



G&D RemoteAccess-IP-CPU

EN Web Application »Config Panel«
Configuring the device



G&D Config Panel 21

RemoteAccess-IP-CPU-Fiber | RACPU 0000005E

EN



Tools



System

Configuration



RemoteGateways



Users



User groups

Status



Information



System monitoring

Home

RemoteGateways

Search... X

1 Devices



<input checked="" type="checkbox"/>	Name ^	Device type	Comment	Monitoring overview	
<input checked="" type="checkbox"/>	RACPU 0000005E ⓘ	RemoteAccess-IP-CPU-Fiber		OK	

Service tools ^



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 2023. All rights reserved.

Version 1.10 – 11/07/2023

Config Panel 21 version: 1.5.007

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

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

www.gdsys.com
sales@gdsys.com

Table of contents

Chapter 1: Basic functions

Introduction	1
System requirements	2
Supported operating systems	2
Recommended resolutions	2
Initial configuration of the network settings	3
Getting started	4
Starting the web application	4
Operating the web application	5
User interface	5
Frequently used buttons	7
Configuring table columns	7
Language settings	9
Selecting the language of the web application	9
Selecting the system language	9
Showing the version number of the web application	10
Closing the web application	10
Basic configuration of the web application	11
Network settings	11
Configuring the network settings	11
Configuring global network settings	12
Reading out the status of the network interfaces	13
Creating and administrating netfilter rules	14
Creating new netfilter rules	14
Editing existing netfilter rules	15
Deleting existing netfilter rules	17
Changing the order or priority of existing netfilter rules	17
Creating an SSL certificate	18
Special features for complex KVM systems	18
Creating a Certificate Authority	18
Creating any certificate	20
Creating and signing an X509 certificate	21
Creating a PEM file	21
Selecting an SSL certificate	22
Firmware update	24
Firmware update of the device	24
Restoring the system defaults	25
Restarting the device	25

Network functions of the devices	26
NTP server	26
Time sync with an NTP server.....	26
Manual setting of time and date.....	27
Logging syslog messages	28
Local logging of syslog messages	28
Sending syslog messages to a server	29
Viewing and saving local syslog messages	30
User authentication with directory services	30
Setting up two-factor authentication on the device	33
Monitoring functions	35
Viewing all monitoring values	35
Enabling/disabling monitoring values	36
Advanced features for managing critical devices	37
Displaying the list of critical monitoring values	37
Confirm the alarm of a critical device	37
Users and groups	38
Efficient rights administration	38
The effective right	38
Efficient user group administration	39
Administrating user accounts	39
Creating a new user account	40
Activating two-factor authentication	41
Renaming a user account	44
Changing the password of a user account.....	44
Changing the user account rights	45
Changing a user account's group membership.....	46
Enabling or disabling a user account	47
Deleting a user account	47
Administrating user groups	48
Creating a new user group.....	48
Renaming a user group	49
Changing the user group rights	49
Administrating user group members	50
(De)activating a user group.....	50
Deleting a user group	50
System rights	51
Rights for unrestricted access to the system (Superuser)	51
Changing the login right to the web application.....	51
Rights to change your own password	52
Authorization to confirm a monitoring alarm.....	52

Advanced functions of the KVM system	53
Identifying a device by activating the Identification LED	53
Saving the configurations	53
Saving the configurations with auto backup function	54
Restoring the configurations	56
Activating premium functions	57
 Chapter 2: RemoteGateways	
Basic configuration of RemoteGateways	58
Changing the name of a RemoteGateway	58
Changing the comment of a RemoteGateway	58
Establishing a KVM-over-IP™ connection 59	
Configuring a KVM-over-IP connection	60
Configuring the network interface	60
Configuring the global network settings	61
Configuring a KVM-over-IP connection	62
Extended settings of KVM-over-IP connection	63
Limiting the bandwidth	63
Classifying IP packets (DiffServ)	64
(De)Activating signals	65
Resetting the KVM-over-IP connection of the computer module	65
Restricting KVM-over-IP remote stations (UID locking)	66
Advanced features for RemoteGateways	67
Copying the config settings (Replace device)	67
Configuring monitoring values	68
Selecting the values to be monitored	68
Viewing status information of a device	68

1 Basic functions

Introduction

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

IMPORTANT: When operating the devices, refer to the manual of the matrix switch.

