deactivates the limit.

Classifying IP packets (DiffServ)

For QoS purposes (Quality of Service) you have the possibility to use **Differentiated Services Codepoints** (DSCP) to classify the IP packets.

Through this classification, you can prioritize the data packets, for example, through a switch.

How to configure the DSCPs of the IP data packets:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab KVM connection.
- 4. Go to the paragraph **Connection settings** and enter the following values:

DiffServ
Data (AR, V):Define the Differentiated Services Codepoint (DSCP) to be used for
the classification of the IP packets of the Data data packets.

NOTE: Take. into consideration that some network switches automatically assign the server class **Network Control** (DSCP name: **CS6**) for *all* data packets.

In such environments, the DSCP 48 option must not be selected!

5. Click on Save.

(De)Activating signals

By default, not only keyboard, video and mouse data but also audio data are transmitted.

How to (de)activate the transmission of audio signals:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab KVM connection.
- 4. Under **Deactivatable signals** select the desired option in the line **Audio**.
- 5. Click on Save.

Determination of the type of video transmission

In the default setting, the computer modules (RemoteAccess-IP-CPU) send the video streams via multicast to the console modules (IP-CON).

This option allows users with »Computer module multi access« right to connect to a computer module to which *another* user is already connected.

IMPORTANT: The multicast streams are controlled by the network switches and enable efficient distribution of the streams to multiple recipients at the same time.

Please note the requirements for the *network switch* for sending the video streams via multicast. Refer to the Installation Guide for detailed information.

Alternatively, you can specify that the computer modules (RemoteAccess-IP-CPU) send the video streams via *unicast* to the console modules (IP-CON).

The connection of a user to a computer module to which another user is already connected is *not* possible in this mode!

NOTE: This option places significantly less demands on the network switch.

You can define the type of video transmission system-wide (see page 53). The system-wide setting is applied by default by all computer modules. In addition, you can specify the type of video transmission individually for each computer module.

How to configure the individual multicast or unicast video transmission settings of a computer module:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab KVM connection.
- 4. Enter your setting in the paragraph Multicast in the line Multicast video:

System:	Apply global system settings (see page 53).
Disabled:	Multicast video disabled.
Enabled:	Multicast video enabled.

Viewing monitoring values

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

How to open the list containing all monitoring values:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab **Monitoring**.

The displayed table contains a list of all available monitoring values.

4. Click on Save.

NOTE: Chapter *Monitoring functions* on page 59 ff. provides more information on how to configure monitoring values.

Viewing status information of a remote gateway

How to view the status information of a remote gateway:

- 1. In the menu, click on Matrix systems > [Name] > RemoteGateways.
- 2. Click on the remote gateway you want to configure and then click on **Configuration**.
- 3. Click on the tab **Information**.
- 4. The following information is displayed in the dialog box that opens now:

Name:	Name of the remote gateway	
Device ID:	Unique ID of the remote gateway	
Status:	Current status (<i>online</i> or <i>offline</i>) of the remote gateway	
Class:	Device class	
Firmware name:	Firmware name	
Firmware rev.:	Firmware version	
Hardware rev.:	Hardware version	
IP address A:	IP address of the network interface	
IP address Transmission:	IP address of the transmission interface	
MAC A:	MAC address of the network interface	
MAC Transmission:	MAC address of the transmission interface	
Serial number:	Serial number of the module	

NOTE: In addition, *Active features* and the *Monitoring* information of the device are displayed.

5. Click on Close.

Configuring remote targets

Changing the name of a remote target

How to change the name of a remote target:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Enter the name of the remote target in the Name field of the Device section.
- 4. Click on Save.

Changing the comment of a remote target

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

How to change the comment of a remote target:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Enter any comment in the **Comment** field of the *Device* section.
- 4. Click on Save.

Saving the resolution of a virtual machine

To make sure the video signal from the virtual machine is displayed correctly on the console modules, you need to provide information about the resolution set in the virtual machine.

How to save the resolution set in a virtual machine in the KVM matrix system:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Select the resolution set in the virtual machine in the **Resolution** field on the *General* tab:

1024x768/60Hz/VESA DMT	
1280x1024/60Hz/VESA DMT	
1680x1050/60Hz/VESA CVT	
1600x1200/60Hz/VESA DMT	
1920x1080/60Hz/CTA-861-D	
2560x1440/60Hz/VESA CVT-RB	
2560x1600/60Hz/VESA CVT-RB	
3840x2160/30Hz/VESA CVT-RB	

Reducing the colour depth of the image data to be transmitted

By default, a remote target transmits image information with a maximum colour depth of 24 bit to the console module.

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

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

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

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

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. In the **Colour depth** field of the *Configuration* section, select one of the following options:

24 Bit: Transmit image data with a maximum colour depth of 24 bits.

18 Bit: Reduce colour depth of image data to 18 bits.

4. Click on Save.

Holding a connection

IMPORTANT: Activating this option may pose a security risk, since reconnecting to the remote target *within the holding period* does not require a new login!

In the default setting of the matrix switch, the existing connection is disconnected when switching from a *remote target* to a "*classic*" *computer module* or to a remote target of another pool. The connection to the "classic" computer module is then established.

You can also hold the connection to the remote target for a specified period of time (1 to 10 minutes) or **permanently**. Within this time span, you can quickly continue the existing connection by reconnecting to the console module.

NOTE: When connecting to another remote target of the same pool, the existing connection cannot be maintained, since only one connection via a remote gateway is possible at any time.

How to set the hold period of a connection:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Set the holding period in the **Hold connection** field of the *Configuration* paragraph between **1** and **10** minutes or **permanently**.

You can also disable the hold function (No).

4. Click on Save.

Connection repeats

If the connection to a remote target is interrupted or not possible, you can configure a number and interval of connection repeats.

NOTE: Connection repeats are **disabled** in the default settings.

How to set the number and the interval of connection repeats:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. In the **Number of connection repeats** field under *Configuration*, you can define the number of connection repeats (between **0** and **999**).
- 4. In the **Interval of connection repeats (seconds)** field, you can define an interval between **1** and **999** seconds at which several connection repeats are executed.
- 5. Click on Save.

Defining the connection parameters for a remote target

How to configure the basic connection parameters for a remote target:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Click on the tab **Connection**.
- 4. Enter the following values:

IP address/DNS name:	Enter the IP address or name of the virtual machine.
Protocol:	Select the protocol used to connect the virtual machine:
	 SSH VNC RDP Streaming
Port:	Enter the port to be used to connect to the terminal server.

5. When selecting the **RDP** protocol, additionally enter the following information:

Remote FX optimisation:	Enable Remote FX optimisation if supported by the RDP server.
	You can enable RemoteFX optimisation specifically for static images (Image) of a common desktop environment or for moving images (Video).

6. When selecting the **VNC** protocol, additionally enter the following information:

Quality:	Select a quality level between 0 (low) and 9 (high).
Compression:	Select a compression level between ${\bf 0}$ (fast) and ${\bf 9}$ (best).
Cursor highlighting:	After enabling the function, the local cursor (circle) of the <i>RemoteAccess-CPU</i> is displayed in addition to the cursor of the virtual machine.

7. When selecting the **Streaming** protocol, additionally enter the following information:

Audio delay:	Set the delay in the range from -2500 to 2500 ms.
--------------	---

Saving login data or use the matrix credentials for login

To automatically log on a user after connecting to the virtual machine, you can save the login data in the web application.

Alternatively you have the option to use the login data of the matrix for the login of the remote targets, as well.

How to capture the credentials for login of the remote target:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Click on the tab **Connection**.
- 4. Enter the following values:

Use matrix credentials:	Enable or disable this function.
	Default: function is disabled.
	If you enable this function, any remote target credentials (username and password) that may have been entered are ignored.
Username	Enter the username of the user to log on.
Password	Enter the password of the user to log on.

NOTE: Depending on the configuration of the virtual machine, it is sometimes necessary to enter both username *and* password; sometimes you only need to enter the password!

Assigning a remote pool

A *remote pool* groups all remote targets that are accessible via the existing remote gateways included in the pool.

All *remote targets* and *remote gateways* are automatically assigned to the default pool. If you want to limit the accessibility, you can do so at any time by assigning a pool that you have defined.

How to change the pool assignment of a remote target:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Click on the tab Remote pool.
- 4. In the Assigned column, click on the slider of the pool (enabled) to which you

NOTE: Each remote target belongs to exactly one remote pool.

If you don't select a *specific* pool, the remote target automatically belongs to the default pool.

want to assign the remote target.

5. Click on Save.

Viewing monitoring values

You can see the list of all monitoring values under RemoteTargets.

How to open the list containing all monitoring values:

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Click on the tab Monitoring.

The displayed table contains a list of all available monitoring values.

4. Click on Save.

NOTE: The chapter *Monitoring functions* on page 59 ff. provides more information on how to configure monitoring values.

Viewing status information of a remote target

How to view the status information of a remote target

- 1. In the menu, click on Matrix systems > RemoteTargets.
- 2. Click on the remote target you want to configure and then click on **Configuration**.
- 3. Click on the tab Information.
- 4. The following information is displayed in the dialog box that opens now:

Name:	Name of the remote target
Device ID:	Physical ID of the remote target
Status:	Current status (online or offline) of the remote target
Class:	Device class

NOTE: In addition, the *Monitoring* information of the remote target are displayed.

5. Click on Close.

Computer module groups and view filters

Computer modules of the KVM matrix system can be arranged in computer module groups and view filters.

Intended use of computer module groups

Creating computer module groups enables administrators to quickly assign the rights of a user or a user group to all computer modules within a group.

NOTE: The different computer modules can be members of *multiple* computer module groups.

Intended use of view filters

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

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

Administrating computer module groups

The »New IP targets« computer module group

By default, the *New IP targets* computer module group is created in the KVM matrix system. This group automatically contains all computer 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 computer modules, change the device group rights (see page 94) of either the user account or the user group.

Creating a new computer module group

How to create a new computer module group:

- 1. In the menu, click on **Computer module groups**.
- 2. Click on Add computer module group and select the type of group you want to add.
- 3. In the **Name** field, you can enter the name of the computer module group.
- 4. In the **Comment** field, you can enter a comment about the computer module group.
- 5. Click on Save.

NOTE: You can assign the rights for this computer module group by changing the device group rights (see page 96) of either the user account or the user group.

Changing the name or comment of a computer module group

How to change the name or comment of a computer module group:

- 1. In the menu, click on **Computer module groups**.
- 2. Click on the computer module group you want to configure and then click on **Configuration**.
- 3. In the Name field, you can change the name of the computer module group.
- 4. In the **Comment** field, you can enter or change a comment about the computer module group.
- 5. Click on Save.

Administrating computer module group members

NOTE: You can assign up to 20 computer modules to each computer module group of the KVM matrix system.

How to administrate the members of a computer module group:

- 1. In the menu, click on Computer module groups.
- 2. Click on the computer module group you want to configure and then click on **Configuration**.
- 3. Click on the **Members** tab.
- 4. In the **Members** column, click on the slider of the computer modules you want to add to the group (enabled).

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

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

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

6. Click on Save.

Deleting a computer module group

How to delete a computer module group:

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

Administrating view filters

To administrate view filters, you can use the **View filter** wizard provided in the menu **Advanced features**.

The wizard shows you how to set up, configure and assign a view filter to one or more user accounts.

How to start the »View filter« wizard:

- 1. In the menu, click on Advanced features.
- 2. Click on View filter and then click on Configuration.
- 3. Follow the instructions of the wizard.

Creating a new view filter

How to create a new view filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In Step 1 of the wizard, click on Add.
- 3. In the Name field, you can enter a name.
- 4. In the **Comment** field, you can enter a comment.
- 5. Click on Save.

Changing the name of a view filter

How to change the name of a view filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In **Step 1** of the wizard, click on the view filter you want to edit and then click on **Edit**.
- 3. Edit the name of and/or the comment about the view filter.
- 4. Click on Save.

Deleting a view filter

How to delete a view filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In **Step 1** of the wizard, click on the view filter you want to delete and then click on **Delete**
- 3. Confirm the confirmation prompt by clicking on Yes or cancel the process by clicking on No.

Adding a computer module to a view filter

How to add a computer module to a view filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In **Step 1** of the wizard, click on the view filter you want to edit and then click on **Edit**.
- 3. In **Step 2**, click on the slider (in the **Show devices** column) of the computer modules you want to add to the view filter.

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

NOTE: To *simultaneously* assign all computer modules to a view filter, mark the check box in the header of the **Show devices** column.

Deleting a computer module from a view filter

How to delete a computer module from the view filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In **Step 1** of the wizard, click on the view filter you want to edit and then click on **Edit**.
- 3. In **Step 2**, click on the slider (in the **Show devices** column) of the computer modules you want to delete from the view filter.

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

NOTE: To *simultaneously* delete all displayed computer modules from the view filter, mark the check box in the header of the **Show devices** column.
Assigning a view filter as default in the OSD

How to set a default filter:

- 1. Start the View filter wizard (see page 168 f.).
- 2. In **Step 1** of the wizard, click on the view filter you want to edit and then click on **Edit**.
- 3. In Step 2, assign one or multiple computer module(s) to the view filter.
- 4. In **Step 3**, click on the slider (in the **Use as default in OSD** column) of the user accounts that will use the view filter as default in the OSD (enabled).

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

NOTE: To *simultaneously* set a view filter as default for all displayed user accounts, mark the check box in the header of the **Use as default in OSD** column.

Accessing computer modules via select keys

After you have defined Select-Key modifier key(s) and a Select-Key Set and activate a Select-Key Set in the user account, you can connect to a computer module by pressing key combinations on the console module keyboard.

Changing select key modifier or valid key type

Select keys enable you to quickly access a particular computer module with a key combination. For this, you can create *select key sets* in the KVM matrix system.

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

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

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Select *at least* one of the listed modifiers under **Select key modifier** in the *Configuration* paragraph by marking the respective entry:

- Ctrl	- Win
- Alt	- Shift
Alt Gr	

4. In the Valid select keys field, you can select one of the following options:

Only numbers:	<i>Only numerical keys</i> are interpreted as select keys when pressed in combination with the select key modifier
Only characters:	<i>Only alphabetic keys</i> are interpreted as select keys when pressed in combination with the select key modifier
Numbers and characters:	<i>Alphabetical and numerical keys</i> 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 desired computer.

5. Click on Save.

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.

Within a select key set, you can define select keys for computer modules you want to access.

NOTE: Global select key sets are available for all users of the KVM matrix system.

You can administrate select key sets comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Select keys**. Click on **Configuration** to start the wizard.

The following paragraphs briefly summarise the wizard's configuration options.

Step 1: Select a matrix switch

• Select the matrix switch on which you want to store the configuration of the select key set.

NOTE: After you selected a matrix switch, you will see the current configuration of the **select key modifier** and the **valid select keys** (see above). If required, you can change these settings directly in this menu.

Step 2: Select a user

• Select a user account for which the configured select keys will be available. When selecting the entry **Available for all (global)**, you create a global select key set that will be available for all users.

Step 3: Select key sets

- Select the select key set you want to configure.
 Click on the buttons Add, Edit or Delete to add a new select key set or to edit or delete an existing set.
- Click on the slider **Activate select key set for current user** if you want to activate the set for the user selected in step 2.

IMPORTANT: If you have selected the table entry **Available for all (global)** in step 2, clicking on the slider activates the set for all users.

NOTE: Only by assigning a select key set to a user account, the select keys defined in the set are accepted as inputs on the console module and switching to the corresponding computer module takes place.

Step 4: Configure a select key set

• Enter the desired key combinations for the computer modules.

ADVICE: In the line **Return to last computer module** you can define a key combination for switching to the computer module that was switched on last.

