



# G&D RemoteAccess-CPU

DE Webapplikation »Config Panel«  
Konfiguration des Geräts



**AND KVM  
FEELS RIGHT.**

**G&D Config Panel 21**  
RemoteAccess-CPU-Fiber | RACPU 000000C8

DE





**Tools**  
System  
**Konfiguration**  
RemoteGateways  
Benutzer  
Benutzerguppen  
**Status**  
Informationen  
Systemüberwachung

Home / RemoteGateways

**RemoteGateways**

Suche... X

1 Geräte



| <input checked="" type="checkbox"/> | Name ^              | Gerätetyp              | Kommentar | Monitoring overview |  |
|-------------------------------------|---------------------|------------------------|-----------|---------------------|--------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | RACPU 000000C8<br>① | RemoteAccess-CPU-Fiber |           | OK                  |                                                                                      |

Service-Werkzeuge ^

Konfiguration

Löschen

---

## **Zu dieser Dokumentation**

Diese Dokumentation wurde mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft.

Für die Qualität, Leistungsfähigkeit sowie Marktgängigkeit des G&D-Produkts zu einem bestimmten Zweck, der von dem durch die Produktbeschreibung abgedeckten Leistungsumfang abweicht, übernimmt G&D weder ausdrücklich noch stillschweigend die Gewähr oder Verantwortung.

Für Schäden, die sich direkt oder indirekt aus dem Gebrauch der Dokumentation ergeben, sowie für beiläufige Schäden oder Folgeschäden ist G&D nur im Falle des Vorsatzes oder der groben Fahrlässigkeit verantwortlich.

## **Gewährleistungsausschluss**

G&D übernimmt keine Gewährleistung für Geräte, die

- nicht bestimmungsgemäß eingesetzt wurden.
- nicht autorisiert repariert oder modifiziert wurden.
- schwere äußere Beschädigungen aufweisen, welche nicht bei Lieferungserhalt angezeigt wurden.
- durch Fremdzubehör beschädigt wurden.

G&D haftet nicht für Folgeschäden jeglicher Art, die möglicherweise durch den Einsatz der Produkte entstehen können.

## **Warenzeichennachweis**

Alle Produkt- und Markennamen, die in diesem Handbuch oder in den übrigen Dokumentationen zu Ihrem G&D-Produkt genannt werden, sind Warenzeichen oder eingetragene Warenzeichen der entsprechenden Rechtsinhaber.

## **Impressum**

© Guntermann & Drunck GmbH 2023. Alle Rechte vorbehalten.

**Version 1.10 – 10.08.2023**

Config Panel 21-Version: 1.5.007

Guntermann & Drunck GmbH

Obere Leimbach 9

57074 Siegen

Germany

Telefon +49 (0) 271 23872-0

Telefax +49 (0) 271 23872-120

[www.gdsys.com](http://www.gdsys.com)

[sales@gdsys.com](mailto:sales@gdsys.com)