System requirements

IMPORTANT: Before the web application can be started via the web browser of a computer, the device from which the web application is loaded must first be connected to the local network. The *Installation* manual of the device provides more information.

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

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

- Apple Safari 16
- Google Chrome 114
- Microsoft Edge 114
- Mozilla Firefox 114

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 the *network interface* » *Network (Management)* «: **192.168.0.1**
- 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 5e (or better) twisted pair cable to connect the network interface of any computer to the device's *network interface Network (Management)*.
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 (see *Network settings* on page 11 ff.) f.
6. Remove the twisted pair cable connection between computer and device.
7. Implement the device in the local network.

Getting started

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

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

Starting the web application

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

How to start the web application

1. Enter the following URL in the address line:

https://[IP address of the device]

2. Enter the following data in the login mask:

Username:	Enter a username.
Password:	Enter a password for your user account.
One-time password:	Enter a one-time password from two-factor authentication.

NOTE: The one-time password is only requested if two-factor authentication has been configured (see page 33 f.) and activated (see page 41 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 44).

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

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

3. Click on **Login**.

Operating the web application

User interface

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

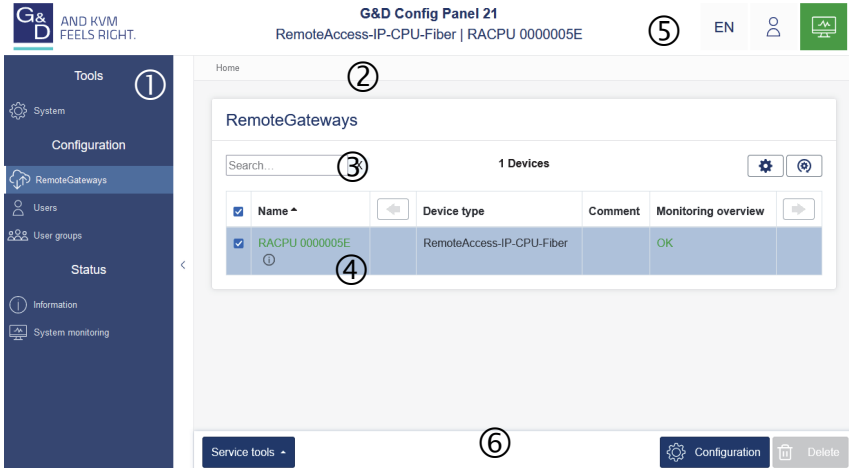


Figure 1: User interface of the web application

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

Menu ①:	In the menu the different functions of the web application are summarised in various topics.
Breadcrumb navigation ②:	<p>The breadcrumb navigation shows you the path to the currently opened dialog.</p> <p>To quickly return to a higher-level dialog, you can click on it in the breadcrumb navigation.</p>
Filter function ③:	<p>You can use the filter function to narrow down the items displayed in the main view.</p> <p>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.</p> <p>To delete the filter, click on the [X] icon.</p>
Main view ④:	After selecting a topic in the menu, the contents of this topic are displayed here.

Shortcuts ⑤:

Language selection: The language identifier (for example **EN** for *English*) shows the currently active language in the web application.

To switch the language, click the language identifier. This opens a submenu that shows the supported languages and the corresponding identifiers.

Switch the language by clicking on the desired language.

User: A click on the user icon opens a submenu:

- The name of the active user is displayed in the submenu.
- Click on *User* to access the user settings of the active user.
- Click on *Logout* to exit the active session.

Monitoring status: This icon shows you at a glance whether all monitoring values are within the normal range (green icon) or if at least one monitoring value is outside the normal range (yellow or red icon).

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

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

Buttons ⑥:

Depending on the dialog shown, different buttons are displayed in this area.