Automatic or manual switching between computer modules

Auto scanning all computer modules (Autoscan)

The *Autoscan* function successively accesses all computer modules that are included in the active scan mode set and available to users.

The *Scantime* setting (see page 175) enables you to define how long you want to switch to a computer module.

When switching to a computer module, the console module name, the name of the currently accessed computer module, and a note regarding the *Autoscan* function are displayed.

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

During inputs, the Autoscan function stops and continues after the inputs are finished.

Applying the Autoscan function

Requirements for using this function:

- Creating a scanmode set (see page 178 ff.)
- Assigning a scanmode set to a user account (see page 178 ff.)

Configuring the scantime of the Autoscan function

By default, a computer module is accessed for 10 seconds before the connection is disconnected and the next computer module is accessed.

Select a time span between 1 and 99 seconds to define how long you want to switch to a computer module.

How to change the scantime:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tab Matrix systems and then go to Personal Profile.
- 4. In the **Scantime (1-99 seconds)** field, enter a time span between **1** and **99** seconds.
- 5. Click on Save.

Auto scanning all active computer modules (Autoskip)

The *Autoskip* function successively switches to computer modules that are included in the active scancode set and available to users.

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

The *Scantime* setting (see page 175) enables you to define how long each computer module is to be accessed.

When accessing the computer modules, the console module name, the name of the currently accessed computer 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 computer module.

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

Applying the Autoskip function

Requirements for using this function:

- Creating a scanmode set (see page 178 ff.)
- Assigning a scanmode set to a user account (see page 178 ff.)

Configuring the scantime of the Autoskip function

By default, a computer module is accessed for 10 seconds before the connection is disconnected and the next computer module is accessed.

Select a time span between 1 and 99 seconds to define how long you want to switch to a computer module.

How to change the scantime:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the Matrix systems tab and then go to Personal Profile.
- 4. In the **Scantime (1-99 seconds)** field, enter a time span between **1** and **99** seconds.
- 5. Click on Save.

Scanning computer modules manually (Stepscan)

By pressing a key, the *Stepscan* function successively switches to all computer modules that are included in the scan mode set and available to users.

When accessing the computer modules, the console module name, the name of the currently accessed computer 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 178 ff.)
- Assigning a scanmode set to a user account (see page 178 ff.)
- Configuring keys to scan the targets manually (see page 178 ff.)

Configuring keys for manually scan

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

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

How to select keys for using the Stepscan function:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the KVM matrix systems tab and then go to Personal Profile.
- 4. In the **Step keys** field, you can select between the following options:

Up/Down:	Arrow keys Up and Down
PgUp/PgDn:	Page t and page t keys
Num Up/Down:	Arrow keys Up and Down of the numeric keypad
Num PgUp/PgDn:	Page <i>t</i> and page <i>t</i> keys of the numeric keypad
Num +/-	Plus and minus keys of the numeric keypad

Administrating scan mode sets

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

Scan mode sets allow you to define the computer modules to be accessed when executing the *Autoscan*, *Autoskip* or *Stepscan* function.

NOTE: Global scan mode sets are available for all users of the KVM matrix system.

You can administrate scan mode sets comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Scan mode sets**. Click on **Configuration** to start the wizard.

The following paragraphs briefly summarise the wizard's configuration options.

Step 1: Select a user

 Select a user account for which the configured scan mode keys will be available. When selecting the entry **Available for all (global)**, you create a global scan mode set that will be available for all users.

Step 2: Scan mode sets

- Select the scan mode set you want to configure.
 Click on the buttons Add, Edit or Delete to add a new scan mode set or to edit or delete an existing set.
- Click on the slider Activate scan mode set for current user if you want to activate the set for the user selected in step 2.

IMPORTANT: If you have selected the table entry **Available for all (global)** in step 2, clicking on the slider activates the set for all users.

NOTE: Only by assigning a scan mode set to a user account, the computer modules defined in the set are considered when executing the *Autoscan*, *Autoskip* or *Stepscan* function.

Step 3: Configure scan mode set

 Click on the slider Add device of all computer modules you want to include in the automatic switching process.

NOTE: Enable the option **Add device** in the column header to add all computer modules to a set.

Configuring the on-screen display

The on-screen display (OSD) of the KVM matrix system enables the user to operate and configure the system. By default, the OSD is provided on all console modules.

Configuration

Most basic functions and features of the OSD can be adjusted to your demands.

You can define a hotkey to open the OSD as well as the position and font size of the OSD.

Any adjustable settings are described on the following pages.

Changing the hotkey to open the OSD

The hotkey to open the OSD is used on the console modules connected to the KVM matrix system. This hotkey enables you to open the OSD in order to operate and configure the system.

NOTE: The hotkey modifier Ctrl and the hotkey Num are the *default* settings.

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 open the OSD:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Select at least one of the modifiers listed under Hotkey modifier:

Ctrl

- Alt
- Alt Gr
- Win
- Shift
- 4. In the **Hotkey** field, select one of the following options:

Pause	Pause key
Insert	Insert key
Delete	Delete keye
Home	<i>Home</i> key
PgUp	Page up key
PgDown	Page down key
Num	Num key
End	End key
Space	Space key

Opening the OSD via double keypress

Instead of opening the OSD with a hotkey, you can define a key to press twice to open the OSD.

How to define the key to open the OSD via double keypress:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Select one of the following options under **OSD via double keypress**:

Off:	Open OSD via double keypress disabled (default)
Ctrl:	Open OSD via double keypress of Ctrl key
Alt:	Open OSD via double keypress of Alt key
Alt Gr:	Open OSD via double keypress of Alt Gr key
Win:	Open OSD via double keypress of Win key
Shift:	Open OSD via double keypress of Shift key
Print:	Open OSD via double keypress of Print key
Cursor-Left:	Open OSD via double keypress of Cursor-Left key
Cursor-Right:	Open OSD via double keypress of Cursor-Right key
Cursor-Up:	Open OSD via double keypress of Cursor-Up key
Cursor-Down:	Open OSD via double keypress of Cursor-Down key

Automatic closing of the OSD after inactivity

If desired, you can set the OSD to close automatically after a period of inactivity.

Define this period by entering a value between 5 and 99 seconds.

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

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

- 1. In the menu, click on User.
- 2. Click on the user account you want to edit and then click on Configuration.
- 3. Click on the tab KVM matrix systems and then go to Personal Profile.
- 4. In the **Timeout of OSD sessions (5-99 seconds)** field, you can define a time span between **5** and **99** seconds.
- 5. Click on Save.

Adjusting the OSD transparency

In the default settings, the screen content under the OSD is semi-visible. The screen content shines through the part that is covered by the OSD.

You can either adjust or turn off the OSD transparency in the personal profile of a user.

How to adjust the OSD transperency:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to edit and then click on Configuration.
- 3. Click on the tab KVM matrix systems and then go to Personal Profile.
- 4. In the **OSD transparency** field, you can select between the following options:

High:	Screen content almost completely visible
Average:	Screen content semi-visible (default)
Low:	Screen content slightly visible
Off:	Screen content is covered

Adjusting the information display

NOTE: You can set the information display separately for computer modules with view rights and all other computer modules.

When switching to a computer module, a temporary information display (5 seconds) opens. The display informs you about the console name, the name of the currently accessed computer 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 general settings of the information display:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to edit and then click on Configuration.
- 3. Click on the tab KVM matrix systems and then go to Personal Profile.
- 4. In the Show OSD info field, you can select between the following options:

5 seconds:	Temporary information display
Perm:	Permanent information display
Off:	Deactivate information display

5. Click on Save.

How to change the general settings of the information display for computer modules with view right:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to edit and then click on **Configuration**.
- 3. Click on the tab KVM matrix systems and then go to Personal Profile.

4. In the **Show OSD info for computer modules with view rights** field, you can select between the following options:

Use regular OSD info:	Using the general setting of the information display (see above)
5 seconds:	Temporary information display
Perm:	Permanent information display
Off:	Deactivate information display

5. Click on Save.

Changing the colour of the information display

By default, information displays (like when accessing a computer module) are shown in light green. In their personal profiles, users can change the colour of the information display.

The following colours are supported:

black	dark red
green	dark yellow
dark blue	purple
dark turquoise	silver
light green	yellow
blue	fuchsia
light turquoise	white

How to change the colour of the information display:

- 1. In the menu, click on User.
- 2. Click on the user account you want to edit and then click on Configuration.
- 3. Click on the tab KVM matrix systems and then go to Personal Profile.
- 4. In the Colour of OSD info field, you can select the desired colour.
- 5. Click on Save.

Defining a default view filter

After the user login, the *Select* menu is displayed. The default setting of the *Select* menu displays all computer modules. By applying a view filter, you can filter the computer modules to be displayed.

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

NOTE: The default view filter is applied directly after you log in on the matrix system.

By applying this view filter, you can change the default and therefore activate another filter.

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

- 1. In the menu, click on Advanced features.
- 2. Click on a view filter and then click on Configuration.
- 3. In step 1, select the desired view filter and click on Save and continue.
- 4. In **step 2**, select the computer modules you want to include in the view filter and click on **Save and continue**.
- 5. In **step 3**, select the users who should use this view filter as default and click on **Save and continue**.

Selecting a keyboard layout for OSD entries

If the characters entered on 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 console keyboard:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on Configuration
- 3. Click on the **General** tab.
- 4. In the Keyboard layout field, you can select one of the following options:

 German 	
 English (US) 	
 English (UK) 	
 French 	
 Spanish 	
 Latin American 	
 Portuguese 	
 Swedish 	
 Swiss-French 	
 Danish 	

Operating the OSD by mouse

In the default settings of the KVM matrix system, the OSD can only be opened with a configured key combination.

If a Microsoft »IntelliMouse Explorer« or another compatible mouse with five keys is connected to the console module, you can open the OSD with mouse keys four and five on the side of the mouse.

How to enable/disable mouse support to operate the OSD:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. In the **OSD by Mouse** field in the paragraph *OSD configuration*, select one of the following options:

On:	Open OSD with mouse key 4 and 5 of a compatible mouse.
Off:	Disable the possibility to open the OSD by mouse.

4. Click on Save.

Enabling/disabling the OSD

This function defines if users of a console module can activate the OSD or if they can use only select keys to switch between channels.

How to (de)activate the OSD:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Under **OSD blocked** in the paragraph *OSD configuration*, select one of the following options:

No:	OSD and displaying of info messages available
OSD menu:	OSD blocked; displaying of info messages available
OSD menu + OSD info:	OSD and displaying of info messages blocked.

Adjusting the OSD resolution

In the defaults of the matrix switch the OSD is displayed on the console monitor in a resolution of 1024×768 pixels if the monitor does support this resolution. If the monitor does not support this resolution, a resolution of 640×480 pixels is used.

You can also set the OSD resolution for the entire system (see table below). Adjusting the resolution for the entire system includes all console modules. However, you can also individually set the OSD resolution for each console module.

How to adjust the OSD resolution of the entire system:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix you want to configure and then click on **Configuration**.
- 3. In the **OSD resolution** field, select one of the following options:

Auto:	If supported by the monitor, the OSD is displayed in a resolution of 1024×768 pixels.
	If the monitor does not support this resolution, a resolution of 640×480 pixels is used. (<i>default</i>).
640×480:	OSD is displayed in a resolution of 640×480 pixels
720×400:	OSD is displayed in a resolution of 720×400 pixels
1024×768:	OSD is displayed in a resolution of 1024×768 pixels

How to adjust the OSD resolution of a particular console module:

- 1. In the menu, click on Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. In the **OSD resolution** field of the paragraph *OSD configuration*, select one of the following options:

System:	Use system-wide (see above) setting (default).
Auto:	If supported by the monitor, the OSD is displayed in a resolution of 1024×768 pixels.
	If the monitor does not support this resolution, a resolution of 640×480 pixels is used. (<i>default</i>).
640×480:	OSD is displayed in a resolution of 640×480 pixels
720×400:	OSD is displayed in a resolution of 720×400 pixels
1024×768:	OSD is displayed in a resolution of 1024×768 pixels

Expanding switchable signals

You can expand the switchable signals of a computer or a console through *channel* grouping

EXAMPLE: To transmit a second video signal and a USB 2.0 signal of the same computer, in addition to a first computer module, connect a second computer module (second video channel) and a **U2-LAN-04-CPU** module (USB2.0) to the computer.

In addition to the first console module, connect a second console module (second video channel) and a **U2-LAN-04-CON** module (USB2.0) to the console the aforementioned computer is accessing.

With the *Vision IP series*, you can switch various computer modules of *one* computer or various console modules of *one* console at the same time.

NOTE: Only in this mode, you can hold the USB signal using the OSD **Operation** menu at the currently active computer. If you switch to another computer after executing the *hold function*, the USB signal remains on the computer that you accessed first.

After disabling the *hold function* on the **Operation** menu, the USB signal switches to the currently active computer.

Expanding the system through channel grouping

The web application lets you assign up to seven additional video channels and one USB 2.0 channel to the KVM channel of the console.

You can also assign up to seven additional video channels to the KVM channel of the computer. In addition, you can create **pools** of four devices for the USB 2.0.

NOTE: Within the channel groups of the console a USB 2.0 channel represents one single device. For computers such a channel represents a group of up to four devices.

By using pools, you can grant up to four users the right to access the USB 2.0 channel *at the same time*. For this, the matrix switch selects an available device from the pool after switching.

Assigning multiple channels to a console or computer creates a *channel group*.

NOTE: The OSD does *not* show any console or computer modules that you added as additional channels to the channel group.

Creating a new channel group

How to create a new channel group:

- 1. In the menu, click on Matrix systems > [Name] > Console modules or Computer modules.
- 2. Click on a console or a computer module that is not assigned to a *channel group*.
- 3. Click on Channel grouping.

The selected module is assigned to the first KVM channel and is shown in the **Device group** column. The right column (**Unassigned**) lists the matrix switch modules you can add to the new channel group.

NOTE: You can assign up to seven additional video channels and one USB channel to a console's KVM channel.

You can assign up to seven additional video channels to the KVM channel of the computer, too. In addition, you can create a **pool** of four devices for the USB 2.0 channel.

NOTE: All channels of a channel group are switched at the same time.

4. In the right column (**Unassigned**), click on the module you want to add. In the left column (**Device group**), click on the channel you want to add the module to.

NOTE: To change the order of already added channels, mark a channel and click on <u>▲</u> (*arrow down*) or <u>▲</u> (*arrow up*). The chosen channel is moved up or down.

- 5. Click on < (*arrow left*) to assign the module to the chosen channel.
- 6. Repeat steps 4 and 5 to add another module to the *channel group*.
- 7. Click on Save.

Adding or deleting modules from a channel group

How to add modules to or delete them from a channel group:

- 1. In the menu, click on Matrix systems > [Name] > Console modules or Computer modules.
- 2. Click on a console module or a computer module that is already assigned to the channel group to which you want to add another module or from which you want to delete a module.
- 3. Click on Channel grouping.

Now you can see the current configuration. The right column (**Not assigned**) lists the matrix switch modules you can add to the channel group.

NOTE: You can assign up to seven additional video channels and one USB channel to a console's KVM channel.

You can assign up to seven additional video channels to the KVM channel of the computer, too. In addition, you can create a **pool** of four devices for the USB 2.0 channel.

4. Add more modules to or delete them from the *channel group*:

Adding modules:	 In the right column (Unassigned), click on the module you want to add. In the left column (Device group), click on the channel to which you want to add the module. Click on (arrow left) to assign the module to the selected channel.
Deleting modules:	 In the right column (Assigned), click on the module you want to delete from the <i>channel group</i>. Click on (arrow right) to delete the module's assignment.