# Inhaltsverzeichnis

## Kapitel 1: Grundfunktionen

|                                                        |           |
|--------------------------------------------------------|-----------|
| <b>Einleitung</b>                                      | <b>1</b>  |
| <b>Systemvoraussetzungen</b>                           | <b>2</b>  |
| Unterstützte Betriebssysteme                           | 2         |
| Empfohlene Grafikauflösungen                           | 2         |
| <b>Erstkonfiguration der Netzwerkeinstellungen</b>     | <b>3</b>  |
| <b>Erste Schritte</b>                                  | <b>4</b>  |
| Start der Webapplikation                               | 4         |
| Bedienung der Webapplikation                           | 5         |
| Die Benutzeroberfläche                                 | 5         |
| Häufig verwendete Schaltflächen                        | 7         |
| Tabellenspalten konfigurieren                          | 7         |
| Spracheinstellungen                                    | 9         |
| Sprache der Webapplikation auswählen                   | 9         |
| Systemsprache auswählen                                | 9         |
| Versionsnummer der Webapplikation anzeigen             | 10        |
| Webapplikation beenden                                 | 10        |
| <b>Grundkonfiguration der Webapplikation</b>           | <b>11</b> |
| Netzwerkeinstellungen                                  | 11        |
| Konfiguration der Netzwerkschnittstelle                | 11        |
| Konfiguration der globalen Netzwerkeinstellungen       | 12        |
| Status der Netzwerkschnittstelle auslesen              | 13        |
| Netzfilterregeln einrichten und administrieren         | 14        |
| Neue Netzfilterregel erstellen                         | 14        |
| Bestehende Netzfilterregel bearbeiten                  | 16        |
| Bestehende Netzfilterregeln löschen                    | 17        |
| Reihenfolge bzw. Priorität der Netzfilterregeln ändern | 18        |
| Erstellung eines SSL-Zertifikats                       | 18        |
| Besonderheiten für komplexe KVM-Systeme                | 19        |
| Erzeugen eines Certificate Authority-Zertifikats       | 19        |
| Erzeugen eines beliebigen Zertifikats                  | 21        |
| X509-Zertifikat erstellen und signieren                | 22        |
| PEM-Datei erstellen                                    | 22        |
| Auswahl eines SSL-Zertifikats                          | 23        |
| Durchführung von Firmware-Updates                      | 25        |
| Firmware-Update eines bestimmten Geräts                | 25        |
| Wiederherstellung der Werkseinstellungen               | 26        |
| Neustart des Gerätes durchführen                       | 26        |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>Netzwerkfunktionen der Geräte</b> .....                       | <b>27</b> |
| NTP-Server .....                                                 | 27        |
| Zeitsynchronisation mit einem NTP-Server.....                    | 27        |
| Manuelle Einstellung von Uhrzeit und Datum .....                 | 28        |
| Protokollierung von Syslog-Meldungen .....                       | 29        |
| Lokale Protokollierung der Syslog-Meldungen .....                | 29        |
| Versand von Syslog-Meldungen an einen Server .....               | 30        |
| Lokale Syslog-Meldung einsehen und speichern .....               | 31        |
| Benutzerauthentifizierung mit Verzeichnisdiensten .....          | 31        |
| Einrichtung der Zwei-Faktor-Authentifizierung am Gerät .....     | 34        |
| <b>Monitoring-Funktionen</b> .....                               | <b>36</b> |
| Alle Monitoring-Werte einsehen .....                             | 36        |
| Monitoring-Werte deaktivieren .....                              | 37        |
| Erweiterte Funktionen zur Verwaltung der kritischen Geräte ..... | 38        |
| Auflistung der kritischen Monitoring-Werte einsehen.....         | 38        |
| Alarm eines kritischen Gerätes bestätigen .....                  | 38        |
| <b>Benutzer und Gruppen</b> .....                                | <b>39</b> |
| Effizienter Einsatz der Rechteverwaltung .....                   | 39        |
| Das Effektivrecht .....                                          | 39        |
| Effizienter Einsatz der Benutzergruppen .....                    | 40        |
| Verwaltung von Benutzerkonten .....                              | 40        |
| Anlegen eines neuen Benutzerkontos .....                         | 41        |
| Aktivierung der Zwei-Faktor-Authentifizierung .....              | 42        |
| Änderung des Namens eines Benutzerkontos .....                   | 45        |
| Änderung des Passworts eines Benutzerkontos.....                 | 45        |
| Änderung der Rechte eines Benutzerkontos .....                   | 46        |
| Änderung der Gruppenzugehörigkeit eines Benutzerkontos.....      | 47        |
| Aktivierung oder Deaktivierung eines Benutzerkontos.....         | 48        |
| Löschen eines Benutzerkontos.....                                | 48        |
| Verwaltung von Benutzergruppen .....                             | 49        |
| Anlegen einer neuen Benutzergruppe.....                          | 49        |
| Änderung des Namens einer Benutzergruppe.....                    | 50        |
| Änderung der Rechte einer Benutzergruppe .....                   | 50        |
| Mitgliederverwaltung einer Benutzergruppe .....                  | 51        |
| Aktivierung oder Deaktivierung einer Benutzergruppe .....        | 51        |
| Löschen einer Benutzergruppe.....                                | 51        |
| System-Rechte .....                                              | 52        |
| Berechtigung zum uneingeschränkten Zugriff (Superuser) .....     | 52        |
| Berechtigung zum Login in die Webapplikation .....               | 52        |
| Berechtigung zur Änderung des eigenen Passworts.....             | 53        |
| Berechtigung zur Bestätigung eines Monitoring-Alarms .....       | 53        |

|                                                                              |           |
|------------------------------------------------------------------------------|-----------|
| <b>Erweiterte Funktionen des KVM-Systems</b> .....                           | <b>54</b> |
| Identifizierung eines Gerätes durch Aktivierung der Identification-LED ..... | 54        |
| Sicherung der Konfigurationseinstellungen .....                              | 54        |
| Sicherung der Konfigurationseinstellungen mit der Auto-Backup-Funktion ..... | 55        |
| Wiederherstellung der Konfigurationseinstellungen .....                      | 57        |
| Freischaltung kostenpflichtiger Zusatzfunktionen .....                       | 58        |

## **Kapitel 2: RemoteGateways**

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>Grundkonfiguration der RemoteGateways</b> .....            | <b>59</b> |
| Änderung des Namens eines RemoteGateways .....                | 59        |
| Änderung des Kommentares eines RemoteGateways .....           | 59        |
| <b>Erweiterte Funktionen für RemoteGateways</b> .....         | <b>60</b> |
| Konfigurationseinstellungen übertragen (Gerät ersetzen) ..... | 60        |
| Monitoring-Werte konfigurieren .....                          | 61        |
| Auswahl der zu überwachenden Monitoring-Werte .....           | 61        |
| Statusinformationen des Geräts einsehen .....                 | 62        |

# 1 Grundfunktionen

## Einleitung

Die Webapplikation *ConfigPanel* bietet eine grafische Benutzeroberfläche zur Konfiguration des KVM-Systems. Sie kann über einen unterstützten Webbrowser (s. Seite 2) bedient werden.

**TIPP:** Die Webapplikation kann unabhängig von den Standorten der am KVM-System angeschlossenen Geräte und Arbeitsplätze im gesamten Netzwerk eingesetzt werden.

Aufgrund der erweiterten Möglichkeiten der grafischen Benutzeroberfläche ist diese mit folgenden Komfortfunktionen ausgestattet:

- übersichtliche Benutzeroberfläche
- Überwachung verschiedener Eigenschaften des Systems
- erweiterte Netzwerkfunktionen (Netzfilter, Syslog, ...)
- Backup- und Restore-Funktion

**WICHTIG:** Der Betrieb der Geräte ist im Handbuch des Matrixswitches beschrieben.

# Systemvoraussetzungen

**WICHTIG:** Bevor die Webapplikation über den Webbrowser eines Computers gestartet werden kann, ist das Gerät, von welchem die Webapplikation geladen wird, zunächst mit dem lokalen Netzwerk zu verbinden (s. Installationsanleitung).

Anschließend sind – sofern nicht bereits erledigt – die auf Seite 3 beschriebenen Netzwerkeinstellungen anzupassen.