Frequently used buttons

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

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

Configuring table columns

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

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

RemoteGateways

Search... X		1 Devices		⚙️ ⌛	
<input checked="" type="checkbox"/>	Name ^	⬅️	Device type	Monitoring overview	➡️
<input checked="" type="checkbox"/>	RACPU 0000005E ①		RemoteAccess-IP-CPU-Fiber	OK	

Figure 2: Table columns (selection) of a RemoteGateway

How to change the columns to be displayed:

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

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



Figure 3: Table configuration

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

A rectangular button with a light gray background. Inside the button, the letters 'EN' are displayed in a blue, sans-serif font.

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

Selecting the system language

The specified system language is assigned to all user accounts by default. **How to set the system language:**

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

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 *RemoteAccess-IP-CPU* devices are equipped with two network interfaces:

- **Network interface *Interface A*:** This interface is used for the connection of the virtual machines.
- **Transmission:** This interface is used for signal transmission between the target module and the IP matrix switch.

NOTE: Access to the device's web application and advanced network functions (network filter, syslog...) is possible via both interfaces.

IMPORTANT: Please mind the separate instructions regarding *Initial configuration of the network settings* on page 3.

Configuring the network settings

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

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

- IP address of *network* interface *Interface A*: **192.168.0.1**
- IP address of the *Transmission* interface address is obtained via **DHCP** (fallback: IP address **172.17.0.10**)
- global network settings: settings obtained using **DHCP**

How to configure the settings of a network interface:

IMPORTANT: It is not possible to use both network interfaces within the same sub-net.

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 **RemoteGateways**.
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. Use **Interface A** or **Transmission** paragraphs to enter the following data:

Operational mode:	Use the pull-down menu to select the operating mode: <ul style="list-style-type: none"> ▪ Off: switches off network interface. ▪ Static: uses static settings. ▪ DHCP: obtains the settings from a DHCP server.
IP address:	Only if the <i>Static</i> operating mode is selected: Enter the interface IP address.
Netmask:	Only if the <i>Static</i> operating mode is selected: Enter the network netmask.

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 **RemoteGateways**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Now go to **Global settings**.
5. Enter the following values and click **Save** afterwards:

Operating mode:	Select the operating mode: <ul style="list-style-type: none"> ▪ Static: Use 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 hostname 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 gateway's IP address.
DNS server 1:	Enter the IP address of the DNS server.
DNS server 2:	Optionally, enter the IP address of another DNS server.

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 **RemoteGateways**.
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 **Transmission** and **Interface A** include the following values:

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

6. Click on **Close**.

Creating and administrating netfilter rules

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

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

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

Creating new netfilter rules

How to create a new netfilter rule:

1. In the menu, click on **RemoteGateways**.
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: <ul style="list-style-type: none">▪ All▪ Transmission▪ Interface A
Option:	In the pull-down menu, select how to interpret the sender information of the rule: <ul style="list-style-type: none">▪ 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:	<p>Enter the IP address of the data packets or - by using the Net-mask field - the address space of the IP addresses.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ 192.168.150.187: for IP address 192.168.150.187 ▪ 192.168.150.0/24: IP addresses of section 192.168.150.x ▪ 192.168.0.0/16: IP addresses of section 192.168.x.x ▪ 192.0.0.0/8: IP addresses of section 192.x.x.x ▪ 0.0.0.0/0: all IP addresses
<p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p>	
MAC address:	Enter the MAC address to be considered in this filter rule.
<p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p>	
Filter rule:	<ul style="list-style-type: none"> ▪ Drop: Data packets whose sender information matches the IP address or MAC address are not processed. ▪ Accept: Data packets whose sender information matches the IP address or MAC address are processed.
Service:	Select a specific service for which this rule is used exclusively, or choose (All) .

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

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

7. Click on **Save**.

NOTE: The new netfilter 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 **RemoteGateways**.
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:	<p>In the pull-down menu, select on which network interfaces the data packets are to be intercepted and manipulated:</p> <ul style="list-style-type: none"> ▪ All ▪ Transmission ▪ Interface A
Option:	<p>In the pull-down menu, select how to interpret the sender information of the rule:</p> <ul style="list-style-type: none"> ▪ 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::	<p>Enter the IP address of the data packets or - by using the Net-mask field - the address space of the IP addresses.</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ 192.168.150.187: for IP address 192.168.150.187 ▪ 192.168.150.0/24: IP addresses of section 192.168.150.x ▪ 192.168.0.0/16: IP addresses of section 192.168.x.x ▪ 192.0.0.0/8: IP addresses of section 192.x.x.x ▪ 0.0.0.0/0: all IP addresses <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p> </div>
MAC address:	<p>Enter the MAC address to be considered in this filter rule.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: The <i>IP address</i> and/or a <i>MAC address</i> can be specified within a rule.</p> </div>
Filter rule:	<ul style="list-style-type: none"> ▪ Drop: Data packets whose sender information 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:	<p>Select a specific service for which this rule is used exclusively, or choose (All).</p>