Deleting a channel group

How to delete a multichannel configuration:

- 1. In the menu, click on Matrix systems > [Name] > Console modules or Computer modules.
- 2. Click on a console module or a computer module already assigned to the *channel group* you want to delete.
- 3. Click on **Channel group** to see the current configuration.

NOTE: The web application deletes a channel group if it does not contain any other channels than KVM channel 1.

4. In the left column (**Device group**), click on a module that is assigned to one of the 2 to 8 channels or to the USB channel.

Click on
(arrow right) to delete the module's assignment.

- 5. Repeat step 4 to delete the assignment of other modules.
- 6. As soon as only one module is assigned to KVM channel 1, click on Save.

The channel group is deleted.

Advanced functions of the KVM matrix switch

Copying the config settings of a matrix switch

You can copy the **General**, **KVM connection**, **Monitoring** and/or **Tradeswitch/CDS** configuration settings of one matrix switch to the settings of one or more other matrix switches.

NOTE: The name and the comment of a matrix switch are not copied.

How to copy matrix switch config settings:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch whose configuration you want to copy.
- 3. Open the menu Service tools and select the entry Copy configuration.
- 4. In the upper area, select which tabs (General, KVM connection, Monitoring and/or Tradeswitch/CDS) of the matrix switch should be copied.
- 5. In the lower area select the matrix switch(es) to which you want to copy the data.
- 6. Click on Copy configuration.

Restoring the connection status after a restart

If you enable the function to **Restore connection state**, after every restart the matrix switch automatically logs in the last active users at the console modules. Then the connection to the last accessing computer modules are automatically restored.

NOTE: The original access order is *not* considered when restoring the connection state. This can result in restrictions when using the multi-user mode.

How to enable or disable the restore of connection states:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch you want to configure and then click on Configuration.
- 3. Select one of the options under **Restore connection state**:

On:	After you restart the matrix switch, the last connection states are restored.
Off:	After you restart the matrix switch, the login box is displayed at all console modules (<i>default</i>).

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 menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch you want to restart.
- 3. Click on Service tools and select the entry Restart.
- 4. Confirm the confirmation prompt by clicking on Yes.

Restoring the connection state after a restart

If you enable the function to **Restore connection state**, after every restart the matrix switch automatically logs in the last active users at the console modules. Then the connection to the last accessing computer modules are automatically restored.

NOTE: The original access order is *not* considered when restoring the connection state. This can result in restrictions when using the multi-user mode.

How to enable or disable the restore of connection states:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch you want to configure and then click on Configuration.
- 3. Select one of the options given under **Restore connection state**:

Off:	After you restart the matrix displayed at all console mod	switch, the login box is dules (<i>default</i>).
On:	After you restart the ma connection states are restored	atrix switch, the last d.

Copying config settings to a new 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 configuration settings of matrix switches:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the new device.
- 3. Click on Service tools and select the entry Replace device.
- 4. Select the device whose configuration settings you want to copy.
- 5. Click on Save.

Freeze mode

When the cable connection between the computer module and the console module is lost during operation, the console monitor no longer show an image in the default settings of the KVM matrix system.

Enable the freeze mode if you want to display the last image received at the console module before the loss of connection. This image is displayed until the connection is re-established.

ADVICE: To emphasize the lost connection, the image last received is either highlighted by a coloured frame and/or the note **Frozen** and the time past since the loss of connection.

You can set the freeze mode for the entire system, too. The setting for the entire system applies to all console modules. In addition, you can set the freeze mode individually for each console module.

How to configure the freeze mode for the entire system:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch you want to configure and then click on Configuration.
- 3. Select one of the options given under Freeze mode:

Off:	Display no image on disconnection (default).
On OSD timer + frame:	Show a coloured frame in case of a disconnection and the message <i>Frozen</i> and the time past since the loss of connection.
On OSD timer:	Show the message <i>Frozen</i> and the time past since the loss of connection.
On Frame:	Show coloured frame in case of a disconnection.

How to configure the freeze mode individually for a console module:

- 1. In the directory tree, click on Matrix systems > [Name] > Console modules.
- 2. Select a console module and then click on **Configuration**.
- 3. Select one of the options given under **Freeze mode**:

System:	Apply setting (see above) to the entire system (<i>default</i>).
Off:	Display no image on disconnection.
On OSD timer + frame:	Show a coloured frame in case of a disconnection and the message <i>Frozen</i> and the time past since the loss of connection.
On OSD timer:	Show the message <i>Frozen</i> and the time past since the loss of connection.
On Frame:	Show coloured frame in case of a disconnection.

Changing push event key modifiers and valid keymodes

NOTE: This function is available only after activating the additional **IP-Control-API** function.

Push event keys let users at console modules trigger push events via XML control.

The triggered push event contains the following information:

- String entered by a user,
- Console modulename and device ID,
- Name and device ID of the computer module switched to the console module.

You can trigger a push event by pushing and holding the push event key modifier and entering a valid string (see entry **Valid push event keys)**.

How to change push event key modifiers or the valid keymode:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Select the matrix switch and then click on Configuration.
- 3. Under **Configuration**, go to **Push event key modifier** and select *at least* one modifier key by ticking the control box:

- Ctrl	• Win
- Alt	- Shift
- Alt Gr	

4. In the Valid push event keys field, select one of the following options:

Only numbers:	<i>Only numerical keys</i> are forwarded as part of a push event when pressing the push event key modifier
Only characters:	<i>Only alphabetic keys</i> are forwarded as part of a push event when pressing the push event key modifier
Numbers and characters:	<i>Numerical and alphabetical keys</i> are forwarded as part of a push event when pressing the push event key modifier

IMPORTANT: The computer's operating system and its application programs are not able to use the selected keymode as hotkey when it is combined with the selected push event key modifier(s),.

5. Click on Save.

Rights administration

Right to change the personal profile

How to change the right to change the personal profile:

- 1. In the menu, click on User or User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab KVM matrix systems and then go to Global device rights.
- 4. In the Edit personal profile field, you can select one of the following options:

Yes:	Allow users to view and edit own user profile
No:	Deny users to view and edit own user profile
Optional functions

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

Name	Function	Description
Push-Get function	The Push-Get function allows the user to push the image on his monitor to the display of another workplace or a large-screen projection or to get it from there.	page 211
IP-Control-API	The IP-Control-API enables text-based XML control of a KVM matrix system over the net- work. It offers developers/administrators the ability to create custom applications for control, send switching commands and retrieve selective information on switching states and computer status. Thanks to easy integration into existing systems, including those from third-party manufacturers, the API offers a flexible and expandable solution that goes beyond the standard functions of the KVM matrix system and enables seamless integration into IT infrastructures from various providers.	page 215
Scripting function	With the scripting function, as part of the IP Control API, you can create, manage and execute scripts. A script is an XML document that contains one or more commands that are executed by the matrix switch. This allows you to automate scenarios such as changing the switching status of individual workplaces, several workplaces or the entire system. HTTP requests can also be used to control external devices.	page 217
EasyControl tool	You can use the EasyControl tool integrated in the web application to connect a console module to a specific computer module or to execute an existing script or script group.	page 278

Name	Function	Description
Tradeswitch function	The TradeSwitch-Function (TS function) optimizes the operation of workplaces that, through multiple console modules, are responsi- ble for the simultaneous monitoring or control of multiple computers. Instead of assigning a separate keyboard and mouse to each console module, the TradeSwitch-Function provides a central keyboard and mouse for controlling the entire workplace. The user can switch these two input devices to	page 230
	any console module using a hotkey.	
CrossDisplay- Switching function	With CrossDisplay-Switching (CDS) as part of the TradeSwitch function, user-friendly switch- ing via mouse movement is enabled. The mouse behaves as if on a "virtual desktop" and can be seamlessly moved across the connected moni- tors. When the mouse pointer moves from one monitor to another, the keyboard-mouse focus is automatically redirected to another module, thus switching to a different computer.	page 236
FreeSeating function	With the FreeSeating function, as part of the TS-Function, the user's personal work environment is automatically restored at any workplace within the group – including the last connected sources. The simplified login process optimizes workflows and increases productivity: The login credentials only need to be entered once to log into all console modules of the group and switch to the most recently used sources. Similarly, a single logout is sufficient to log out the entire group.	page 137
MatrixGuard function	The MatrixGuard function allows any matrix switch within the MatrixGuard system to take over the role of the database leader if the origi- nal database leader fails or becomes inaccessi- ble. This transition is performed automatically according to predefined rules. The participants in the MatrixGuard connect to the new leader, and the system resumes operation automati- cally. The full operation of the remaining com- ponents is ensured. Manual intervention is not required.	page 263

Name	Function	Description
Direct Redundancy Shield function	With the DirectRedundancyShield (DRS) the KVM installation can be protected by implementing a redundant KVM-over-IP matrix system that takes over instantly if the first system fails or cannot be accessed. Once the DRS function has been configured, each console module and each computer module establishes two permanent connections to the active and the passive KVM-over-IP matrix via the network, only using one transmission line. If the primary connection is broken, the previously passive connection takes over auto- matically and directly. The transition is seam- less, without any delay in the image transmission.	page 272
2-factor authentication	To provide a greater level of security, optional two-factor authentication (2FA) can be used to query a second factor based on a device in the user's possession. 2FA makes use of a time-based one-time pass- word (TOTP). Authenticator apps or hardware tokens can be used.	page 50
Supported devices	In the standard scope of delivery, the IP matrix switch supports a maximum of 20 end devices. The number of devices can be increased by pur- chasing a feature key.	page 93

Name	Function	Description
SecureCert Feature	Feature to implement certified security functions. The following certifications are taken into account:	
	 Common Criteria EAL2+ DoDIN APL as <i>Video Distribution System over IP</i> FIPS 140-3 	
	IMPORTANT: This feature is only available with the order of new devices. After sales implementation is not possible!	
	The <i>SecureCert feature</i> can be ordered with the following devices:	
	• Devices of the <i>ControlCenter-IP</i> series from firmware 1.6.0	
	• Devices of the <i>ControlCenter-IP-XS</i> series from firmware 1.1.0	
	• Devices of the <i>VisionXS-IP</i> series from firmware 1.4.0	
	 Devices of the <i>Vision-IP</i> series from firmware 2.4.0 	
	• Devices of the <i>RemoteAccess-IP-CPU</i> series from firmware 1.3.0	
	an display the activated functions in the respective	a avaruian tabla

ADVICE: You can display the activated functions in the respective overview table. For this, add the Active features column (see *Configuring table columns* on page 10 ff.).

Viewing the status information of matrix switches

The context menu of matrix switches 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 matrix switches:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on Configuration.
- 3. Click on the tab **Information**.
- 4. The following information are displayed. Depending on the configuration, you see further information here, e.g. the cascade mode.

Name:	Matrix switch name
Device ID:	Physical ID of the matrix switch
Status:	Current status (Online or Offline) of the matrix switch
Class:	Device class
Firmware name:	Firmware name
Firmware rev:	Firmware version
Hardware rev.:	Hardware revision
IP Address A:	IP address of network interface A
IP Address B:	IP address of network interface B
IP Address Transmission:	IP address of the Transmission interface
KVM ports:	Number of console ports on the matrix switch
MAC A:	MAC address of network interface A
MAC B:	MAC address of network interface B
Serial number:	Serial number of the matrix switch

NOTE: In addition, *Active features*, the *Link status*, and the *Monitoring* information of the device are displayed.

5. Click on Close.

Push-get function (optional)

IMPORTANT: Using the Push-get function requires the purchase and activation of the premium **Push-get Function**.

The optional *Push-Get function* allows the user to push the switch state of his console module to another console module or to get it from there.

Changing the right to execute 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. In the menu, click on User or User groups.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab Matrix systems and go to Individual rights.
- 4. Select the desired console module on the left side of the list field of the paragraph **Individual console rights**.

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

5. In the **Push-Get** field on the right side, you can select between the following options:

Yes: Allow use of *Push-get* function

No: Deny use of *Push-get* function

Changing push-get key modifiers and valid keys

Push-get keys let you push orget the switch state from or to a console module by using key combinations. For this, you can create *Push-get key sets* in the matrix system.

In combination with a defined push-get key modifier a push-get key set defines the key combination to be pressed for push or get switch states.

In addition to the push-get key modifier you can also define valid keys to be used as push-get keys.

How to change push-get key modifiers or valid keys:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Select at least one of the listed modifiers under **Push get key modifier** by marking the respective entry:

- Ctrl	- Win
- Alt	Shift
• Alt Gr	

4. Under Valid push-get keys, you can select one of the following options:

Only numbers:	<i>Only numerical keys</i> are interpreted as push-get keys when pressed in combination with the push get key modifier
Only characters:	<i>Only alphabetic keys</i> are interpreted as push-get keys when pressed in combination with the push get key modifier
Numbers and characters:	<i>Aphabetical and numerical keys</i> are interpreted as push-get keys when pressed in combination with the push get key modifier

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

Administrating push-get key sets

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

Within push-get key sets you can define push-get keys for selected console modules to push/get the switch state of a console module.

NOTE: Global push-get key sets are available for all users of the KVM matrix system.

You can administrate push-get key sets comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Push-get keys**. Click on **Configuration** to start the wizard.

The following paragraphs briefly summarise the wizard's configuration options.

Step 1: Select a matrix switch

• Select a matrix switch on which you want to store the configuration of the pushget keys.

NOTE: After you selected a matrix switch, you will see the current configuration of the **Push-get key modifier** and the **valid push-get keys** (see above). If required, you can change these settings directly in this menu.

Step 2: Select a user

Select a user account for which the configured push-get keys are available.
 When selecting the entry Available for all (global), you create a global push-get key set that will be available for all users.

Step 3: Select push-get key set

- Select the push-get key set you want to configure.
 Click on the buttons Add, Edit or Delete to add a new select key set or to edit or delete an existing set.
- Click on the slider Activate push-get key for current user if you want to activate the set for the user selected in step 2.

IMPORTANT: If you have selected the table entry **Available for all (global)** in step 2, click on the slider to activate the set for all users.

NOTE: Only when a push get-key set is assigned to a user account, the push get-keys defined in the set are evaluated when entries are made at the workplace.

Step 4: Configure push-get key set

• Enter the desired key combinations for the console modules.

IP-Control-API (optional)

IMPORTANT: Using the IP-Control-API requires the purchase and activation of the premium function **IP-Control-API**.

After you activate the additional *IP-Control-API* function, you are able to access the KVM matrix system over a TCP/IP connection and you can use the network interfaces to send text-based commands in the form of XML files to the matrix switch.

NOTE: The structure of a valid XML document as well as possible commands and their syntax are desribed in the chapter *XML control of a matrix switch* in the separate *Configuration and Operation Guide*.

Supported functions via text-based control

You can use the text-based control to perform the following functions:

- Logon User: user logon at a console module
- Logout User: •user logout at a console module
- Connect CPU: Accesses computer module with a console module

NOTE: This function can only be executed if an user with the computer module access rights *ViewOnly* or *FullAccess* is logged on to the console module or if it is an *OpenAccess* console with these rights.

- Disconnect CPU: disconnects active access
- List Connections: queries connections between connected devices
- List MatrixSwitches: •queries known matrix switches
- List CPUs: •queries known computer modules
- List Consoles: queries known console modules
- Redirection: •redirects keyboard and mouse data

NOTE: Only after you have purchased the additional *Tradeswitch* function (see page 230 ff.), you are enabled to forward keyboard and mouse data to another console module or another computer module.

ADVICE: On request, our support will provide you with examples for API encryption in the programming languages C# and C++.