Die Webapplikation *ConfigPanel* wurde erfolgreich mit diesen Webbrowsern getestet:

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

## Unterstützte Betriebssysteme

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

## Empfohlene Grafikauflösungen

- Eine Mindestauflösung von 1280×800 Bildpunkten wird empfohlen.
- Die Webapplikation ist für die Darstellung der Inhalte im Querformat (Landscape-Modus) optimiert.
- Das Hochformat (Portrait-Modus) wird unterstützt. Möglicherweise sind in diesem Modus *nicht* alle Inhalte sichtbar.

# Erstkonfiguration der Netzwerkeinstellungen

**HINWEIS:** Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

- IP-Adresse der *Netzwerkschnittstelle »Network (Management)«*: **192.168.0.1**
- globale Netzwerkeinstellungen: Bezug der Einstellungen via **DHCP**

Grundlegende Voraussetzung für den Zugriff auf die Webapplikation ist die Konfiguration der Netzwerkeinstellungen des Gerätes, auf welchem die Webapplikation betrieben wird.

## So konfigurieren Sie die Netzwerkeinstellungen vor der Integration des Gerätes in das lokale Netzwerk:

1. Verbinden Sie die Netzwerkschnittstelle eines beliebigen Rechners mit der *Netzwerkschnittstelle Network (Management)* des Gerätes. Verwenden Sie hierzu ein Twisted-Pair-Kabel der Kategorie 5e (oder höher).
2. Stellen Sie sicher, dass die IP-Adresse der Netzwerkschnittstelle des Rechners Teil des Subnetzes ist, welchem auch die IP-Adresse des Gerätes angehört.

**HINWEIS:** Verwenden Sie beispielsweise die IP-Adresse *192.168.0.100*.

3. Schalten Sie das Gerät ein.
4. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile die URL **192.168.0.1** ein.
5. Konfigurieren Sie die Netzwerkschnittstelle(n) und die globalen Netzwerkeinstellungen wie im Abschnitt *Netzwerkeinstellungen* auf Seite 11 f. beschrieben.
6. Entfernen Sie die Twisted-Pair-Kabelverbindung zwischen dem Rechner und dem Gerät.
7. Integrieren Sie das Gerät in das lokale Netzwerk.

# Erste Schritte

In diesem Kapitel lernen Sie die grundlegende Bedienung der Webapplikation kennen.

**HINWEIS:** Die detaillierte Erläuterung der Funktionen und Konfigurationseinstellungen erfolgt in den folgenden Kapiteln dieses Handbuchs.

## Start der Webapplikation

**HINWEIS:** Informationen zu den Systemvoraussetzungen der Webapplikation finden Sie auf Seite 2.

**So starten Sie die Webapplikation:**

1. Geben in der Adresszeile folgende URL ein:

**https://[IP-Adresse des Gerätes]**

2. Geben Sie in die Login-Maske folgende Daten ein:

|                         |                                                                      |
|-------------------------|----------------------------------------------------------------------|
| <b>Benutzername:</b>    | Geben Sie Ihren Benutzernamen ein.                                   |
| <b>Passwort:</b>        | Geben Sie das Passwort Ihres Benutzerkontos ein.                     |
| <b>Einmal-Passwort:</b> | Geben Sie das Einmal-Passwort der Zwei-Faktor-Authentifizierung ein. |

**HINWEIS:** Das Einmal-Passwort wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 34 ff.) und aktiviert wurde (s. Seite 42 ff.).

**WICHTIG:** Ändern Sie das voreingestellte Passwort des Administratorkontos.

Melden Sie sich hierfür mit dem Administratorkonto in der Webapplikation an und ändern Sie anschließend das Passwort (s. Seite 45).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

- **Benutzername:** Admin
- **Passwort:** s. Login-Information auf dem Etikett an der Geräteunterseite

3. Klicken Sie auf **Login**.

# Bedienung der Webapplikation

## Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus mehreren Bereichen:

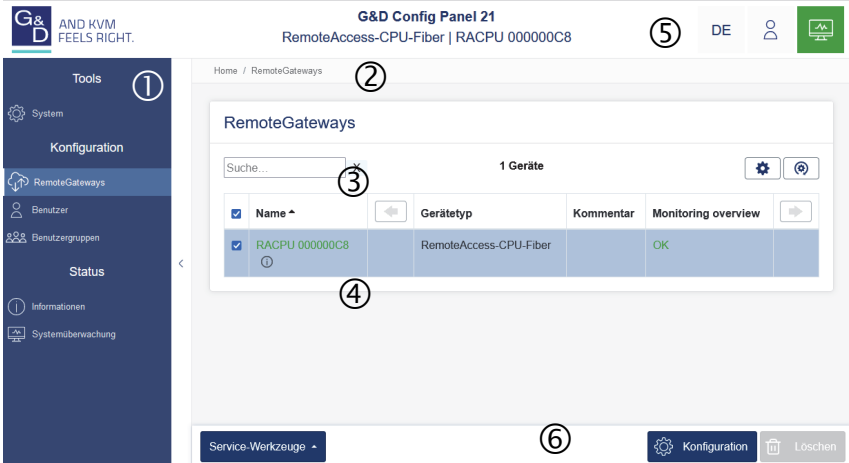


Abbildung 1: Benutzeroberfläche der Webapplikation

Die unterschiedlichen Bereiche der Benutzeroberfläche dienen verschiedenen Aufgaben. Die folgende Tabelle listet den Anwendungszweck jedes Bereichs auf:

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Menü ①:</b>                  | Im Menü sind die unterschiedlichen Funktionen der Webapplikation in Themenbereichen zusammengefasst.                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Brotkrumen-Navigation ②:</b> | Die Brotkrumennavigation zeigt Ihnen den Pfad zum derzeit geöffneten Dialog an.<br>Um schnell zu einem übergeordneten Dialog zurückzukehren können Sie diesen in der Brotkrumen-Navigation anklicken.                                                                                                                                                                                                                                                                 |
| <b>Filterfunktion ③:</b>        | Die Filterfunktion kann genutzt werden, um die in der Hauptansicht angezeigten Elemente einzugrenzen.<br>Geben Sie im Textfeld einen Teil des Namens des gesuchten Elements ein. Daraufhin werden ausschließlich solche Elemente in der Hauptansicht angezeigt, die diesen Text in einer der <i>angezeigten</i> Spalten enthalten. Die Groß-/Kleinschreibung der Namen wird bei der Filterung ignoriert.<br>Um die Filterung aufzuheben, klicken Sie auf <b>[X]</b> . |
| <b>Hauptansicht ④:</b>          | Nach der Auswahl eines Themenbereichs im Menü werden hier die Inhalte des Themenbereichs dargestellt.                                                                                                                                                                                                                                                                                                                                                                 |

**Schnellzugriffe ⑤**

**Sprachauswahl:** Die Sprachkennung (beispielsweise **DE** für *Deutsch*) zeigt die derzeit aktive Sprache in der Webapplikation an.

Zur Umschaltung der Sprache klicken Sie auf die Sprachkennung. Daraufhin öffnet sich ein Untermenü, das die unterstützten Sprachen und die zugehörigen Kennungen anzeigt.

Schalten Sie mit einem Klick auf die gewünschte Sprache die Sprache um.

**Benutzer:** Nach einem Klick auf das Benutzersymbol öffnet sich ein Untermenü:

- Im Untermenü wird der Name des aktiven Benutzers angezeigt.
- Mit einem Klick auf *Benutzer* gelangen Sie zu den Benutzereinstellungen des aktiven Benutzers.
- Klicken Sie auf *Abmelden*, um die aktive Sitzung zu beenden.

**Monitoring-Status:** Dieses Icon zeigt Ihnen auf den ersten Blick, ob alle Monitoringwerte im Normbereich sind (grünes Icon) oder mindestens ein Monitoring-Wert auffällig ist (gelbes oder rotes Icon).

Das Icon *Monitoring-Status* nimmt jeweils die Farbe des *schlechtesten* Monitoring-Wertes an.

Wird das Icon in gelber oder roter Farbe angezeigt, gelangen Sie mit einem Klick auf das Icon in den Dialog *Aktive Alarme*.

**Schaltflächen ⑥:**

Abhängig vom dargestellten Dialog werden in diesem Bereich verschiedene Schaltflächen angezeigt.

## Häufig verwendete Schaltflächen

Die Benutzeroberfläche verwendet verschiedene Schaltflächen zur Durchführung von Operationen. Über die Bezeichnungen und Funktionen der in vielen Dialogmasken verwendeten Schaltflächen informiert Sie die folgende Tabelle:

|                           |                                                                                                                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Konfiguration:</b>     | Aufruf der Konfigurationseinstellungen des ausgewählten Elements (Gerät, Benutzer, ...)                                                                                                                  |
| <b>Service-Werkzeuge:</b> | Bei Auswahl eines Gerätes in der Hauptansicht können Sie über die Service-Werkzeuge bestimmte Aufgaben (beispielsweise Update, Backup, Syslog-Anzeige) erreichen.                                        |
| <b>Speichern:</b>         | Speicherung der eingegebenen Daten. Der geöffnete Dialog wird weiterhin angezeigt.                                                                                                                       |
| <b>Abbrechen:</b>         | Die von Ihnen eingegebenen Daten werden verworfen und der Dialog geschlossen.                                                                                                                            |
| <b>Schließen:</b>         | Die eingegebenen Daten werden zwischengespeichert und der Dialog geschlossen.<br>Erst nach einem Klick auf <b>Speichern</b> oder <b>Abbrechen</b> werden die Daten permanent gespeichert oder verworfen. |

## Tabellenspalten konfigurieren

Die anzuzeigenden Tabellenspalten in den Themenbereichen **RemoteGateways** und **Benutzer** können Sie an Ihre Bedürfnisse anpassen.

Im Themenbereich **RemoteGateways** werden standardmäßig die Spalten *Name*, *Gerätetyp*, *Kommentar* und *Monitoring-Übersicht* angezeigt:

### RemoteGateways

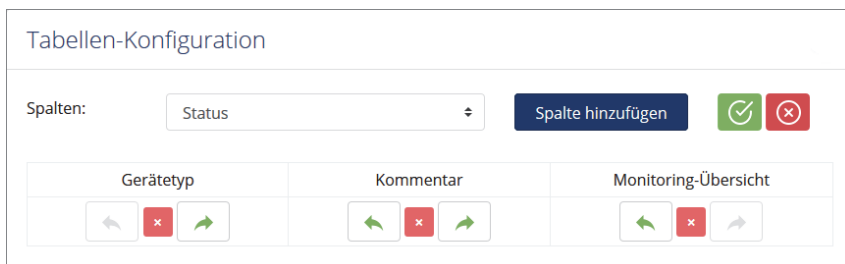
|                                     |                                                                                                       |                                                                                     |                        |                                                                                                                                                                          |                                                                                      |
|-------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Suche... X                          |                                                                                                       | 1 Geräte                                                                            |                        |   |                                                                                      |
| <input checked="" type="checkbox"/> | Name ^                                                                                                |  | Gerätetyp              | Monitoring overview                                                                                                                                                      |  |
| <input checked="" type="checkbox"/> | RACPU 000000C8<br> |                                                                                     | RemoteAccess-CPU-Fiber | OK                                                                                                                                                                       |                                                                                      |