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

NOTE: The new netfilter 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 **RemoteGateways**.
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 **RemoteGateways**.
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 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 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 18) must be used when creating certificates for these devices.

Alternatively, the identical PEM file (see page 21) 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**:

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

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

How to create the Certificate Authority:

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

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

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

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

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

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

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

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

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

Creating any certificate

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

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

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

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

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

How to create the certificate request:

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

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

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

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

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

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

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

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

Creating and signing an X509 certificate

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

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

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

Creating a PEM file

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

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

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

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

- a. Linux

```
cat server.crt > gdc.d.pem  
cat server.key >> gdc.d.pem  
cat ca.crt >> gdc.d.pem
```

- b. Windows

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

2. The *gdc.d.pem* file is created 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 18).

How to select the SSL certificate you want to use:

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

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

5. Select the certificate you want to use:

G&D certificate #1: This certificate is enabled for *new* devices.

NOTE: Make sure that you use the same certificate for all devices within the KVM system.

G&D certificate #2: This certificate is supported by some older G&D devices with integrated web application.

User certificate: Select this option if you want to use a certificate purchased from a certificate authority or if you want to use a user certificate.

Now you can import and upload the certificate:

1. Click on **Import certificate from file** and use the file dialog to select the .pem file you want to import.

You can also copy the plain text of the server certificate, the server's private key and the certificate of the certificate authority to the text box.

2. Click on **Upload and activate** to store and activate the imported certificate for the device.

6. Click on **Save**.

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.

Firmware update

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

Firmware update of the 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 the device:

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

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

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

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

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

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

IMPORTANT: Do **not** close the browser session while the device is being updated! Do **not** turn off the device or disconnect it 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 **RemoteGateways**.
2. Click on the desired device.
3. Open the menu **Service tools** and select the entry **Restart**.
4. Confirm the confirmation prompt with **Yes**.

Network functions of the devices

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

The following functions can be configured for the **RemoteAccess-CPU**:

- Authentication against directory services (LDAP, Active Directory, RADIUS, TACACS+)
- Time synchronisation via NTP server
- Forwarding of log messages to syslog servers

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 **RemoteGateways**.
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **Network**.
4. Go to the paragraph **NTP server** and enter the following values:

NTP time sync:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the the time synchronization: <ul style="list-style-type: none">▪ Disabled (<i>default</i>)▪ Enabled
NTP server 1:	Enter the IP address of a time server.
NTP server 2:	<i>Optionally</i> enter the IP address of a second time server.
Time zone:	Use the pull-down menu to select the time zone of your location.

5. Click 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 **RemoteGateways**.
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.

Local logging of syslog messages

How to locally log syslog messages:

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

Syslog local:	By selecting the corresponding entry in the pull-down menu, you can enable or disable the local logging of syslog messages: <ul style="list-style-type: none"> ▪ Disabled ▪ Enabled (<i>default</i>)
Log level:	In this pull-down menu, select the severity from which a log message is to be logged. The selected severity and all lower severity levels are logged.
<div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> If you select the severity 2 - <i>Critical</i>, messages for this code as well as for the severity levels 1 - <i>Alert</i> and 0 - <i>Emergency</i> are logged. </div>	

5. Click on **Save**.

Sending syslog messages to a server

How to send syslog messages to a server:

1. In the menu, click on **RemoteGateways**.
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: <ul style="list-style-type: none"> ▪ 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. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> If you select the severity 2 - <i>Critical</i>, messages for this code as well as for the severity levels 1 - <i>Alert</i> and 0 - <i>Emergency</i> are logged. </div>
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: <ul style="list-style-type: none"> ▪ 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 **RemoteGateways**.
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* on page 33), 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 **RemoteGateways**.
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 names can be subject to a naming convention when using external directory services (see *Creating a new user account* on page 40).