Configuring access 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 menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the device you want to configure and then click on Configuration.
- 3. Click on the tab Network and go to Remote Control.
- 4. To create a new access, click on Add remote control access. To adit an existing access, click on Edit.
- 5. Enter or edit the following data:

Port:	Enter the port you want to use for text-based communication.
	Ports 80, 443 and 27996 are not available for XML control.
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 or TLS to transmit the data entirely encrypted.
Key:	After enabling the encryption type CBC-3DES , enter the key (192 bit) in the form of 48 hex digits.
Initialization vector:	Enabling the encryption type CBC-3DES additionally requires an initialization vector. Enter the initialization vector (64 bit) in the form of 16 hex digits.
Certificate Authentication:	With TLS encryption <i>enabled</i> , you can additionally enable Certificate authentication after uploading a certificate (in the <i>Remote Control</i> section of the <i>Network</i> tab).

Scripting function (optional)

IMPORTANT: Using the scripting function requires the purchase and activation of the premium function **IP-Control-API**.

The scripting function lets you create, manage and execute scripts.

A script is an XML document that contains one or more commands carried out by the matrix switch.

EXEMPLARY SCRIPT TO ESTABLISH A CONNECTION

The structure of a valid XML document and any possible commands as well as their syntax are described in the chapter *XML control of the matrix switch* of the separate *Configuration and Operation Guide*.

ADVICE: Use the OSD of the matrix system to save the switching states of a console module/multiple console modules or of the entire system in a script (see chapter *Scripting function* of the separate *Configuration and Operation Guidel*).

The scripts stored in the matrix system can be executed via the OSD of the KVM matrix system.

Configuring scripts

You can configure the »Scripting« function comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Scripts and script groups**.

Step 1: Select the option »Scripts«

• Select the option **Scripts** to create, edit or merge individual scripts to control a device.

Steps 2 and 3: Create, edit, merge or delete scripts

NOTE: Script commands are stored in an XML document. Each XML document can contain one or more commands.

The structure of a valid XML document as well as possible commands and their syntax are described in the chapter *XML control of a matrix switch* in the separate *Configuration and Operation Guide*.

NOTE: For controlling external devices HTTP requests can be used.

EXAMPLE: With the following GET request, you can switch off outlet 4 of a connected ePower-Switch. The two line breaks at the end are important here so that the target device interprets the request correctly.

GET /hidden.htm?M0:04=0FF HTTP/1.1

IMPORTANT: Only users with assigned **Superuser** rights are able to create, edit and delete scripts in the web application.

How to create a new script:

- 1. Click on Add script.
- 2. Enter the following data into the dialogue box:

Name:	Enter the desired script name.
Enabled:	Enable or disable the execution <i>and</i> display of the script in the Script menu.
Execution delay:	After calling the script, you can delay its execution by up to 999 seconds. Enter the desired delay time in seconds.
Comment:	If desired, enter a comment about the script.
XML code:	Enter the XML code or HTTP request using script commands.

How to edit an existing script:

- 1. Select the script you want to edit and click on Edit.
- 2. Enter or update the following data into the dialogue box:

Name:	Enter the desired script name.
Enabled:	Enable or disable the execution <i>and</i> display of the script in the Script menu.
Execution delay:	After calling the script, you can delay its execution by up to 999 seconds. Enter the desired delay time in seconds.
Comment:	If desired, enter a comment about the script.
XML code:	Enter the XML code or HTTP request using script commands.

3. Click on Save.

How to delete an existing script:

- 1. Select the script you want to delete and click on **Delete**.
- 2. Confirm the security prompt by clicking on Yes.

How to merge existing scripts into a new script:

1. Select the existing scripts you want to merge.

ADVICE: Press the Ctrl key to select several scripts from the list.

- 2. Click on Merge.
- 3. Enter the following data:

Name:	Enter the desired script name.
Comment:	If desired, enter a comment about the script.

4. If desired, you can change the order of the scripts you want to merge. Mark a script and click on (*arrow up*) or (*arrow down*). The selected script is moved either up or down.

NOTE: The XML documents of the selected scripts are copied to a new script in the selected order. In the new script, you can edit the XML document (created from the individual scripts) as required.

5. Click on Save.

Step 4: Define owner

A script can be executed by users who are the *owner* of the script or are assigned with rights to execute the script.

NOTE: Only scripts without owners can be added to script groups.

• Activate the **Owner** slider in the line of the user to be entered as the owner of the script.

Step 5: Script availability

If a script is *not* assigned to a console module, it is shown on all console modules whose users are assigned with the right to execute the script.

If the script is assigned to one or several console modules, it is shown only at the *assigned* console module(s) if their users are assigned with the right to execute the script.

• Activate the **Available** slider in the row of the console modules on which to show the script.

NOTE: Use the **Available** option in the column header to move the sliders of all console modules.

NOTE: Use the slider in the **EasyControl** line to control the availability of the script in the **EasyControl** tool.

ADVICE: Do not activate any slider if you want the script to be available on all console modules.

Step 6: Target device

In the script configuration, you can specify whether the script is to be executed locally *or* on *another* matrix switch or device.

NOTE: Prerequisite for the execution on another matrix switch is that the additional **IP-Control-API** function is also activated on the target matrix switch.

- Enable the **Execute on this device** slider *or* enter the IP address and port of the other matrix switch or device.
- Activate the **lgnore device response** slider if the device response should not be evaluated.

Configuring script groups

You can configure the »Scripting« function comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Scripts and script groups**.

Step 1: Select the option »Scripts groups«

• Select the option **Scripts groups** to organise several existing scripts in a script group.

Steps 2 and 3: Create, edit or delete script groups

How to create a new script group:

- 1. Click on Add script group.
- 2. Enter the following data into the dialogue box:

Name:	Enter the desired name of the script group.
Enabled:	Enable or disable the execution <i>and</i> display of the script group in the script menu.
Execution delay:	After calling the script group, you can delay its execution by up to 999 seconds. Enter the desired delay time in seconds.
Comment:	If desired, enter a comment about the script group.

3. Click on Save.

How to edit an existing script group:

- 1. Select the script group you want to edit and click on Edit.
- 2. Enter or update the following data into the dialogue box:

Name:	Enter the desired name of the script group.	
Enabled:	Enable or disable the execution <i>and</i> display of the script group in the script menu.	
Execution delay:	After calling the script group, you can delay its execution by up to 999 seconds. Enter the desired delay time in seconds.	
Comment:	If desired, enter a comment about the script group.	

How to delete an existing script group:

- 1. Select the script group you want to delete and click on Delete.
- 2. Confirm the security prompt by clicking on Yes.

Step 4: Add scripts to group or delete them from group

The dialog lists all scripts of the matrix switch to which no owner has been assigned.

- Click on the Add slider on the row of the scripts you want to add to the group.
- Disable the **Add** slider on the row of the scripts you want to delete from the group.

NOTE: Use the Add option in the column header to move the sliders of all scripts.

Step 5: Define order of script execution

■ If desired, you can change the order of the scripts within a group. Mark a script and click on (arrow up) or (arrow down). The selected script is moved either up or down.

Step 6: Script group availability

• Click on the **Available** slider in the row of the console modules on which to show the script group.

NOTE: Use the **Available** option in the column header to move the sliders of all console modules.

ADVICE: Do not activate any slider if you want the script to be available on all console modules.

Assigning rights to execute scripts and script groups

NOTE: Users always have the right to execute and delete their own scripts (**Owner**). This option does not require any additional rights.

Executing a script that is not assigned to your own user account requires the right to execute this script. The same applies for script groups.

The **right to execute scripts** can be assigned in the settings of a user account. You can also manage this right via user groups (see *Efficient rights administration* on page 68).

Defining the right to execute a script

How to change the right to execute a particular script:

- 1. In the men, click on **User** or on **User groups**.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab KVM matrix systems and then go to Scripting rights.
- 4. In the list field of the **Scripting rights** paragraph, select the desired script from the list on the left-hand side.

ADVICE: If necessary, use the *Search* box to limit the scripts that appear in the selection window.

5. In the **Execution** field on the right-hand side, select one of the following options:

Activated:	Allow the execution of the script.
Deactivated:	Deny the execution of the script.

Defining the right to execute a script group

How to change the right to execute a particular script group:

- 1. In the men, click on **User** or on **User groups**.
- 2. Click on the user account or the user group you want to configure and then click on **Configuration**.
- 3. Click on the tab KVM matrix systems and then go to Scripting group rights.
- 4. In the list field of the **Scripting group rights** paragraph, select the desired script group from the list on the left-hand side.

ADVICE: If necessary, use the *Search* box to limit the script groups that appear in the selection window.

- 5. Select the desired script group from the list on the left-hand side.
- 6. Under Execution, select one of the following options:

Activated:	Allows the execution of the script group.
Deactivated:	Denies the execution of the script group.

Assigning and configuring script keys

After the script key modifier(s) and a script key set have been adjusted and a script key set has been activated in the user account, a script can be executed by pressing key combinations on the console module keyboard.

Using script keys at a console module

Opening the OSD is not necessary for using script keys to execute scripts. Hence, scripts can be executed much faster if you know the script keys required for the execution.

How to use script keys to execute a script:

1. Press the script key modifier key(s) defined in the matrix system and the script key assigned to the script.

EXAMPLE:

- Script key modifier keys:Win+Shift
- Script key for script: 1

Press and hold the keys Win+Shift while pressing script key 1. The scrip is executed when releasing the keys.

Changing the script key modifier and the valid keys

Script keys let you execute scripts quickly with the help of hotkeys. For this, you can create *script key sets* in the matrix system.

Together with a defined script key modifier, a script key set defines the hotkey to be pressed to execute a script.

In addition to defining the script key modifier, you can also define keys to be used as script keys.

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

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Select at least one of the modifiers listed in the **Script key modifier** field by marking the respective entry:

- Ctrl	- Win
- Alt	 Shift
Alt Gr	

4. In the Valid keys field, select one of the following options:

Only numbers:	<i>only numerical keys</i> are interpreted as script keys when pressed in combination with the script key modifier
Only characters:	<i>only alphabetic keys</i> are interpreted as script keys when pressed in combination with the script key modifier
Numbers and characters:	<i>alphabetical and numerical keys</i> are interpreted as script keys when pressed in combination with the script key modi- fier

IMPORTANT: The selected valid keys and the script key modifier(s) are *no longer* provided as key combinations to the operating system and the applications installed on the computer.

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

Administrating script key sets

The KVM matrix system lets you create 20 global script key sets or ten additional, individual script key sets for each user.

Within script key sets you can define individual script keys to execute individual scrips.

```
NOTE: Global script key sets are available to all users of the KVM matrix system.
```

You can administrate script key sets comfortably with a wizard. Click on the menu Advanced features and select the entry Script keys. Click on Configure to start the wizard.

The following paragraphs briefly summarise the wizard's configuration options.

Step 1: Select a device

• Select the matrix switch on which you want to store the configuration of the script key set.

NOTE: After you selected a matrix switch, you will see the current configuration of the **script key modifier** and the **valid select keys** (see above). If required, you can change these settings directly in this menu.

Step 2: Select a user

• Select a user account for which the configured script keys are available. When selecting the entry **Available for all (global)**, you create a global script key set that will be available to all users.

Step 3: Add or select script key sets

- Select the script key set you want to configure.
 Click on the buttons Add, Edit or Delete to add a new script key set or to edit or delete an existing set.
- Click on the slider **Activate script key set for current user** if you want to activate the set for the user selected in step 2.

IMPORTANT: If you have selected the table entry **Available for all (global)** in step 2, clicking on the slider activates the set for all users.

NOTE: Only by assigning a script key set to a user account, the script keys defined in the set are accepted as inputs and execute the assigned script.

Step 4: Assign scripts and edit script key sets

• Enter the desired key combinations to execute scripts or script groups.

OSD settings fo the Scripting function

Editing the default menu mode

In the defaults, after accessing the OSD at a console module, you can select a computer via the *Select* menu. If desired, you can use your personal profile to define that the *Script* menu is shown directly after you open the OSD.

ADVICE: Independent of the default setting, you can always use the hotkey Ctrl+X to switch between *Select* menu and *Script* menu.

How to edit the default menu mode:

- 1. In the menu, click on Users.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tabs KVM matrix systems and then go to Personal profile.

4. In the **Default OSD menu** field, select one of the following options:

Select:The Select menu is shown after you open the OSD.Script:The Script menu is shown after you open the OSD.

5. Click on Save.

Switching threshold to switch the menu mode by mouse

In addition to switching the menu mode via the hotkey Ctrl+X you can also use the mouse to switch between menu modes.

ADVICE: After the activation of the switching of the menu mode by mouse, you can move the mouse to the left or to the right to switch between the two modes in the *Select* menu and in the *Script* menu.

IMPORTANT: Switching the menu mode by mouse is *not* possible if the entry is not available in the *Select* menu or in the *Script* menu!

How to activate/deactivate the switching threshold and/or adjust its sensitivity:

- 1. In the menu, click on Users.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tabs KVM matrix systems and then go to Personal profile.
- 4. In the Select/script menu mouse switching field, select one of the following options:

Off:	Mouse switching of the OSD menu mode deactivated (<i>default</i>)
Sensitivity 1:	lowest sensitivity level for mouse switching of the OSD menu mode
Sensitivity 10:	maximum sensitivity level for mouse switching of the OSD menu mode
Sensitivity 2-8:	further sensitivity levels for mouse switching of the OSD menu mode

Tradeswitch function (optional)

IMPORTANT: Using the Tradeswitch function requires the purchase and activation of the premium **TS-Function**.

The Tradeswitch function optimises the operation of workplaces monitoring multiple computers over multiple modules.

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

In order to enable this, several console modules of a KVM matrix system are arranged into a group. Only one of the group's modules is provided with keyboard and mouse.

By using a hotkey, users are now able to switch the two input devices to the monitors of the other console modules. This makes it possible to operate the connected computer modules and computers.

Computer modules can also be integrated into the tradeswitch group and the keyboard and mouse signals can be switched directly to them. This makes it possible, for example, to operate a laptop that has its own monitor.

Changing tradeswitch key and valid key type

Tradeswitch keys allow you to switch the keyboard and mouse signals of a console module to another console module or computer module by entering a key combination.

You can group any console modules and/or computer modules into a workplace and individually define the keys to be pressed to switch the keyboard and mouse signals to a specific console module or computer module.

In addition to the tradeswitch key modifier, you can also define the valid key type for tradeswitch keys.

How to change tradeswitch key modifier or valid tradeswitch keys:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. In the **Tradeswitch key modifier** field, select *at least* one of the listed key modifiers by checking the respective box.

Ctrl		
 Alt 		
 Alt Gr 		
• Win		
Shift		

4. In the Valid tradeswitch keys field, select one of the following options:

Only numbers:	<i>Only numerical keys</i> are interpreted as tradeswitch keys when pressed in combination with the tradeswitch key modifier.	
Only characters:	<i>Only alphabetic keys</i> are interpreted as tradeswitch keys when pressed in combination with the tradeswitch key modifier.	
Numbers and characters:	<i>Alphabetical and numerical keys</i> are interpreted as tradeswitch keys when pressed in combination with the tradeswitch key modifier	
TMDODTANT. T	"he colocted transmede and tradeswitch transmedificat(a)	

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 computer.

Administrating tradeswitch workplaces

You can comfortably manage the tradeswitch workplaces with a wizard. Click on the **Advanced features** menu and select **Tradeswitch/FreeSeating/Cross-Display Switching**.

To start the wizard, click Configure.

The following sections briefly summarize the configuration options of the wizard.

Step 1: Select a matrix switch

• Select the matrix switch on which you want to store the configuration of the tradeswitch workplace.

NOTE: After you selected a matrix switch, you will see the current configuration of the »Tradeswitch« function and »CrossDisplay-Switching« (see above). If required, you can change these settings directly in this menu.