Abbildung 2: Tabellenspalten (Auswahl) eines RemoteGateways

### So ändern Sie die anzuzeigenden Spalten:

**HINWEIS:** Die Spalte **Name** wird *immer* als erste Spalte der Tabelle angezeigt.

1. Klicken Sie auf das Zahnradsymbol (⚙️) oberhalb der Tabelle.



**Abbildung 3: Tabellenkonfiguration**

2. Zum Hinzufügen einer Spalte wählen Sie diese im Drop-Down-Feld Spalten aus und klicken auf Spalte hinzufügen.
3. Zum Löschen einer Spalte klicken Sie auf die rote Schaltfläche (X) unterhalb der Spaltenüberschrift.
4. Klicken Sie auf die grüne **Anwenden**-Schaltfläche (✓), um die Änderungen zu speichern oder klicken Sie auf die rote **Verwerfen**-Schaltfläche (✗).

### So ändern Sie die Reihenfolge der Spalten:

**HINWEIS:** Die Spalte **Name** wird *immer* als erste Spalte der Tabelle angezeigt.

1. Klicken Sie auf das Zahnradsymbol oberhalb der Tabelle.
2. Um eine Spalte nach links zu verschieben, klicken Sie auf das ⬅️-Symbol dieser Spalte.
3. Um eine Spalte nach rechts zu verschieben, klicken Sie auf das ➡️-Symbol dieser Spalte.
4. Klicken Sie auf die grüne **Anwenden**-Schaltfläche (✓), um die Änderungen zu speichern oder klicken Sie auf die rote **Verwerfen**-Schaltfläche (✗).

### So setzen Sie die Tabellenkonfiguration auf die Standardwerte zurück

1. Klicken Sie auf das Symbol **Tabellenkonfiguration zurücksetzen** (🔄) oberhalb der Tabelle.
2. Bestätigen Sie die Sicherheitsabfrage mit einem Klick auf **Ja**.

## Spracheinstellungen

### Sprache der Webapplikation auswählen

So ändern Sie die Sprache der Webapplikation:

1. Klicken Sie auf das Sprachkürzel der aktuellen Sprache rechts oben.
2. Schalten Sie die zu verwendende Sprache mit einem Klick auf die gewünschte Sprache um.



**HINWEIS:** Die eingestellte Sprache wird in den Benutzereinstellungen des aktiven Benutzers gespeichert. Bei der nächsten Anmeldung dieses Benutzers wird die zuvor ausgewählte Spracheinstellung angewendet.

### Systemsprache auswählen

Die festgelegte *Systemsprache* wird standardmäßig allen Benutzerkonten zugewiesen.

So stellen Sie die **Systemsprache** ein:

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Systemsprache**.
3. Wählen Sie die gewünschte Sprache.
4. Klicken Sie auf **Speichern**.

## Versionsnummer der Webapplikation anzeigen

So zeigen Sie die Versionsnummer der Webapplikation an:

1. Klicken Sie im Menü auf **Informationen**.
2. Auf dem Reiter **Allgemein** werden u. a. Informationen zur *ConfigPanel*-Version angezeigt.

## Webapplikation beenden

Mit der *Abmelden*-Funktion beenden Sie die aktive Sitzung der Webapplikation.

**WICHTIG:** Verwenden Sie immer die *Abmelden*-Funktion nach Abschluss Ihrer Arbeit mit der Webapplikation.

Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die Webapplikation:

1. Klicken Sie auf das **Benutzersymbol** rechts oben.
2. Klicken Sie auf **Abmelden**, um die aktive Sitzung zu beenden.



# Grundkonfiguration der Webapplikation

## Netzwerkeinstellungen

Das Gerät ist mit einer Netzwerkschnittstelle ausgestattet. Die Netzwerkschnittstelle erlaubt die Integration eines Gerätes in ein Netzwerk.

**WICHTIG:** Beachten Sie die separaten Anweisungen zur *Erstkonfiguration der Netzwerkeinstellungen* auf Seite 3.

## Konfiguration der Netzwerkschnittstelle

Zur Anbindung des Gerätes an ein lokales Netzwerk sind die Einstellungen des Netzwerks zu konfigurieren.

**HINWEIS:** Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

- IP-Adresse der *Netzwerkschnittstelle*: **192.168.0.1**
- globale Netzwerkeinstellungen: Bezug der Einstellungen via **DHCP**

## So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:

**HINWEIS:** Der *Link Local*-Adressraum 169.254.0.0/16 ist gemäß RFC 3330 für die interne Kommunikation zwischen Geräten reserviert. Die Zuordnung einer IP-Adresse dieses Adressraums ist nicht möglich!

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Schnittstellen**.
5. Erfassen Sie im Abschnitt **Schnittstelle A** folgende Daten:

|                       |                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Betriebsmodus:</b> | Wählen Sie den Betriebsmodus der <b>Schnittstelle A</b> aus: <ul style="list-style-type: none"> <li>▪ <b>Aus:</b> Netzwerkschnittstelle ausschalten.</li> <li>▪ <b>Statisch:</b> Es wird eine statische IP-Adresse zugeteilt.</li> <li>▪ <b>DHCP:</b> Bezug der IP-Adresse von einem DHCP-Server.</li> </ul> |
| <b>IP-Adresse:</b>    | Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die IP-Adresse der Schnittstelle an.                                                                                                                                                                                                         |
| <b>Netzmaske:</b>     | Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die Netzmaske des Netzwerkes an.                                                                                                                                                                                                             |

6. Klicken Sie auf **Speichern**.

## Konfiguration der globalen Netzwerkeinstellungen

Die globalen Netzwerkeinstellungen stellen auch in komplexen Netzwerken sicher, dass die Webapplikation aus allen Teilnetzwerken erreichbar ist.