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

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

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

IMPORTANT: When using two-factor authentication, the fallback mechanism **cannot** be used (see *Setting up two-factor authentication on the device* on page 33).

6. Click on **Save**.

Setting up two-factor authentication on the device

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

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

IMPORTANT: If you no longer have access to your possession-based factor or if it is broken, you will lose access to the system. Take precautions by, for example, keeping the emergency codes in a safe place if you are using the internal OTP server and configuring settings that will minimise the risk of losing access (see *Activating two-factor authentication* on page 41).

How to activate 2FA on the device:

1. In the menu, click on **RemoteGateways**.
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:	<ul style="list-style-type: none"> ▪ Disabled (<i>default</i>) ▪ Enabled
OTP server:	<p>Select the option Internal (<i>default</i>), if you will be using an authentication server that is provided in the device.</p> <p>If you want to use a specific external directory service, select the corresponding entry from the pull-down menu:</p> <ul style="list-style-type: none"> ▪ LDAP ▪ Active Directory ▪ Radius ▪ TACACS+ <p>Once you have selected a directory service, enter the settings for the directory service server in the dialogue screen that opens.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: Note that usernames may be subject to a naming convention if a directory service is used (see <i>Creating a new user account</i> on page 40).</p> </div>
Login only for users with configured 2FA:	<p>If the internal OTP server is used, you can specify whether login for users without activated 2FA will be permitted (<i>default</i>) or prevented. This option can be used to set up a transition period for setting up the OTPs, for example.</p> <ul style="list-style-type: none"> ▪ No (<i>default</i>) ▪ Yes <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>IMPORTANT: If an external directory service is used, the second factor will be required for every user profile on login.</p> </div>

6. Click on **Save**.

IMPORTANT: Use time sync with an NTP server (see page 26). Alternatively, you can set the time and date manually (see page 27).

Information on activating two-factor authentication is provided on page 41.

Monitoring functions

Viewing all monitoring values

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

How to show a list of all monitoring values:

1. In the menu, click on **RemoteGateways**.
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.

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

1. In the menu, click on **RemoteGateways**.
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 **RemoteGateways**.
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 5) 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**.

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 *TargetConfig*.

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

Right	User <i>JDoe</i>	Group <i>Office</i>	Group <i>TargetConfig</i>	Effective right
Config Panel Login	No	No	Yes	Yes
Change own password	No	Yes	No	Yes

The settings of the *Config Panel Login* and *Change own password* rights result from the rights assigned to the user groups.

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.

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

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

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

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

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

Administering 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.

Creating a new user account

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

How to create a new user account:

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

Name:	Enter a user name.
NOTE: User names can be subject to a naming convention when using external directory services (see <i>User authentication with directory services</i> on page 30 ff.).	
Password:	Enter the user account password.
Confirm password:	Repeat the password.
Clear text:	If necessary, mark this entry to view and check both passwords.
Full name:	If desired, enter the user's full name.
Comment:	If desired, enter a comment regarding the user account.
Enabled:	Mark this checkbox to activate the user account.
NOTE: If the user account is deactivated, the user is not able to access the KVM system.	

4. Click on **Save**.

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

5. If two-factor authentication is activated on the device (see page 33), the settings for the user account must be made in the next step (see page 41).

Activating two-factor authentication

NOTE: To use two-factor authentication, it first needs to be set up on the device (see page 33).

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* on page 33 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 super-user rights (see page 51), or the user must be logged in with the corresponding user profile (see page 51) and have the right *Change own password* (see page 52).

IMPORTANT: Use time sync with an NTP server (see page 26). Alternatively, you can set the time and date manually (see page 27).