Step 2: Tradeswitch workplace

Select a tradeswitch workplace you want to configure.
 Click on Add, Edit or Delete to create a new tradeswitch workplace or edit or delete existing ones.

Step 3: Configure tradeswitch workplace

- Entering a key combination to switch the monitor adds a module to the tradeswitch workplace.
- Delete an already entered key combination to delete a module from the tradeswitch workplace.
- Click on the slider **Tradeswitch leader** in the row of the module whose keyboard and mouse are used to operate the tradeswitch workplace.
- Click on the slider **FreeSeating member** in the rows of the modules to be included when restoring the last FreeSeating session (see *Restore the last FreeSeating session* on page 137).

NOTE: Each console module of a tradeswitch workplace can be FreeSeating member. Console modules can be a FreeSeating member in several tradeswitch workplaces.

IMPORTANT: To use the FreeSeating function, at least the tradeswitch leader must be a FreeSeating member.

Step 4: Tradeswitch configuration completed

You can now use the configured key combinations to switch between monitors .

Advanced functions

Configure Tradeswitch visualization

If you purchased the *Tradeswitch function*, the messages *»Forwarding to…«* (on the Tradeswitch leader) or *»FORWARDED«* (on the target workplace) can be displayed at the monitor at a console module.

Additionally (or alternatively) you can activate a frame that permanently or temporarily marks the monitor of the module connected via tradeswitch function.

How to configure the Tradeswitch visualization for a console module:

- 1. In the menu, click on KVM Matrix systems > [Name] > Console modules.
- 2. Click on the console module you want to configure and then click on **Configuration**.
- 3. Click on the **General** tab.
- 4. Under Tradeswitch visualization, you can select between the following options:

No:	Disable Tradeswitch visualization
Yes OSD:	The message »Forwarding to« (at the Trade- switch leader) or »FORWARDED« (at the target workplace) is displayed on the screen.
Yes Frame temporary:	A frame temporarily marks the monitor of the module connected via tradeswitch function.
Yes Frame:	A frame permanently marks the monitor of the module connected via tradeswitch function.
Yes OSD+Frame temporary:	The message »Forwarding to« (at the Trade- switch leader) or »FORWARDED« (at the target workplace) is temporarily displayed on the screen.
	In addition, a frame temporarily marks the monitor of the module connected via tradeswitch function.
Yes OSD+Frame:	The message »Forwarding to« (at the Trade- switch leader) or »FORWARDED« (at the target workplace) is permanently displayed on the screen.
	In addition, a frame permanently marks the monitor of the module connected via tradeswitch function.

Customizing the appearance of the tradeswitch frame

You can set the display duration of the tradeswitch frame as well as its appearance (color settings, transparency effect and frame width) system-wide.

Each user of the matrix system can use his or her personal profile to change the system-wide default by making an individual adjustment.

How to change the *system-wide* appearance of the tradeswitch frame:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Customize the settings in the **Tradeswitch frame configuration** section to suit your needs:

Temporary display time:	Set the temporary display duration of the tradeswitch frame between 0.0 (off) and 10.0 seconds.	
Colour settings:	Select the brightness and colour of the tradeswitch frame.	
Transparency effect:	Select the transparency effect (normal or high) of the Tradeswitch frame.	
Frame width:	Select the frame width (normal to quadruple) of the Trade- switch frame.	

How to change the appearance of the tradeswitch frame for a *specific* user account:

- 1. In the menu, click on **User**.
- 2. Click on the user account you want to configure and then click on **Configuration**.
- 3. Click on the tabs KVM matrix systems and then go to Personal profile.
- 4. Enable the Personal tradeswitch frame display option.
- 5. Customize the settings in the **Tradeswitch frame configuration** section to suit your needs:

Temporary display time:	Set the temporary display duration of the tradeswitch frame between 0.0 (off) and 10.0 seconds.	
Colour settings:	Select the brightness and colour of the tradeswitch frame.	
Transparency effect:	Select the transparency effect (normal or high) of the Tradeswitch frame.	
Frame width:	Select the frame width (normal to quadruple) of the Trade- switch frame.	

CrossDisplay-Switching (optional)

IMPORTANT: Using the CrossDisplay-Switching function requires the purchase and activation of the premium **TS-Function** (see page 230 ff.).

With **CrossDisplay-Switching (CDS)**, you can use the mouse to switch between the modules of a Tradeswitch configuration (see page 230 ff.).

IMPORTANT: Depending on operating system and mouse driver, there might be some restrictions:

- Under *Mac OS*, the mouse might jitter at the edge of the screen.
- Under *Linux* there might be some problems when placing and moving the mouse.

NOTE: It is possible that mouse gestures used by some programs (like Firefox) to run functions cannot be applied.

Using »CrossDisplay-Switching«



Figure 1: Exemplary order of three monitors

How to use *CrossDisplay-Switching* to switch to another module:

Move the cursor to the edge of an active monitor placed next to another monitor.

The matrix switch switches to the module of the next monitor and positions the cursor. You will barely realize the switching between computers.

EXAMPLE: If you move the cursor to the right edge of **Monitor 2**, the matrix switch switches to the module connected to **Monitor 3**.

If you move the cursor to the left edge of **Monitor 2**, the matrix switch switches to the module connected to **Monitor 1**.

If you reach the outer edges (left edge of **Monitor 1** or right edge of **Monitor 3**) *CrossDisplay-Switching does not* take place.

If you hold a mouse key while moving the mouse, switching cannot be carried out. However, you can still drag and drop objects.

ADVICE: When using multi head groups, you can enable specific mouse modes that allow drag and drop operations when working with Windows and Linux operating systems (see page 259).

NOTE: You can define the monitor order in the web application (see page 259).

Requirements for »CrossDisplay-Switching«

Using CrossDisplay-Switching requires the following:

- Enabled premium **Tradeswitch** function (see page 230).
- Established and configured *Tradeswitch configuration* (see page 232).
- Enabled CrossDisplay-Switching (see page 243).
- Order of workplace monitors saved in the web application (see page 240).

IMPORTANT: Only USB computer modules connected to the computer by USB cables support *CrossDisplay-Switching*.

Order and proportions of monitors

Figure 1 shows three monitors placed in a row.

In addition to monitors placed next to each other, any combinations are supported. Even the monitors' proportions can vary. The following table shows some examples and describes special features.

NOTE: In the web application you can save the order and proportions of your monitors according to how they are placed on the desk.

12		In addition to switching to a monitor placed on the left or the right side of the active monitor, you can also switch to monitors placed above or below the active monitor:
3 4		Move the cursor to one of the edges between monitors 1 and 3 or 2 and 4 to switch from an upper monitor to a lower monitor (or vice versa).
		If the monitors are placed as shown on the left, it is important to mind the exact <i>vertical</i> cursor position when reaching the lower edge of Monitor 1 :
		• In the first third you can switch to monitor 2.
		• In the second third you can switch to monitor 3.
2	J 4	• In the last third you can switch to monitor 4.
1 3 4		If the monitors are placed as shown on the left, it is important to mind the exact <i>horizontal</i> cursor position when reaching the left or right edge of Monitor 3 :
2	5	• In the upper half you can switch to monitors 1 or 4.
		 In the lower half you can switch to monitors 2 or 5

Implementing multi-head monitors

NOTE: A description on how to create CDS multihead groups is given on page 253. For *CDS with multihead groups*, the individual channels are not managed, configured and switched as group, but individually in the KVM matrix system.

Matrix systems support computers whose desktop is displayed on multiple monitors (see page 191 ff.). These computers are called *multi-head computers*.

By default, the monitor of a multi-head computer is displayed in the standard monitor size. However, you can change the size (monitor 2 in the example below) to the proportions of the other monitors:



Figure 2: Two monitors of a multi-head computer between other monitors

NOTE: Install the driver **CrossDisplay-Switching - Multi-Monitor Support** if you cannot move the cursor across the two monitors of a multi-head computer.

You can download the driver from www.gdsys.com/en/start under More from G&D and Tools & Drivers.

The »CrossDisplay-Switching« view

In the web application, you can save the order and proportions of console monitors. Based on these information, the matrix switch switches to the desired monitor if you move the cursor to the edge of a monitor.

Search X	Raster on/off	
Name 🔺		
CON1		
CON2		
Add 🖈		< Remove
	•	-
	Position X: Y:	- Size X: Y: +
	•	+

Figure 3: The view »CrossDisplay-Switching«

The tab is divided into four parts. The following paragraphs provide detailed information about each part.

List of modules

The *left column* lists all console modules and computer modules that are assigned to the tradeswitch workplace and *not* yet placed in the workspace.

Click on **Add** to move the selected module to the display range.

ADVICE: You can also drag and drop the modules by mouse to move the module to the display range.
Workspace

The *right column* (in the following called *workspace*) shows monitors of modules you can switch by using *CrossDisplay-Switching*.

Monitors are displayed as rectangles. Both the module name and the assigned tradeswitch key are displayed in the rectangle. You can use the handles and the **Size** buttons underneath the grid to change the rectangles' height and width.

Click on **Remove** to remove the selected rectangle from the workspace.

ADVICE: You can also use »drag and drop« mouse operations to delete rectangles from the workspace.

The workspace's standard zoom level shows 20×15 units. However, you can adjust the size of the workspace:

- Press Q (zoom in) to maximize the workspace. The maximum zoom level shows a workspace of 4×3 units.
- Press Q (zoom out) to minimize the workspace. In the minimum zoom level, the workspace is displayed as 38×28 units (default setting).

NOTE: The maximum size of the workspace is adjusted dynamically if you drag an element beyond the available workspace.

You can increase the original size of 20×15 units as required.

Basic configuration

IMPORTANT: Before you can configure the *CrossDisplay-Switching* feature, you need to enable the premium **Tradeswitch** function (see page 230) and create a *Tradeswitch configuration* (see page 232).

Enabling CrossDisplay-Switching for the entire system

If you want to use the *CrossDisplay-Switching* function, we recommend that you activate the function for the entire system. This affects all computer modules that use the system-wide setting (*default*).

You can override the system-wide settings for each computer module and enable or disable *CrossDisplay-Switching* for certain computer modules only.

ADVICE: You can also disable the system settings and enable *CrossDisplay-Switching* only in the settings of computer modules on which you want to use the function.

How to change the CrossDisplay-Switching system settings:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Click on the General tab.
- 4. In the field **Mouse mode | CrossDisplay-Switching**, you can select between the following options:

Relative mouse coordingates CDS disabled:	Disable CrossDisplay-Switching for the entire system.
Absolute mouse coordinates CDS activated:	Enable CrossDisplay-Switching for the entire system.

ADVICE: You can enable or disable *CrossDisplay-Switching* for certain modules independently of the selected system settings (see below).

5. Click on Save.

Adjusting the general CDS mouse speed

If *CrossDisplay-Switching* is enabled, the mouse speed is not controlled by the operating system of the computer, but by the matrix switch.

If the cursor moves too fast or too slow, you can adjust the speed in the matrix switch.

You can adjust the mouse speed for the entire system or for one computer module only.

How to change the system settings of the mouse speed:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on Configuration.
- 3. Click on the General tab.
- 4. Move the **CDS mouse speed** slider to the desired value.
- 5. Click on Save.

CDS mouse positioning

When moving the mouse cursor to an edge of the active monitor with a second monitor placed next to the active monitor, the mouse cursor remains at the position at which the switching to the module of the second monitor takes place.

NOTE: When using CDS for switching, a mouse cursor may be visible on several monitors.

In addition, when leaving the monitor, the matrix switch can position the mouse cursor so that it is barely visible. For this, you can use the settings **Right** and **Bottom**.

You can define this setting for the entire system. By default, all CDS modules use the system-wide setting. However, you can also individually define the mouse position for each CDS module.

How to change the system setting of the mouse position:

- 1. In the menu, click on Matrix systems > [Name] > Matrix.
- 2. Click on the matrix switch and then click on **Configuration**.
- 3. Click on the General tab.

4. In the **CDS mouse positioning** field, you can select between the following options:

Off:	The mouse cursor remains at the position at which the switching to the module of the next monitor takes place (<i>default</i>).
On:	According to the CDS mouse hideout setting the mouse cursor is positioned so that it is barely visible.
	Only during <i>multi-user access</i> , the cursor remains at the position at which the switching to the next monitor takes place.
On (multi access:	According to the CDS mouse hideout setting, even during <i>multi-user access</i> , the mouse cursor is positioned so that it is barely visible.

ADVICE: You can enable or disable this function for particular modules independently from the selected system setting.

5. With activated CDS mouse positioning, you can select between the following options in the **CDS mouse hideout** field:

Right:	The mouse cursor is placed on the right edge of the monitor so that it is barely visible.
Bottom:	The mouse cursor is placed on the bottom edge of the monitor so that it is barely visible.

6. Click on Save.

Enabling CrossDisplay-Switching for a specific computer module

How to change the CrossDisplay-Switching settings for a specific computer module:

- 1. In the menu, click on Matrix systems > [Name] > Computer modules.
- 2. Click on the computer module you want to configure and then click on **Configuration**.
- 3. Click on the General tab.
- 4. In the field **Mouse mode | CrossDisplay-Switching**, you can select between the following options:

System:	The system settings are adopted (default)
Relative mouse coordingates CDS disabled:	Disable CrossDisplay-Switching for the specific computer module.
Absolute mouse coordinates CDS activated:	Enable <i>CrossDisplay-Switching</i> for the specific computer module.

- If you select Absolute mouse coordinates | CDS activated for this specific computer module, then select the desired options in the fields CDS mouse speed, CDS mouse positioning and CDS mouse hideout as described in the system settings (see page 244 ff.).
- 6. Click on Save.

Configuring the CrossDisplay-Switching function

You can configure the CrossDisplay-Switching function comfortably with a wizard. Click on the menu **Advanced features** and select the entry **Tradeswitch/FreeSeating/ CrossDisplay-Switching**. Click on **Configure** to start the wizard.

NOTE: Steps 1 through 4 (see page 232 ff.) of the wizard show you how to create a tradeswitch workplace.

NOTE: A tradeswitch workplace is a basic requirement to set up the »CrossDisplay-Switching« function.

Step 5: Position displays

How to add monitors to the workspace:

- 1. In the *left column*, select a console module or a computer module.
- 2. Click on the Add icon.

ADVICE: You can also drag and drop monitors by mouse.

In the workspace, each added module is displayed as a grey rectangle (4×3 units) with a black frame and is placed on a free position.

The rectangle symbolises the monitor of the module placed on your desk. The name of the connected module and the assigned tradeswitch key are displayed in the rectangle.

How to remove monitors from the workspace:

- 1. In the *right column*, select the rectangle of the monitor you want to remove.
- 2. Click on the **Remove** icon.

ADVICE: You can also drag and drop monitors by mouse.

Each removed module monitor is added to the list of modules in the left column.

How to move monitors within the workspace:

IMPORTANT: Exact switching is only possible if the monitors shown in the web application are placed in the same order as on your desk.

NOTE: Spaces between the monitors in the workspace are skipped during *CrossDisplay-Switching*.

- 1. Move the mouse over the rectangle of the monitor you want to move.
- 2. Press and hold the **left mouse key** while dragging the rectangle to the desired position.

If the frame of the rectangle turns red while dragging it, the current position is (partly) occupied and therefore the rectangle cannot be placed there.

Drag the handle beyond the right or left edge if the workspace is too small for the monitor size you want to adjust. The workspace maximizes automatically.

3. Release the left mouse key when a green frame is displayed.

ADVICE: For finetuning and as an alternative to mouse operations, you can use the **Position** buttons below the grid after clicking a rectangle.

How to adjust proportions among monitors:

NOTE: Adjust the monitor proportions exactly to be able to position the mouse precisely and switch between monitors.