### So konfigurieren Sie die globalen Netzwerkeinstellungen:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Globale Netzwerkeinstellungen**.
5. Erfassen Sie folgende Daten:

|                       |                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Betriebsmodus:</b> | Wählen Sie den gewünschten Betriebsmodus: <ul style="list-style-type: none"><li>▪ <b>Statisch:</b> Verwendung von statischen Einstellungen.</li><li>▪ <b>DHCP:</b> Bezug der Einstellungen von einem DHCP-Server.</li></ul>                                                                                                                                                        |
| <b>Host-Name:</b>     | Geben Sie den Host-Namen des Gerätes ein.<br><b>WICHTIG:</b> Falls bei aktiviertem DHCP der DHCP-Server selbst keinen Host-Namen vergibt, wird der hier erfasste Host-Name verwendet. Ansonsten wird der vom DHCP-Server bezogene Host-Name verwendet.<br><br>Im Betriebsmodus <i>DHCP</i> werden die folgenden Einstellungen automatisch bezogen. Eine Eingabe ist nicht möglich. |
| <b>Domäne:</b>        | Geben Sie die Domäne an, welcher das Gerät angehören soll.                                                                                                                                                                                                                                                                                                                         |
| <b>Gateway:</b>       | Geben Sie die IP-Adresse des Gateways an.                                                                                                                                                                                                                                                                                                                                          |
| <b>DNS-Server 1:</b>  | Geben Sie die IP-Adresse des DNS-Servers an.                                                                                                                                                                                                                                                                                                                                       |
| <b>DNS-Server 2:</b>  | Geben Sie <i>optional</i> die IP-Adresse eines weiteren DNS-Servers an.                                                                                                                                                                                                                                                                                                            |

6. Klicken Sie auf **Speichern**.

## Status der Netzwerkschnittstelle auslesen

Den aktuellen Status der Netzwerkschnittstelle des Gerätes können Sie in der Webapplikation auslesen.

### So ermitteln Sie den Status der Netzwerkschnittstelle:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Informationen**.
4. Gehen Sie zum Bereich **Link Status**.
5. Im Abschnitt **Schnittstelle A** werden Ihnen folgende Daten angezeigt:

|                          |                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Link detected:</b>    | Verbindung zum Netzwerk hergestellt ( <b>ja</b> ) oder unterbrochen ( <b>nein</b> ).                                                                  |
| <b>Auto-negotiation:</b> | Die Übertragungsgeschwindigkeit und des Duplex-Verfahren wurde automatisch ( <b>ja</b> ) oder manuell vom Administrator konfiguriert ( <b>nein</b> ). |
| <b>Speed:</b>            | Übertragungsgeschwindigkeit                                                                                                                           |
| <b>Duplex:</b>           | Duplexverfahren ( <b>full</b> bzw. <b>half</b> )                                                                                                      |

6. Klicken Sie auf **Speichern**.

## Netzfilterregeln einrichten und administrieren

Im Auslieferungszustand der Geräte haben alle Netzwerkrechner Zugriff auf die Webapplikation *ConfigPanel* (offener Systemzugang).

**HINWEIS:** Der offene Systemzugang erlaubt uneingeschränkte Verbindungen über die Ports 80/TCP (HTTP), 443/TCP (HTTPS) und 161/UDP (SNMP).

Sobald eine Netzfilterregel erstellt ist, wird der offene Systemzugang deaktiviert und alle eingehenden Datenpakete mit den Netzfilterregeln verglichen. Die Liste der Netzfilterregeln wird hierbei in der gespeicherten Reihenfolge abgearbeitet. Sobald eine Regel zutrifft, wird die entsprechende Aktion ausgeführt und die nachfolgenden Regeln werden ignoriert.

### Neue Netzfilterregel erstellen

**So erstellen Sie eine neue Netzfilterregel:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Netzfilter**.
5. Erfassen Sie folgende Daten:

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Option:</b>                    | <p>Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist:</p> <ul style="list-style-type: none"><li>▪ <b>Normal:</b> Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li><li>▪ <b>Invertiert:</b> Die Regel gilt für Datenpakete, deren Absenderinformation <i>nicht</i> der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li></ul>                                                       |
| <b>IP-Adresse/<br/>Netzmaske:</b> | <p>Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes <b>Netzmaske</b> – den Adressraum der IP-Adressen ein.</p> <p><b>Beispiele:</b></p> <ul style="list-style-type: none"><li>▪ <b>192.168.150.187:</b> nur die IP-Adresse 192.168.150.187</li><li>▪ <b>192.168.150.0/24:</b> IP-Adressen des Raums 192.168.150.x</li><li>▪ <b>192.168.0.0/16:</b> IP-Adressen des Raums 192.168.x.x</li><li>▪ <b>192.0.0.0/8:</b> IP-Adressen des Raums 192.x.x.x</li><li>▪ <b>0.0.0.0/0:</b> alle IP-Adressen</li></ul> |

**HINWEIS:** Innerhalb einer Regel können wahlweise die *IP-Adresse* und/oder eine *MAC-Adresse* angegeben werden.

|                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MAC-Adresse:</b>                                                                                                             | Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.                                                                                                                                                                                                                                              |
| <b>HINWEIS:</b> Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden. |                                                                                                                                                                                                                                                                                                                                  |
| <b>Filterregel:</b>                                                                                                             | <ul style="list-style-type: none"><li>▪ <b>Drop:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden <i>nicht</i> verarbeitet.</li><li>▪ <b>Accept:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.</li></ul> |
| <b>Service:</b>                                                                                                                 | Wählen Sie einen bestimmten Service, für den diese Regel exklusiv angewendet wird oder wählen Sie ( <b>Alle</b> ).                                                                                                                                                                                                               |

6. Klicken Sie auf **Hinzufügen**, um die Daten in einer neuen Filterregel zu speichern.

Die neue Filterregel wird an das Ende der Liste der bestehenden Filterregeln angefügt.