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

How to activate 2FA in the user account:

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

5. Enter the following data in the menu:

Encryption key:	When the parameter 2FA for this user is changed from Disabled to Enabled , a encryption key is generated and displayed automatically.
<div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> IMPORTANT: Base32 format must be used for the entry. </div>	
Click on Generate to obtain a new encryption key.	
Hash algorithm:	<ul style="list-style-type: none"> ▪ SHA1 ▪ SHA256 (<i>default</i>) ▪ SHA512
Validity period (secs):	Enter how long the one-time password should remain valid. The value entered must be between 10 and 200 seconds (<i>default</i> : 30 seconds).
<div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> ADVICE: It is a good idea to avoid selecting a validity period that is too short, as access problems could otherwise occur if the time is not synchronised correctly. </div>	
Length of OTP:	<ul style="list-style-type: none"> ▪ 6 digits (<i>default</i>) ▪ 8 digits
OTP window width:	The window width specifies how many previous one-time passwords are valid in addition to the current one. It is not possible to allow future one-time passwords. The value entered must be between 1 and 20 (<i>default</i> : 1).
<div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> ADVICE: To avoid access problems from occurring as the result of the time not being synchronised correctly, it can be a good idea to permit several previous one-time passwords. </div>	
Show QR code & copy security key:	Clicking the button validates the entries that have been made. A security key is generated and a QR code is displayed that contains the generated security key and that can be used to scan in with an authenticator app. The security key is copied to the clipboard.
Verification code:	Enter a verification code here that you receive from a hardware token or an authenticator app that you are using. Only numbers can be entered in this field.

6. Click on **Save**.

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

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

NOTE: A user who has been successfully authenticated against the directory service but who does not have an account with the same name in the database of the KVM system will be given the rights of the user *RemoteAuth*. The OTP 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 45).

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 47).

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

Renaming a user account

How to change the name of a user account:

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

NOTE: User names can be subject to a naming convention when using external directory services (see *User authentication with directory services* on page 30 ff.).

Changing the password of a user account

NOTE: The activated *Superuser* right
(see *Rights for unrestricted access to the system (Superuser)* on page 51 ff.)
or the right *Change own password*
(see *Rights to change your own password* on page 52 ff.)
are prerequisite for changing the password of a user 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:

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

4. Click on **Save**.

Changing the user account rights

Any user account can be assigned with different rights.

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

Name	Right	Page
Change own password	Change own password	page 52
Superuser right	Unrestricted access to the configuration of the system	page 51
Config Panel Login	Login to the <i>ConfigPanel</i> web application	page 51
Confirm monitoring alert	Confirmation of a monitoring alarm	page 52

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

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

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

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

6. Click on **Save**.

Enabling or disabling a user account

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

How to enable or disable a user account:

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

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

4. Click on **Save**.

Deleting a user account

How to delete a user account:

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

Administrating user groups

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

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

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

Creating a new user group

The user can create up to 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 table lists the different user rights. Further information about the rights is given on the indicated pages.

Name	Right	Page
Change own password	Change own password	page 52
Superuser right	Unrestricted access to the configuration of the system	page 51
Config Panel Login	Login to the <i>ConfigPanel</i> web application	page 51
Confirm monitoring alert	Confirmation of a monitoring alarm	page 52

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

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

5. Click on **Save**.

Changing the login right to the web application

How to change the login right to the web application:

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

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

5. Click on **Save**.

Rights to change your own password

How to change the right to change your own password:

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

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

5. Click on **Save**.

Advanced functions of the KVM system

Identifying a device by activating the Identification LED

Some devices provide an *Identification* LED.

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

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

1. In the menu, click on **RemoteGateways**.
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 device:

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: <ul style="list-style-type: none"> ▪ Disabled (<i>default</i>) ▪ Enabled
Filename prefix:	Enter the filename prefix. ADVICE: When the auto backup function is enabled, the filename prefix field is automatically filled with the UID of the device. You can change this entry. IMPORTANT: Only letters (upper and lower case), numbers (0 to 9) and the characters - and _ are permitted. The prefix may contain a maximum of 25 characters.
Backup password:	<i>Optional:</i> 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: <ul style="list-style-type: none"> ▪ NFS: <i>name:/directory1/directory2</i> ▪ CIFS: <i>//name/directory1/directory2</i>
Protocol:	Choose between the following protocols: <ul style="list-style-type: none"> ▪ NFS (<i>default</i>) ▪ CIFS
Port:	Enter the port. This field is filled automatically depending on the selection in the <i>protocol</i> field: <ul style="list-style-type: none"> ▪ 2049 (when selected <i>NFS</i>) ▪ 445 (when selected <i>CIFS</i>)