The monitor resolution is not important for this step.

1. Click on the rectangle of the monitor for which you want to change the size.

On each of the rectangle's corners and in the middle between the two corners you can see adjustment handles (small black squares).

2. Click one of the handles and hold the **left mouse key** while dragging the handle to the desired position.

If the frame of the rectangle turns red while dragging it, the position is (partly) occupied and therefore the rectangle cannot be placed there.

Drag the handle beyond the right or left edge if the workspace is too small for the monitor size you want to adjust. The workspace maximizes automatically.

3. Release the left mouse key after a green frame is displayed.

ADVICE: For finetuning and as an alternative using a mouse, you can use the **Position** buttons below the grid after clicking on a rectangle.

4. If required, repeat steps 2 and 3 with the other handles of the rectangle.

Step 6: Configure CDS settings of computer modules

How the change »CrossDisplay Switching« settings of computer modules:

- 1. Click on the computer module you want to configure and then click on Edit.
- 2. In the **CrossDisplay-Switching** field, you can select between the following options:

System:	The matrix switch settings are applied to the entire system (see above).
Disabled:	<i>CrossDisplay-Switching</i> is disabled for this computer module. The system settings are ignored.
Enabled:	<i>CrossDisplay-Switching</i> is enabled for this computer module. The system settings are ignored.

3. Click on Save.

How to change the mouse speed of computer modules:

- 1. Click on the computer module you want to configure and then click on Edit.
- 2. In the **CDS mouse speed** field, you can select between the following options:
 - a. If you want to apply the system settings of the mouse speed to the computer module, enable the option **System**.
 - b. If you want to set an individual mouse speed, disable the **System** option and set the desired value.
- 3. Click on Save.

How to adjust the *CrossDisplay* resolution of a computer module:

NOTE: With active *CrossDisplay-Switching*, the mouse speed is not controlled by the operating system of the computer but by the matrix switch.

If the cursor speed changes between horizontal and vertical mouse movements, the monitor resolution could not be auto detected.

In such cases, a resolution of 1680×1050 pixels applies. If the monitor's resolution differs from this resolution, the mouse moves as described above.

In this case, you can adjust the monitor resolution manually.

- 1. Click on the computer module you want to configure and then click on Edit.
- 2. Disable the Auto option in the CDS resolution field.
- 3. Enter the vertical and horizontal resolution in the input boxes.
- 4. Click on Save.

How to change the mouse position of a particular computer module:

- 1. Click on the computer module you want to configure and then click on Edit.
- 2. In the **CDS mouse positioning** field, you can select between the following options:

System:	Use systemwide (see above) setting (default).
Off:	The mouse cursor remains at the position at which the switching to the module of the next monitor takes place.
On:	According to the CDS mouse hideout setting the mouse cursor is positioned so that it is barely visible.
	Only during <i>multi-user access</i> , the cursor remains at the position at which the switching to the next monitor takes place.
On+Multi:	According to the CDS mouse hideout setting, even during <i>multi-user access</i> , the mouse cursor is positioned so that it is barely visible.

3. With activated CDS mouse positioning, you can select between the following options in the **CDS mouse hideout** field:

Right:	The mouse cursor is placed at the right edge of the monitor so that it is barely visible.
Bottom:	The mouse cursor is placed at the bottom edge of the monitor so that it is barely visible.

4. Click on Save.

Messages

In some cases CrossDisplay-Switching cannot be used.

In such cases, a message is displayed on the monitor of the console module. The messages have the following meaning:

Message	Meaning
No CDS: Globally disabled	No CDS possible as the function is deactivated for the entire system (see <i>Enabling CrossDisplay-Switching for the</i> <i>entire system</i> on page 243)
No CDS: Disabled	No CDS possible as the computer module uses relative mouse coordinates (see <i>Enabling CrossDisplay-Switching</i> <i>for a specific computer module</i> on page 246).
No CDS: No Tradeswitch modifier	No CDS possible because no tradeswitch key modifier (see <i>How to change tradeswitch key modifier or valid trade-</i> <i>switch keys:</i> on page 231) has been configured.
No CDS: Computer module not found	No CDS possible because the computer module was not found.
No CDS: Computer module multiuser mode	No CDS possible as a user is already connected to the computer module and this does not support MultiAccess (see <i>Access mode for simultaneous access to computer modules</i> on page 97).
No CDS: Computer module not supported	No CDS possible as the computer module does not support switching via CDS.
	Contact our support team for more information.
No CDS: Console not found	No CDS possible because the console module does not exist in the matrix switch database (anymore).
No CDS: Console MultiAccess mode	No CDS possible because the console module is included in several Workplaces (Tradeswitch configurations) and does not support multiuser CDS.
No CDS: Unknown error	No CDS possible.
	Contact our support team for more information.

CDS multihead groups

CDS multihead groups let you create a CDS workplace. You can switch *any* video channel to the monitors of this workplace.

The video channel can be either the (only) video channel of a computer with one graphics output only or a *given* video channel of a computer with multiple graphics outputs.

The configuration settings of a CDS multihead group provide the matrix switch with the resolutions and order of connected video channels belonging to one display range of a computer. These information allow flexible switching via CDS.

IMPORTANT: If two different users operate two different targets of a CDS multihead group at the same time, the mouse jumps between the affected video channels of both users.

Differences between CDS modes

CDS multihead groups expand the functional range of CrossDisplay-Switching (CDS):

• In **CDS with channel grouping** mode, the matrix switch can display an additional video channel (added via channel group) of a computer with multiple graphics outputs only on monitors of console modules that also have a compatible channel group

Showing the *first* video channel of another target on an *additional* monitor of a channel group is not possible.

• **CDS with multihead groups** lets you display on *every* monitor either the (only) video channel of a computer with one graphics output or a *given* video channel of a computer with multiple graphics outputs.

IMPORTANT: In **CDS** with channel grouping mode, connect each computer module within the group to the computer using a USB cable.

Example of use

The following example shows the difference between the two CDS modes:

EXAMPLE: A display range of 3840×1200 pixels is defined in the graphics settings of a computer. The computer uses two video channels with 1920×1200 pixels each to transmit the display range to two monitors.



CDS with channel groups

The chapter *Implementation of multihead monitors* (see page 240) describes how to implement multihead computers with channel groups into the CDS configuration.

In the CDS configuration, the *combined* size of the monitors belonging to a channel group (monitors **2a** and **2b** in the example below) is adjusted so that their size ratio fits the other monitors:



IMPORTANT: Only monitor *2b* of the CDS workplace can display the *second* video channel of a multihead computer!

It is *not* possible to display the first video channel of a target on this monitor.

At the CDS workplace, when moving the mouse cursor to the right-hand margin of monitor **1**, the matrix switch switches to monitor **2a** and places the cursor in a way that you barely realise the changing between the cursors of both computers.

When moving the mouse cursor to the right-hand margin of monitor **2a**, the matrix switch detects with the help of the CDS configuration that the next monitor **2b** is connected to another graphics output of the already accessed computer. Therefore, a switching does *not* take place and the mouse cursor is *not* positioned.

When switching a computer with only one video channel to monitor **2a**, you need to drag the mouse through the unused display range of monitor **2b** before using CDS switching to switch to monitor **3**.

NOTE: This type of CDS configuration is recommended when you always switch multihead computers to particular monitors of the CDS workplace (**2a** and **2b** in the example).

CDS with mulithead groups

CDS with multihead groups allows you to display the individual video channels of multihead computers on any monitor of the CDS workplace.



You can switch the two display ranges of the multihead computer mentioned in the example above to monitors 1 and 2, monitors 2 and 3 or monitors 3 and 4.

NOTE: For *CDS with multihead groups*, instead of being grouped, individual channels are managed, configured and switched within the KVM matrix system.

You can switch *any* video channel to *each* monitor of the CDS workplace. The channel can be either the (only) video channel of a computer with one graphics output or a *given* video channel of a computer with multiple graphics outputs.

NOTE: CDS with multihead groups requires *additional* configuration settings.

According to the configuration of the CDS multi head group, the matrix switch detects the order of the devices and the resolution of each channel. This way, switching via CDS takes place reliably at the margins of the display range.

Requirements

- Enabled premium **Tradeswitch** function (see page 230).
- Established and configured *Tradeswitch configuration* (see page 232 ff.).
- Enabled CrossDisplay-Switching (see page 243).
- The channels of multihead computers must not be part of channel groups (see page 192). If necessary, delete the channel groups of the computer modules you want to configure.

IMPORTANT: Channel groups are required to implement multihead computers as described in the chapter *Implementation of multihead monitors* (see page 240).

Both CDS operating modes can be used at the same time in a KVM matrix system. However, you can use only one operating mode per computer and per CDS workplace.

- Order and size ratio of the monitors at the CDS workplace are saved in the web application (see page 241).
- The computer modules used at the individual video channels of a computer are all individually connected to the computer via USB.

The »Member configuration« view

During basic CDS configuration you already defined order and size ratio of the monitors belonging to the CDS workplace (see page 241).

When configuring CDS multihead groups, you first reproduce the computer's display ranges and then enter their resolutions.

IMPORTANT: The configuration of CDS multihead groups *must* comply with the configuration of the computer's graphics settings!

The following screenshot shows two adjoining video channels (1920×1200 each) of a multihead computer (see example on page 253). The combined display range of the *CDS multihead group* has a resolution of 3840×1200 pixels.



The tab is divided into two parts The following paragraphs provide a detailed description of these parts.

List of computer modules

The table on the *left-hand side* lists all computer modules that are not part of a CDS multihead group.

By clicking on **Add** you can move the highlighted module into the display range.

ADVICE: You can also use »drag and drop« mouse operations to move modules to the display range.

Workspace

The workspace on the *right-hand side* shows the display ranges of video channels of multihead computers. Each display range is transmitted by a separate computer module.

The display ranges are displayed as rectangles. The name of the computer module and the resolution of its display range is displayed inside of the rectangle.

You can arrange the individual display ranges in horizontal or vertical order or in blocks. Blocks must be put together to form complete quadrangles. L-shaped arrangements are *not* supported.

IMPORTANT: The display range entered in the workspace must reflect the computer's *entire* display range.

Click on **Remove** to delete the selected rectangle from the workspace.

ADVICE: You can also use »drag and drop« mouse operations to delete rectangles from the workspace.

At default zoom level, the workplace is displayed in units of 4×4 . You can adjust the size of the display range:

- Click on (*coom in*) to maximize the workspace. At maximum zoom level, the workspace is displayed in units of 2×2.
- Click on (*coom out*) to minimize the workspacer. At minimum zoom level, the workspace is displayed in units of 20×20 (default).

NOTE: The maximum size of the workspace adjusts dynamically when you move an element over the available workspace.

You can expand the default size of 16×16 units as far as you wish.

Configuring CDS multihead groups

You can configure the CDS multihead groups comfortably with a wizard. Click on the menu **Advanced features** and select the entry **CDS multihead groups**. Click on **Configure** to start the wizard.

NOTE: Steps 1 through 4 (see page 232 ff.) of the Tradeswitch function/CrossDisplay-Switching wizard show you how to create a tradeswitch workplace.

NOTE: Steps 5 and 6 (see page 247 ff.) of the Tradeswitch function/CrossDisplay-Switching wizard show you how to set up the CrossDisplay-Switching function.

Step 1: Administrate CDS multihead groups

How to create a new CDS multihead group:

- 1. Click on Add.
- 2. In the Name field, you can enter the name of the group.
- 3. *Optional:* In the **Comment** field, you can enter a comment about the group.
- 4. Select one of the options listed in the **CDS mouse mode** field:

NOTE: By default, when reaching one of the edges of the active monitor, switching does not take place if a mouse button is pressed while moving the mouse.

When working with Windows and Linux operating systems, you can enable specific mouse modes that allow drag and drop operations.

Standard:	When reaching one of the edges of the active monitor, switching does not take place if a mouse button is pressed while moving the mouse.
Windows:	Under <i>Windows</i> operating systems switching takes place even when pressing a mouse key while moving the mouse to the edge of the active monitor.
Linux:	Under <i>Linux</i> operating systems switching takes place even when pressing a mouse key while moving the mouse to the edge of the active monitor.

5. Click on Save.

How to change the settings of a CDS multihead group:

- 1. Click on the group you want to configure and then click on Edit.
- 2. In the Name field, you can change the name of the group.

- 3. *Optional:* In the **Comment** field, you can change or enter a comment about the group.
- 4. Select one of the options listed in the **CDS mouse mode** field:

NOTE: By default, when reaching one of the edges of the active monitor, switching does not take place if a mouse button is pressed while moving the mouse.

When working with Windows and Linux operating systems, you can enable specific mouse modes that allow drag and drop operations.

Standard:	When reaching one of the edges of the active monitor, switching does not take place if a mouse button is pressed while moving the mouse.
Windows:	Under <i>Windows</i> operating systems switching takes place even when pressing a mouse key while moving the mouse to the edge of the active monitor.
Linux:	Under <i>Linux</i> operating systems switching takes place even when pressing a mouse key while moving the mouse to the edge of the active monitor.

5. Click on Save.

How to delete a CDS multihead group:

- 1. Click on the group you want to delete and then click on Delete.
- 2. Confirm the security prompt by clicking on **Yes** or cancel the process by clicking on **No**.

Step 2: Configure CDS multihead groups

Saving order and resolutions of workspaces

Arrange the display ranges of the graphics cards installed in the multihead computer as they are displayed in the computer's graphics configuration.

IMPORTANT: You can arrange the individual display ranges into horizontal or vertical order or in blocks. Blocks must be put together to form complete quadrangles. L-shaped arrangements are *not* supported.

How to add a workspace to the display range:

- 1. Select a computer module from the *left column*.
- 2. Click on Add.

ADVICE: You can also drag and drop computer modules by mouse.

In the workspace, each added computer module is displayed as a grey rectangle $(1 \times 1 \text{ units})$ with a black frame and is placed on a free position.

The name of the computer module and the resolution of its display range are displayed inside the rectangle.

How to remove a display range from the workspace:

- 1. On the right-hand side of the workspace, select the rectangle symbolizing the display range you want to delete.
- 2. Click on Remove.

ADVICE: You can also drag and drop display ranges by mouse.

How to move a display range within the workspace:

IMPORTANT: Exact switching is possible only if the monitor arrangement stored in the web application complies with the arrangement at the workstation.

NOTE: Empty spaces between display ranges are not valid.

- 1. Move the mouse over the rectangle symbolizing the display range you want to move.
- 2. Press and hold the **left mouse key** while dragging the rectangle to the desired position within the workspace.

If the frame of the rectangular turns red while dragging it, the position is already occupied and therefore not valid.

Drag the over the right or the bottom frame if the workspace is too small for the desired position. This way, the workspace becomes automatically larger.

3. Release the left mouse key when a green frame is displayed.

ADVICE: as an alternative to using a mouse, you can use the **Position** buttons below the grid after clicking on a rectangle.

How to adjust the resolution of a display range:

- 1. In the table on the left, enter the **resolutions** of the computer modules of the CDS multihead group.
- 2. Click on Save and continue.

MatrixGuard (optional)

IMPORTANT: Using the MatrixGuard function requires the purchase and activation of the premium **MatrixGuard Function**.

IMPORTANT: The MatrixGuard Function is *not* compatible with U2-LAN devices.

If the current database leader is unavailable, the MatrixGuard function organises the forwarding of the leader role to another, available matrix switch of the MatrixGuard.

All matrix switches of a MatrixGuard system share a common (virtual) MatrixGuard address. The MatrixGuard automatically determines the database leader based on the availability and priority of its members.

IMPORTANT: Configure the same MatrixGuard address on each matrix switch of the MatrixGuard system (see page 270).