7. Klicken Sie auf **Speichern**.

**HINWEIS:** Die neue Netzfilterregel wird nicht auf aktive Verbindungen angewendet. Starten Sie das Gerät neu, wenn Sie die Trennung der aktiven Verbindungen und die anschließende Anwendung aller Regeln wünschen.

## Bestehende Netzfilterregel bearbeiten

### So bearbeiten Sie eine bestehende Netzfilterregel:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Netzfilter**.
5. Markieren Sie in der Liste der bestehenden Netzfilterregeln die zu ändernde Regel.
6. Die aktuellen Einstellungen der Regel werden im oberen Bereich des Dialogs angezeigt. Prüfen und ändern Sie die folgenden Daten.

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Option:</b>                    | <p>Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist:</p> <ul style="list-style-type: none"><li>▪ <b>Normal:</b> Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li><li>▪ <b>Invertiert:</b> Die Regel gilt für Datenpakete, deren Absenderinformation <i>nicht</i> der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li></ul>                                                                                                                                                                                         |
| <b>IP-Adresse/<br/>Netzmaske:</b> | <p>Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes <b>Netzmaske</b> – den Adressraum der IP-Adressen ein.</p> <p><b>Beispiele:</b></p> <ul style="list-style-type: none"><li>▪ <b>192.168.150.187:</b> nur die IP-Adresse 192.168.150.187</li><li>▪ <b>192.168.150.0/24:</b> IP-Adressen des Raums 192.168.150.x</li><li>▪ <b>192.168.0.0/16:</b> IP-Adressen des Raums 192.168.x.x</li><li>▪ <b>192.0.0.0/8:</b> IP-Adressen des Raums 192.x.x.x</li><li>▪ <b>0.0.0.0/0:</b> alle IP-Adressen</li></ul> <div><p>Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p></div> |
| <b>MAC-Adresse:</b>               | <p>Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.</p> <div><p>Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p></div>                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Filterregel:</b>               | <ul style="list-style-type: none"><li>▪ <b>Drop:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden <i>nicht</i> verarbeitet.</li><li>▪ <b>Accept:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.</li></ul>                                                                                                                                                                                                                                                                                                                                       |

**Service:** Wählen Sie einen bestimmten Service, für den diese Regel exklusiv angewendet wird oder wählen Sie **(Alle)**.

7. Klicken Sie auf **Ändern**, um die von Ihnen geänderten Daten zu speichern.
8. Klicken Sie auf **Speichern**.

**HINWEIS:** Die geänderte Netzfilterregel wird nicht auf aktive Verbindungen angewendet. Starten Sie das Gerät neu, wenn Sie die Trennung der aktiven Verbindungen und die anschließende Anwendung aller Regeln wünschen.

## Bestehende Netzfilterregeln löschen

**So löschen Sie bestehende Netzfilterregeln:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Netzfilter**.
5. Markieren Sie in der Liste der bestehenden Netzfilterregeln die zu löschende Regel.
6. Klicken Sie auf **Löschen**.
7. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.
8. Klicken Sie auf **Speichern**.

## Reihenfolge bzw. Priorität der Netzfilterregeln ändern

Die Liste der Netzfilterregeln wird in der gespeicherten Reihenfolge abgearbeitet. Sobald eine Regel zutrifft, wird die entsprechende Aktion ausgeführt und die nachfolgenden Regeln werden ignoriert.

**WICHTIG:** Achten Sie – insbesondere beim Hinzufügen neuer Regeln – auf die Reihenfolge bzw. Priorität der einzelnen Regeln.

### So ändern Sie die Reihenfolge/Priorität der bestehenden Netzfilterregeln:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Netzfilter**.
5. Markieren Sie in der Liste der bestehenden Netzfilterregeln jene Regel, deren Reihenfolge/Priorität Sie ändern möchten.
6. Klicken Sie auf die Schaltfläche **Pfeil hoch**, um die Priorität zu erhöhen oder auf die Schaltfläche **Pfeil runter**, um die Priorität zu verringern.
7. Klicken Sie auf **Speichern**.

## Erstellung eines SSL-Zertifikats

Die Erstellung eines SSL-Zertifikats kann beispielsweise mit der freien Implementierung des SSL/TLS-Protokolls *OpenSSL* erfolgen.

**WICHTIG:** Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation (s. Seite 18 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

Detaillierte Informationen zur Bedienung von OpenSSL finden Sie auf folgenden Websites:

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

**WICHTIG:** Voraussetzung für die Erstellung eines SSL-Zertifikats ist die Software OpenSSL. Folgen Sie ggf. den Anleitungen auf den oben genannten Websites, um die Software zu installieren.

Die Anleitung auf den folgenden Seiten erläutert *exemplarisch* die Erstellung eines SSL-Zertifikates.

## Besonderheiten für komplexe KVM-Systeme

Falls innerhalb eines KVM-Systems verschiedene G&D-Geräte miteinander kommunizieren sollen, ist bei der Erstellung von Zertifikaten für diese Geräte das identische *Certificate Authority*-Zertifikat (s. Seite 19) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 22) verwendet werden. In diesem Fall sind alle Merkmale der Zertifikate identisch.

## Erzeugen eines Certificate Authority-Zertifikats

Das *Certificate Authority*-Zertifikat berechtigt den Inhaber digitale Zertifikate (z. B. für einen Matrixswitch) zu erstellen.