User:	<i>Optional:</i> Enter the name of the user.
Password:	<i>Optional:</i> Enter a password to secure the share.
Time:	Enter the following data: <ul style="list-style-type: none"> ▪ Hour (numbers 0 to 23) ▪ Minute (numbers 0 to 59)
Selection of the day:	You can choose between the following options: <ul style="list-style-type: none"> ▪ 1. to 31. day of the month ▪ Select all (every day of the month)

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

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

IMPORTANT: 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 device:

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

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

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

7. Click **Restore**.

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

Activating premium functions

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

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

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

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

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

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

5. Click on **Save**.

2 RemoteGateways

You can configure the settings of the RemoteGateway and view the device's status information in the web application's *RemoteGateways* menu.

Basic configuration of RemoteGateways

Changing the name of a RemoteGateway

How to change the name of a RemoteGateway:

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

Changing the comment of a RemoteGateway

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

ADVICE: For example, use the comment field to note the location of the RemoteGateway.

How to change the comment of a RemoteGateway:

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

Establishing a KVM-over-IP™ connection

G&D's **KVM-over-IP™** technology makes it possible to transmit signals between the computer module and the IP matrix switch using a Gigabit Ethernet (layer 3).

NOTE: The **Transmission** interface of the computer module is used for signal transmission between the target module and the IP matrix switch.

The **Network** interface *Interface A* is used for communication with the virtual computers.

Access to the device's web application is possible via both interfaces.

Only after the initial setup of the KVM-over-IP™ connection between the target module and the IP matrix switch can the target module be used with the IP matrix switch.

By default, the following setting of the *Transmission* interface is preselected:

- IP address of the *Transmission* interface:
Obtain address via **DHCP** (Fallback: IP address:172.17.0.10)

By default, the following setting of the *Network* interface is preselected:

- IP address of the *Network* interface *Interface A*: 192.168.0.1

Configuring a KVM-over-IP connection

Configuring the network interface

How to configure the settings of a network interface:

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

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

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **Network**.
5. Go to the paragraph **Interfaces**.
6. Use **Interface A** or **Transmission** paragraphs to enter the following data:

Operational mode:	Use the pull-down menu to select the operating mode: <ul style="list-style-type: none">▪ Off: switches off network interface.▪ Static: uses static settings.▪ DHCP: obtains the settings from a DHCP server.
IP address:	Only if the <i>Static</i> operating mode is selected: Enter the interface IP address.
Netmask:	Only if the <i>Static</i> operating mode is selected: Enter the network netmask.

7. Click on **Save**.

Configuring the global network settings

Even in complex networks global network settings ensure that the device is available from all partial networks.

How to configure the global network settings:

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **Network**.
5. Now go to **Global settings**.
6. Enter the following values:

Operating mode:	Select the operating mode: <ul style="list-style-type: none"> ▪ Static: Use static settings. ▪ DHCP: Obtain settings from a DHCP server.
NOTE: When selecting the <i>DHCP</i> mode, the following settings are applied automatically. It is not possible to enter any vlaues.	
Hostname:	Enter the device's hostname.
Domain:	Enter the domain to which the device should belong.
Gateway:	Enter the gateway's IP address.
DNS server 1:	Enter the IP address of the DNS server.
DNS server 2:	Optionally, enter the IP address of another DNS server.

7. Click on **Save**.

Configuring a KVM-over-IP connection

How to configure a KVM-over-IP connection:

1. Start the web application of **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Enter the following data under **Configuration**:

Control port:	Enter the number of the port you want to use.
Communication port:	Enter the number of the port you want to use.
Data port:	Enter the number of the port you want to use.

6. 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 the same certificate!

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>Creating an SSL certificate</i> on page 18).
Activated, separate certificate:	<p>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 18).</p> <p>Click Upload certificate and select the .pem file to import in the file dialog. Click Upload and activate to save and activate the certificate.</p>

7. Click on **Save**.

Extended settings of KVM-over-IP connection

Limiting the bandwidth

By default, the device uses the maximum available bandwidth of a Gigabit Ethernet. 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. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Under **Max. bandwidth** in the **Connection Settings** section you can set the bandwidth limit of a KVM-over-IP connection in MBit/sec.