Rules for the assignment of the leader role

1. When negotiating the leader role, the assigned priorities are taken into account (see page 270).

If *several* matrix switches have the highest priority, the MatrixGuard function decides which matrix switch is assigned the leader role.

2. When restarting a matrix switch that used to be the database leader before the restart, the system checks whether a new leader exists in the MatrixGuard system.

If this is the case, the booting matrix switch is downgraded to follower during the restart.

3. If a leader matrix switch becomes available again without restarting the device (e.g. after a temporary failure of a network component), the leader role is renegotiated if a new leader has become available in the MatrixGuard system in the meantime.

Example 1: Restart of all components

If all KVM components are restarted (e.g. after a power failure), each matrix switch checks whether one or more matrix switches of the MatrixGuard system are available as soon as it has initialized its network functions.

The first available matrix switch automatically becomes the database leader, since no other matrix switch of the MatrixGuard is available at this time.

The then starting matrix switches are automatically downgraded to follower during the boot process (see rule no. 2).

Example 2: Failure of the current database leader

All matrix switches in the MatrixGuard system regularly check whether the database leader is available. As soon as the database leader is no longer available, the remaining matrix switches renegotiate the leader role based on the assigned priorities.

IMPORTANT: When another matrix switch takes over the **leader** role, all end devices *briefly* lose the connection to the KVM matrix system and all open **Config Panel** sessions are terminated.

Example 3: Recognition of another database leader

A MatrixGuard system may contain only one available database leader.

If, for example, after the network connection of the previously active database leader has been restored, another database leader becomes available within the MatrixGuard system, the leader matrix switches renegotiate the leader role based on the assigned priorities.

IMPORTANT: When another matrix switch takes over the **leader** role, all end devices *briefly* lose the connection to the KVM matrix system and all open **Config Panel** sessions are terminated.

Example 4: Failure of a network component

If a network component fails, it is possible to separate a MatrixGuard system into several individual parts.

If the network switch fails, none of the matrix switches reaches another matrix switch included in the MatrixGuard system.

The current follower matrix switches therefore renegotiate the leader role. Since each follower matrix switch cannot reach another matrix switch due to the missing network connection, each matrix switch takes over the leader role for itself.

As soon as the network component is available again, the matrix switches renegotiate the roles as described in example 3.

Important notes

• Each matrix switch manages its MatrixGuard settings autonomously.

When setting up the MatrixGuard function, it is therefore necessary to separately configure the settings in *all* matrix switches of the group via the web application of the individual matrix switches.

The group automatically negotiates the **leader** role. The other matrix switches are automatically configured as database **follower**.

• All matrix switches of the MatrixGuard group are assigned the same virtual network interface.

The web application of the current leader can be reached via the IP address of the virtual network interface.

• After setup, the current MatrixGuard role of a matrix switch is displayed on the overview page of the MatrixGuard function.

You can also display the **Database mode** column in the web application under **Matrix** systems > Matrix (see page 10) and get the status from there.

• Each IP matrix switch supports a maximum of 20 end devices in the standard scope of delivery. Make sure that all participants of the **MatrixGuard** support sufficient end devices!

Requirements

Before configuring the MatrixGuard function, make sure to meet the following requirements:

- A functioning KVM matrix system is available.
- The matrix switches are in the same subnet.
- The network switches are able to forward **multicast** packets.
- The MatrixGuard feature is enabled for all matrix switches.

IMPORTANT: Use of the MatrixGuard function *is not* possible with **activated DHCP server** (see page 4) and/or when using the **DirectRedundancyShield** function (see page 272)!

Configuring a MatrixGuard member

IMPORTANT: Each matrix switch manages its MatrixGuard settings autonomously.

When setting up the MatrixGuard function, it is therefore necessary to separately configure the settings in all matrix switches of the group via the web application of the individual matrix switches.

You can configure each MatrixGuard member conveniently with a wizard. Click on the menu **Advanced features** and select **MatrixGuard**. To start the wizard, click on **Configure**.

The following sections briefly summarize the wizard's configuration options.

Overview: Configuration of a MatrixGuard member

If you have already configured the member's MatrixGuard function, the wizard starts with an overview of the member's most important settings.

NOTE: When configuring the MatrixGuard function for the first time, the wizard immediately starts with **step 1** (see below).

You can find the following information in the overview:

- **Priority:** User-defined priority of this matrix switch
- MatrixGuard member: Name of this matrix switch
- MatrixGuard role: Role this matrix switch currently has in the MatrixGuard group.

You can perform the following actions on the overview page of the wizard:

- **Remove member:** After clicking this button you will be prompted to select the future operating mode and to configure the connection to the leader.
- Assign leader role: If the member is currently operated as follower (see column MatrixGuard role), you can click on this button to make it the leader.
- Configure: Click on this button to go to configuration steps 1 to 3 (see below).

Step 1: Set system time

IMPORTANT: If the time difference between the matrix switches is too large, an encrypted connection cannot be established between the matrix switches.

Therefore, we strongly recommend using an NTP server for automatic time alignment.

How to change the NTP time sync settings:

1. Under NTP server, enter the following data:

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

2. Click on Save and continue.

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

1. Go to NTP server.

IMPORTANT: If necessary, disable the option **NTP time sync**. Otherwise, it is not possible to set the time and date manually.

- 2. In the Time field of the Time/date paragraph, enter the time in the format hh:mm:ss.
- 3. In the **Date** field of the **Time/date** paragraph, enter the current date in the format

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

DD.MM.YYYY.

4. Click on Save and continue.

Step 2: Set certificate

Communication between matrix switches is possible only if all devices use certificates of the same *Certificate Authority*.

For self-created certificates, be sure to use the same *certificate authority* or alternatively use **Certificate #1** (preferred) or **Certificate #2** for all matrix switches.

How to select the SSL certificate to be used:

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

1. Select the SSL certificate you want to use:

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

3. Click on Save and continue.

Step 3: Configure members

In this step, you configure the MatrixGuard settings of the matrix switch whose web application you have opened:

• Priority: Assign this matrix switch a priority between 1 (high) and 10 (low).

NOTE: The matrix switches negotiate the leader role based on the defined priorities.

The matrix switch with the highest priority is assigned the leader role. If this priority is assigned to several matrix switches, the MatrixGuard function decides which of these matrix switches gets the leader role.

IMPORTANT: Assign priority 1 to exactly one **MatrixGuard** participant and other priorities to the other participants.

In this way you can avoid a *permanent* role assignment of all MatrixGuard participants in the event of *short-term* network failures.

• Interface: Select the network interface via which this matrix switch is available in the MatrixGuard group.

You can select the physical network interfaces and (if configured) also the link aggregation interface.

• MatrixGuard address: Assign the matrix switch an IP address that is not assigned in the subnet.

IMPORTANT: Assign the *same* virtual IP address to all matrix switches included in the MatrixGuard group.

• MatrixGuard netmask: Enter the netmask of the subnet.

IMPORTANT: The MatrixGuard function requires all matrix switches to be on the same subnet.

NOTE: A virtual network interface is set up using the parameters **MatrixGuard address** and **MatrixGuard network**.

The current leader of the MatrixGuard system is available under this virtual IP address.

• **Port (»local«** and **»remote«**): Define the port (usually 27996) through which this device communicates with the other devices of the MatrixGuard group.

NOTE: Assign the same port to all devices included in the MatrixGuard group.

Click on Save and continue to add this device to the MatrixGuard system.

IMPORTANT: Make sure that the computer and console modules are *directly* connected to the IP matrix system via the **MatrixGuard** address.

The easiest way to ensure this is to decouple and re-connect the computer and console modules to the IP-Matrix via the web application of the **MarixGuard** leader (see chapter *Basic configuration of the KVM-over-IP*TM *connection* in the installation manual).

DirectRedundancyShield (optional)

NOTE: Using the DirectRedundancyShield feature requires the purchase and activation of the premium **DirectRedundancyShield feature** for both matrix switches.

The DirectRedundancyShield (DRS) is based on the application of an active and a passive matrix switch. Both matrices establish independent encrypted connections to all KVM-over-IP end devices at system startup.

Thus, two connections to independent matrix switches are available to the end devices. The end devices use the DRS to automatically connect to the matrix switch, which has the DRS status **Active**.

During operation, the DRS ensures that the switching states of the KVM-over-IP end devices are continuously synchronized at both matrix switches. In case the first matrix switch is no longer accessible, a second matrix switch is available via DRS. The continued operation of the matrix system is ensured with a changeover time of less than one second while maintaining all switching states.

The DRS status

The **DRS status** column of the respective matrix switch can be displayed via **matrix** systems > matrix in the web application (see page 10) and the status can be viewed. By activating the DRS function, the DRS status column is automatically displayed.

The DRS status can be as follows:

- Active: The matrix switch which has the DRS status Active is currently being operated. The end devices connect to this matrix switch. The switching states are transferred from this matrix switch to the matrix switch having the DRS status **Passive**.
- **Passive**: The matrix switch which has the DRS status **Passive** is not currently being operated. The switching states of the matrix switch, which has the DRS status **Active**, are transmitted to this passive matrix switch. It can start operating at any time in the event the currently active matrix switch fails. In this case, the DRS status immediately changes from **Passive** to **Active**.

It is also possible to carry out maintenance operations (e.g., a firmware update) on the matrix switch with the DRS status **Passive**.

• **Deactivated**: The DRS function has *not* yet been configured. The switching states are *not* transmitted and synchronized.

IMPORTANT: To operate your matrix system via an external IP control (see *IP-Control-API (optional)* on page 215 ff.), you must select the matrix switch with DRS status **Active**. In this case, a verification of the DRS status should be integrated before executing commands.

Rules for the assignment of the DRS status

- 1. When configuring the DRS function, the DRS status is initially determined.
- 2. When restarting a matrix switch which occupied the DRS status **Active** before the restart, it is verified whether the second matrix switch has taken over the connections and the status **Active** in the meantime. In this event, the restarting matrix switch is assigned the DRS status **Passive**.
- 3. If both matrix switches become available again as soon as the device is restarted (for example, after a temporary failure of a network component), the DRS status is assigned according to the initial setup.

Example 1: Restart of all KVM components

When all KVM components are restarted (for example, after a power failure), the first available matrix switch automatically receives the DRS status **Active**, since the other matrix switch is not yet available at this point. The subsequent starting matrix switch automatically receives the DRS status **Passive** during the boot process.

Example 2: Failure of the active matrix switch

The two matrix switches of the DRS group regularly check whether the active matrix switch is available. Whenever the active matrix switch is no longer accessible, the previously passive matrix switch is automatically and immediately assigned the DRS status **Active**.

Example 3: Failure of a network component

If a network component fails, it is possible to separate a DRS group. If the network switch fails, the two matrix switches are unable to communicate with the respective counterpart. Both matrix switches receive the DRS status **Active**. As soon as the network component is accessible again, the DRS status is assigned according to the initial setup (see *Step 1: Initial setup and definition of the target system* on page 275 ff.).

Important notes

- The **Database mode** column of the respective matrix switch can be displayed via **matrix systems > matrix** in the web application (see page 10) and the status can be viewed.
- You can view the DRS status column of the respective matrix switch by selecting matrix systems > matrix in the web application (see page 10) and check the status. By activating the DRS function, the DRS status column is automatically displayed.

Requirements

Before configuring the DRS function, make sure to meet the following requirements:

- A functioning KVM matrix system is available.
- Both matrix switches communicate with each other via a network connection.
- The *DirectRedundancyShield-Feature* is enabled in both matrix switches.
- Both matrix switches are set to database mode Leader.
- The *DirectRedundancyShield-Feature* must be supported by the end devices used. This is generally the case for all G&D devices that use KVM-over-IP for transmission. A firmware update may be required. Supported are:
 - Devices of the *VisionXS-IP* series from firmware 1.3.0
 - Devices of the Vision-IP series from firmware 2.3.0
 - Devices of the RemoteAccess-IP-CPU series from firmware 1.2.0
- Both matrix switches support **sufficient end devices**. Each IP matrix switch supports a maximum of 20 end devices in the standard scope of delivery.

IMPORTANT: Using the DirectRedundancyShield function is not possible with **activated DHCP server** (see page 4) and/or when using the **MatrixGuard** function (see page 263)!

Configuring the DRS function

The configuration of the DRS function for the two devices is performed conveniently with a wizard. In the web application of the matrix switch which is to initially adopt the DRS status **Active**, click the **Advanced features** menu and select **DirectRedundancyShield (DRS)**. To start the wizard, click on **Configure**.

IMPORTANT: It is recommended to complete the entire system configuration if possible before activating the DRS function! After the configuration of the DRS function is completed, the passive matrix switch receives the database information of the active matrix switch once.

For direct switching between the matrix switches, continuous database synchronization (system-wide settings as well as configuration of the terminals, user rights, etc.) was dispensed with for the DRS function. Only switching states are synchronized. Later changed configuration parameters on the active matrix switch must be manually adjusted using the wizard and transferred to the passive matrix switch again (see *Step 2: Adjust configuration* on page 276).

The following sections briefly summarize the wizard's configuration options.

Step 1: Initial setup and definition of the target system

How to configure the DRS function:

1. Enter the following data:

Di Re Si	rect edundancy hield (DRS):	 Enabled Disabled (default)
IP address/ hostname of the target system:		Enter the IP address or the host name of the initial passive matrix switch (target system).
Control port of the target system:		Enter the number of the control port of the target system (<i>default: 18246</i>).
	NOTE: The follo field Direct-Redu	owing input boxes appear as soon as you select <i>Enabled</i> in the ndancyShield (DRS) .
	The entries in t active matrix s	hese fields are not permanently stored in the database of the witch but are only used for the following connection setup.
User of the target system with superuser rights:		Enter the user name of a user of the target system with superuser rights.
Password:		Enter this user's password.
One-time password:		Enter the one-time password for the two-factor authentication of this user.
	NOTE: The one tion has been se	-time password must only be entered if two-factor authentica- et up (see page 50 ff.) and has been enabled (see page 72 ff.).

2. Click on Save and continue.

IMPORTANT: The matrix system restarts and the connections to the end devices are reestablished. Plan for a short downtime of the system at this point!

Step 2: Adjust configuration

In step 2, the configuration of the active matrix switch can be transferred to the passive matrix switch.

IMPORTANT: Click **Save and continue** to transfer the configuration of the active matrix switch to the passive matrix switch/the specified target system. As a result, the original data of the target system will be overwritten. The transfer process can take up to 5 minutes. During this time, the target system is offline and is not available for operation.

1. Click on Save and continue.

IMPORTANT: Do not restart either matrix switch during the transfer process and do not close the browser session.

2. Enter the following data in the pop-up window that opens:

User name:	Enter the user name of a user of the source system with superuser rights.
Password:	Enter this user's password.
One-time password:	Enter the one-time password for the two-factor authentication of this user.
NOTE: The one tion has been se	-time password must only be entered if two-factor authentica- et up (see page 50 ff.) and has been enabled (see page 72 ff.).
Name of the target system:	Enter a name for the target system if the previous name is not to be used. The previous name of the target system is read out and entered here by default.
Select the IP address of the source system used for connection to the end devices:	Select the IP address of this active matrix switch used for the connection to the end devices. You may also click on the input box and enter the IP address.

- 3. Click on Continue.
- 4. If an error message appears, click **Cancel** and repeat the process.

Step 3: DRS configuration completed

After successfully transferring the configuration to the passive matrix switch/the target system, the DRS is set up on both matrix switches.

ADVICE: Check in the web application of the passive matrix switch whether all end devices have established the connection to the passive matrix switch and the configuration has been successfully adopted.