NOTE: Entering the value 0 deactivates the limit.

6. Click on **Save**.

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.

You can define a DSCP for the IP packets of the keyboard, mouse and control data (**Communication** data packets), as well as the IP packets of the video, audio and RS232 data (**Data** data packets).

How to configure the DSCPs of the IP data packets:

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Enter the following data under **Connection settings**:

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

DiffServ Data:	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 service class Network Control (DSCP name: CS6) for <i>all</i> data packets. In such environments, the DSCP 48 option must not be selected!

6. Click on **Save**.

(De)Activating signals

By default, the device transfers not only keyboard, video and mouse data but also audio data .

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

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Enter the following data under **Deactivatable signals**:

Audio:	Select Enabled or Disabled .
---------------	--

6. Click on **Save**.

Resetting the KVM-over-IP connection of the computer module

A computer module connected to an IP matrix *permanently* stores the pairing data of the IP matrix.

How to delete the pairing data of the computer module

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Under **Remote**, click on **Reset connection**.

Restricting KVM-over-IP remote stations (UID locking)

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

TIPP: Activate the function **UID locking** if you want to *specify* which IP matrix switches should be able to connect to the computer module.

How to enable/disable UID locking:

1. Start the web application of the **computer module**.
2. In the menu, click on **RemoteGateways**.
3. Click on the computer module and then click on **Configuration**.
4. Click on the tab **KVM connection**.
5. Enter your setting in the paragraph **UID locking**:

UID locking:	Only the remote stations specified in the list may establish a KVM-over-IP connection (Enabled), or all remote stations 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 computer module.
Add IP matrix:	Click this button and enter the UID of the IP matrix that is allowed to connect to this computer module. Click on Save .
Remove:	Click on a permitted IP matrix and then on Remove to revoke the permission.

6. Click on **Save**.

Advanced features for RemoteGateways

Copying the config settings (Replace device)

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

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

How to copy target module config settings:

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

Configuring monitoring values

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

Selecting the values to be monitored

By default, the KVM system monitors a variety of device's values.

If required, you can limit the evaluation and monitoring of properties.

How to manage the values to be monitored:

1. In the menu, click on **RemoteGateways**.
2. Click on the computer module you want to configure and then click on **Configuration**.
3. Click on **Monitoring**.
4. Enable or disable individual monitoring values by sliding the slider to the *left* (**off**) or to the *right* (**on**).

<p>NOTE: In order to enable or disable <i>all</i> values you can use the check box in the header of the Enabled column.</p>

5. Click on **Save**.

Viewing status information of a device

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

How to view the status information

1. In the menu, click on **RemoteGateways**.
2. Click on the computer module you want to configure and then click on **Configuration**.
3. Click on **Information**.

4. The following information is displayed in the dialog box that opens now:

RemoteGateways	
Name:	Name of the device
Device ID:	Physical ID of the device
Status:	Current status (online or offline) of the device
Class:	Device class
Hardware information	
Firmware name:	Firmware name
Firmware rev.:	Firmware version
Hardware rev.:	Hardware revision
IP address Network:	IP address of <i>Network</i> interface
IP address Transmission:	IP address of <i>Transmission</i> interface
MAC Network:	MAC address of <i>Network</i> interface
MAC Transmission:	MAC address of <i>Transmission</i> interface
Serial number	Serial number of the device
Active features	
This area lists all activated additional functions.	
Link status	
Link detected:	Connection to the network established (yes) or interrupted (no).
Auto-negotiation:	The transmission speed and the duplex method have been configured automatically (yes) or manually by the administrator(no).
Speed:	Transmission speed
Duplex	Duplex method (full or half)
NOTE: In addition, the <i>monitoring</i> information of the device is displayed.	

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

NOTES



G&D. AND KVM FEELS RIGHT.

Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

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

US-Büro | US-Office

G&D North America Inc.

4001 W. Alemda Avenue | Suite 100, Burbank, CA 91505 | Phone +1-818-748-3383
sales.us@gdsys.com | www.gdsys.com