IMPORTANT: Once the DRS configuration is complete, modify the configuration parameters only on the active matrix switch and transfer them as soon as possible to the passive matrix switch (see *Step 2: Adjust configuration* on page 276). In this way, you can ensure that no changes are lost and that both matrix switches are synchronized. On the passive matrix switch, configuration is only possible to a limited extend.

IMPORTANT: If you operate the DRS function with **UID locking** enabled, you must manually add the respective counterpart to UID locking in both matrix switches after completing the DRS configuration

(see Restricting KVM-over-IP counterparts (UID locking) on page 55 ff.).

This is the only way that the two matrix switches can subsequently communicate with each other and synchronize the switching states.
EasyControl (optional)

IMPORTANT: Using the EasyControl tool requires the purchase and activation of the premium **IP-Control-API** (see page 278 ff.).

You can use the **EasyControl** tool integrated in the web application to connect a console module to a specific computer module or to execute an existing script or script group.

After activating the **IP-Control-API** (see page 278 ff.), all users who assigned with the right to access the tool (see page 87) can use it.

Starting the »EasyControl« tool

How to start the tool:

1. Enter the following URL in the address line:

https://[IP address of the device]

2. Enter the following data in the login mask:

A of	gree to the terms use:	Click on the text to read the terms of use. Click on the checkbox to accept the terms of use.									
	NOTE: The terms made (see <i>Showi</i>	s of use only appear if a corresponding configuration has been <i>ing terms of use</i> on page 15 ff.).									
Username:		Enter a username.									
Password:		Enter a password for your user account.									
2. (1	Factor Auth Code OTP):	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.									
	NOTE: The 2 two-factor aut and activated (see	2-Factor Auth Code (TOTP) is only requested if thentication has been configured (see page 50 f.) the page 72 ff.).									

- 3. Click on Login.
- 4. Click on the EasyControl icon.

Establishing and disconnecting a connection

Use the tool in **Connection** mode to connect a console module to a computer module.

G& AND	KVM 5 RIGHT.	G&D EasyCont	trol	EN
	Connection		Script	
	Console 1 Connected to Target 1		Target 1 1 console connected	
	Console 2	Disconnect	Target 2	
	Console 3		Target 3	
				‡

The left column lists the console modules on which you are logged in at the moment.

NOTE: The following console modules are *not* listed here:

- Grouped console modules (except main channel 1),
- CON modules of U2-, U2+ or U2-LAN variants.

ADVICE: You can use scripts (see below) to log on to other console modules without having to log on to the OSD.

The *right* column lists all **computer modules** you can access according to the access rights assigned to your account.

NOTE: The following computer modules are *not* listed here:

- Grouped computer modules (except main channel 1),
- CPU modules of U2-, U2+ or U2-LAN variants

If a console or computer module has an active connection to a remote terminal, a short note indicates this condition in the list:

- **Console modules:** Connected to [*name of computer module*]
- **Computer modules:** [x] console(s) connected

Switching functions

How to connect a console module and a computer module:

- 1. Click on Connection.
- 2. *Successively* click the buttons of the console module and the computer module which you want to connect with each other.

NOTE: The last clicked button is displayed as *marked*. Click anywhere outside of the button or on the button to cancel the mark.

The two devices connected via mouse click remain marked until the next click is made.

How to disconnect a console module from a computer module:

- 1. Click on the button of the *console module* you want to disconnect from a computer module.
- 2. Click on Disconnect.

How to show the remote station of the connected computer module:

1. Click on the button of the *console module* or *computer module* whose remote station you want to show.

The selected module and the module connected to it are now marked in the lists.

Hiding modules on the user interface

How to show or hide console or computer modules from the list:

1. Click on the gears icon at the bottom right (💽).

Each entry in the list of the console or computer modules contains the slider $\ensuremath{\mathsf{Hide}}$ device.

2. Activate the sliders of modules you want to hide from the list.

Deactivate the sliders of modules you want to show on the list.

3. Click the gears icon again (🔁).

Executing scripts

Use the tool in **Script** mode to execute an existing script or script group.

Each page of the user interface contains 12 buttons. Each of these buttons can be assigned a script or a script group.

G& AND KVM FEELS RICHT.	G&D	EasyControl			EN
	Connection		Script		
Configure button	Con	figure button		Configure button	
Configure button	Con	figure button		Configure button	
Configure button	Con	figure button		Configure button	
Configure button	Con	figure button		Configure button	
All notifications Only errors	Add Delete « 1	1 2 3 »	Skin 1 Ski	n 2 Skin 3 Bright Dark	

To be able to call a script or a script group using the tool, the following requirements must be met:

- The user logged in to EasyControl is assigned the right to execute a script or script groups.
- In the settings of the script or the script group the use in EasyControl is permitted.

IMPORTANT: When opening the script view of the tool for the first time, no buttons are configured yet.

You can only execute scripts or script groups after you have configured the buttons.

Configuring the interface

How to assign a script or a script group to an unconfigured button:

IMPORTANT: Unconfigured buttons are only visible in the configuration view. These buttons are not visible in the user view.

1. Click on the gears icon at the bottom right (.).

All available buttons are displayed in the middle of the view.

NOTE: Buttons that have already been configured show the name of the assigned script or script group.

Unconfigured buttons are marked with Configure.

- 2. Click on an unconfigured button marked with Configure.
- 3. Select the script or script group you want to execute using this button.

How to assign a colour to a configured button:

1. Click on the gears icon at the bottom right ().

All available buttons are displayed in the middle of the view.

NOTE: Buttons that have already been configured show the name of the assigned script or script group.

Unconfigured buttons are marked with Configure.

- 2. Click on a configured button.
- 3. Select the desired colour of this button.

How to add a page to or delete it from the view:

- 1. Click on the gears icon at the bottom right (💽).
- 2. Click on **Add** in the middle of the footer to add another empty page.

Click on **Delete** to delete the currently displayed page.

NOTE: Only empty pages can be deleted.

How to delete the configuration of a configured button:

- 1. Click on the gears icon at the bottom right $(\textcircled{\bullet})$.
- 2. Click on the **[X]** in the upper right corner of a configured button.

G& AND	KVM S RIGHT.			G&D EasyControl									
			Connection			Script							
	Script '	1			ipt 2		Script 3						
				Scr	ipt 4								
				« 1	2 3 »			\$ 7					

Operating the user interface

How to execute a script or a script group:

1. Click on Script.

All configured buttons are displayed in the middle of the view.

- 2. If necessary, use the page selection in the middle of the footer to select the page containing the desired button.
- 3. Click on the desired button.

General configuration settings

All notifications	Only errors	Skin 1 Skin 2 Skin 3 Bright Dark	‡	7
-------------------	-------------	----------------------------------	----------	---

Showing all notifications or only errors

- 1. Click on the gears icon at the bottom right ().
- 2. Select one of the given options:

All notifications:	Show all status and error notifications
Only errors:	Show only error notifications

3. Click the gears icon again (😰).

Changing the colour scheme of the tool

NOTE: The selected colour scheme is saved in the user settings of the active user. When using the tool the next time, the previously selected colour scheme is applied.

How to change the colour scheme:

- 1. Click on the gears icon at the bottom right (.).
- 2. Click on the button of the colour scheme you want to use (Skin 1, Skin 2 or Skin 3).
- 3. Each colour scheme is available in a variant for light and dark working environments. Select the desired variant:

Bright:Apply variant for bright surroundingsDark:Apply variant for dark surroundings

4. Click the gears icon again (🔅).

Closing the tool

How to close the tool:

1. Click on the **Exit** () icon at the bottom right.

Possible messages and their meanings

There are various messages that can appear on the monitor of the console module in certain cases. You have the option of adjusting or deactivating these information displays (see *Adjusting the information display* on page 184 ff.).

Below you find a selection of possible messages and their meanings:

Message	Meaning
Forwarding to	The console module is the leader workplace of the Trade- switch workplace (see <i>Administrating tradeswitch work- places</i> on page 232). This message appears when the input devices are switched to another console module or DWC.
	You can switch this message off if you want (see <i>Configure Tradeswitch visualization</i> on page 233).
FORWARDED	The console module is a target workplace of the Trade- switch workplace. This message appears when the input devices are switched from the leader workplace to this console module.
	You can switch this message off if you want (see <i>Configure Tradeswitch visualization</i> on page 233).
No CDS: Globally disabled	No CDS possible as the function is deactivated for the entire system (see <i>Enabling CrossDisplay-Switching for the entire system</i> on page 243 ff.).
No CDS: Disabled	No CDS possible as the computer module uses relative mouse coordinates (see <i>Enabling CrossDisplay-Switching</i> <i>for a specific computer module</i> on page 246 ff.).
No CDS: No Tradeswitch modifier	No CDS possible because no tradeswitch key modifier (see <i>Changing tradeswitch key and valid key type</i> on page 230 ff.) has been configured.
No CDS: Computer module not found	No CDS possible because the computer module was not found.
No CDS: Computer module multiuser mode	No CDS possible as a user is already connected to the computer module and this does not support MultiAccess (see <i>Access mode for simultaneous access to computer modules</i> on page 97 ff.).
No CDS: Computer module not supported	No CDS possible as the computer module does not support switching via CDS.
	Contact our support team for more information.
No CDS: Console not found	No CDS possible because the console module does not exist in the matrix switch database (anymore).
No CDS: Console MultiAccess mode	No CDS possible because the console module is included in several Workplaces (Tradeswitch configurations) and does not support multiuser CDS.
No CDS: Unknown error	No CDS possible.
	Contact our support team for more information.

Message	Meaning
Not connected	The console module is not connected to any computer module (for detailed information, please refer to the separate manual <i>Configuration and operation</i>).
Computer module not available	The console module should be connected to a computer module. However, this computer module is not available in the system.
No user logged in	The console module should be connected to a computer module. However, no user is logged on (for detailed information, please refer to the separate manual <i>Configuration and operation</i>).
Insufficient access rights	The console module should be connected to a computer module. However, the user rights do not allow this (see <i>Adjusting access and configuration rights</i> on page 94 ff.).
No MultiAccess right	The console module should be connected to a computer module. However, another user is already connected and the user does not have MultiAccess rights (see <i>Access mode for simultaneous access to computer modules</i> on page 97 ff.).
Unknown route to computer module	The console module should be connected to a computer module. However, the matrix switch does not know where the computer module is connected (for detailed information, please refer to the separate manual <i>Configuration and operation</i>).
No route to computer module available	The console module should be connected to a computer module. The matrix switch knows how to reach the computer module. However, there is no free line via which the computer module can be reached (for detailed information, please refer to the separate manual <i>Configuration and operation</i>).
Connection failed	The console module should be connected to a computer module. However, the router was unable to fulfill its task.
VIEW ONLY	Operation of the connected computer module is disabled (see <i>Adjusting access and configuration rights</i> on page 94 ff.).
	You can switch this message off if you want (see <i>How to</i> change the general settings of the information display for computer modules with view right: on page 184).
MULTIUSER	If several users are connected to a computer module, the number of connected users is displayed.
	You can switch this message off if you want (see <i>Multi-user information</i> on page 114 ff.).
AUTOSCAN	The computer module uses the autoscan function (see <i>Auto scanning all computer modules (Autoscan)</i> on page 174 ff.).
AUTOSKIP	The computer module uses the autoskip function (see <i>Auto scanning all active computer modules (Autoskip)</i> on page 176 ff.).

Message	Meaning
STEPSCAN	The console module uses the stepscan function and the keys to scan the computer modules manually are active (see <i>Scanning computer modules manually (Stepscan)</i> on page 177 ff.).
HDCP content suppressed	The connected computer module has detected HDCP- protected image data that may not be displayed.
Frozen for	When using freeze mode, the image last received is either highlighted by a coloured frame and/or the note Frozen and the time past since the loss of connection (see <i>Freeze</i> <i>mode</i> on page 201 ff.)
Please reconnect	A disconnection has been detected. Check the cables.
Communication was interrupted Auto-switched to channel	A CON-2 console module was automatically switched to the specified channel due to a connection failure.
Stream CPU	Index of the displayed video stream when switching of the video stream (when connected to a DH computer module)
Illegal format	Problem with video parameters: Incorrect data format
Pixel clock too high	Problem with video parameters: Pixel clock higher than supported by the current console module
Resolution too high	Problem with video parameters: Image width or image hight greater than supported by the current console module
Pixel clock too low	Problem with video parameters: Pixel clock below the minimum clock rate
Resolution too low	Problem with video parameters: Image width or image height less than required for output
Invalid parameter	Problem with video parameters: Image parameters inconsistent or incorrect
No AV-stream received	The reception of AV data is configured. However, no AV data is received.

Ν	Λ	F?		٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	۰	٠	٠	٠	٠	٠	٠
				٠	٠	٠	۰	۰	٠	٠	٠	۰	۰	۰	٠	۰	۰	٠	۰	۰	۰	٠	٥
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
•	•	•	•	•			•			•	•					•						•	•
•				•					•	•	•		٠		•	•	•			•		•	0
•				•												٠							•
•	•	•	•	•			٠					٠				٠		٠				•	
•	٠	٠	•	٠	•		۰		٠	٠	٠					٠		٠				٠	•
٠	٠	٠	٠	٠	•	٠	٠	•	٠	٠	٠	٠	٠	•	٠	٠	٠	٠	٠	٠	•	٠	٠
٠	٠	٠	٠	٠	•	٠	٠	•	٠	٠	٠	۰	۰	•	٠	٠	٠	۰	٠	٠	•	٠	۰
۰	٠	٠	۰	٠	٠	٠	۰	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	۰	٠	٠	٠	٠	۰
٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	۰
٠	٠	٠	٠	٠	•	۰	٠	•	٠	٠	٠	۰	۰	•	٠	٠	٠	٠	٠	٠	•	٠	۰
٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	۰
٠	۰	*	•	٠	٠	•	٠	٠	٠	٠	٠	۰	۰	٠	٠	٠	۰	٠	۰	٠	٠	٠	۰
•			•	•			•			•	•				•							•	•
•	•	•	•	•						•	•					•						•	•
•	•	•	•	•	•					•	•				•	•						٠	
•	•	•	•	•			۰			٠												٠	
٠	٠	٠	٠	٠	٠	٠	۰	٠	٠	۰	۰	۰	۰	٠	٠	٠	٠	۰	٠	٠	٠	٠	٠
٠	٠	•	٠	٠	•	٠	٠	•	٠	٠	٠	٠	٠	•	•	٠	٠	٠	٠	٠	•	•	٠
٠	٠	٠	٠	٠	•	٠	٠	•	٠	٠	٠	۰	۰	•	•	٠	٠	٠	٠	٠	•	٠	٠
۰	٠	٠	۰	٠	٠	٠	۰	٠	٠	۰	۰	۰	٠	٠	٠	٠	٠	۰	٠	٠	٠	٠	۰
۰	٠	٠	۰	٠	٠	٠	۰	٠	٠	٠	٠	٠	٠	•	٠	٠	٠	۰	•	•	•	٠	۰
٠	۰	٠	٠	•	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	۰
٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	•	٠	٠	٠	٠	٠	٠	٠	۰
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
				•	•			•	•				•	•	•	•	•		•	•	•	•	•
•	•	•	•	•	•			•		•	•			•	•	•					•	•	•
•				•	•			•						•	•	•	•			•	•	٠	•
•		•	•	•			۰			٠	٠											٠	•



G&D. FEELS RIGHT.

Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

Obere Leimbach 9 | D-57074 Siegen | Germany Phone +49 271 23872-0 sales@gdsys.com | www.gdsys.com US-Bùro | US-Office G&D North America Inc. 4540 Kendrick Plaza Drive, Suite 100 | Houston, TX 77032 | USA Phone 1-346-620-4362 sales.us@gdsys.com | www.gdsys.com