**So erstellen Sie zunächst einen Schlüssel für das Certificate Authority-Zertifikat:**

**WICHTIG:** Der im folgenden Schritt zu erstellende Schlüssel wird *nicht* verschlüsselt. Lesen Sie ggf. in der Dokumentation von OpenSSL nach, um zu erfahren wie ein verschlüsselter Schlüssel erstellt werden kann!

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

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

2. Der Schlüssel wird durch OpenSSL erstellt und unter dem Dateinamen *ca.key* gespeichert.

**So erstellen Sie das Certificate Authority-Zertifikat:**

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

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

2. OpenSSL erfragt nun einige Daten, die in das Zertifikat integriert werden.

Nachfolgend werden die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

| Feld                                      | Beispiel                 |
|-------------------------------------------|--------------------------|
| Country Name (2 letter code)              | DE                       |
| State or Province Name                    | NRW                      |
| Locality Name (eg, city)                  | Siegen                   |
| Organization Name (eg, company)           | Guntermann & Drunck GmbH |
| Organizational Unit Name<br>(eg, section) |                          |
| Common Name (eg, YOUR name)               | Guntermann & Drunck GmbH |
| Email Address                             |                          |

**WICHTIG:** In der Zeile *Common Name* darf *nicht* die IP-Adresse des Gerätes eingegeben werden!

Geben Sie die von Ihnen gewünschten Daten ein und bestätigen Sie jede Eingabe durch Betätigung der **Eingabetaste**.

3. Das Zertifikat wird durch OpenSSL erstellt und unter dem Dateinamen *ca.crt* gespeichert.

**WICHTIG:** Verteilen Sie das Zertifikat *ca.crt* an die Webbrowser der Rechner, die die Webapplikation nutzen. Anhand dieses Zertifikats kann die Gültigkeit und das Vertrauen des eigenen Zertifikats im Gerät erfolgreich geprüft werden.

## Erzeugen eines beliebigen Zertifikats

So erstellen Sie zunächst einen Schlüssel für das zu erstellende Zertifikat:

**WICHTIG:** Der im folgenden Schritt zu erstellende Schlüssel wird nicht verschlüsselt. Lesen Sie ggf. in der Dokumentation von OpenSSL nach, um zu erfahren wie ein verschlüsselter Schlüssel erstellt werden kann!

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

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

2. Der Schlüssel wird durch OpenSSL erstellt und unter dem Dateinamen *server.key* gespeichert.

So erstellen Sie die Zertifikatsanforderung:

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die **Eingabetaste**:

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

2. OpenSSL erfragt nun einige Daten, die in das Zertifikat integriert werden.

Nachfolgend sind die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

| Feld                                      | Beispiel                 |
|-------------------------------------------|--------------------------|
| Country Name (2 letter code)              | DE                       |
| State or Province Name                    | NRW                      |
| Locality Name (eg, city)                  | Siegen                   |
| Organization Name (eg, company)           | Guntermann & Drunck GmbH |
| Organizational Unit Name<br>(eg, section) |                          |
| Common Name (eg, YOUR name)               | 192.168.0.10             |
| Email Address                             |                          |

**WICHTIG:** Geben Sie die IP-Adresse des Geräts auf dem das Zertifikat installiert wird in der Zeile *Common Name* ein.

Geben Sie die von Ihnen gewünschten Daten ein und bestätigen Sie jede Eingabe durch Betätigung der **Eingabetaste**.

3. Falls gewünscht, kann zusätzlich das *Challenge Password* festgelegt werden. Dieses ist bei Verlust des geheimen Schlüssels für einen Zertifikatswiderruf erforderlich.
4. Jetzt wird das Zertifikat erstellt und unter dem Dateinamen *server.csr* gespeichert.

## X509-Zertifikat erstellen und signieren

1. Geben Sie folgenden Befehl in der Eingabeaufforderung ein und betätigen Sie anschließend die Eingabetaste:

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

2. Das Zertifikat wird durch OpenSSL erstellt und unter dem Dateinamen *server.crt* gespeichert.

## PEM-Datei erstellen

**HINWEIS:** Die *.pem*-Datei beinhaltet die folgenden drei Komponenten:

- Zertifikat des Servers
- Privater Schlüssel des Servers
- Zertifikat der Zertifizierungsstelle

Falls die drei Komponenten separat vorliegen, fügen Sie diese nacheinander im Feld *Klartext* ein, bevor Sie das im Gerät gespeicherte Zertifikat aktualisieren.

1. Geben Sie folgende(n) Befehl(e) in der Eingabeaufforderung ein und betätigen Sie anschließend die Eingabetaste:

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. Durch die Kopieroperation(en) wird die Datei *gdc.d.pem* erstellt. Diese enthält das erstellte Zertifikat und dessen Schlüssel sowie das Zertifikat der *Certificate Authority*.

## Auswahl eines SSL-Zertifikats

Jedes G&D-Gerät mit integrierter Webapplikation wird ab Werk mit mindestens einem SSL-Zertifikat ausgestattet. Das Zertifikat erfüllt zwei Funktionen:

- Die Verbindung des Webbrowsers mit der Webapplikation kann über eine SSL-gesicherte Verbindung erfolgen. In diesem Fall erlaubt das SSL-Zertifikat dem Anwender, die Gegenseite zu authentifizieren.

Weicht die IP-Adresse des Geräts von der im Zertifikat angegebenen IP-Adresse ab, wird eine Unstimmigkeit durch den Webbrowser gemeldet.

**TIPP:** Importieren Sie ein eigenes Zertifikat, so dass die IP-Adresse des Geräts mit der im Zertifikat angegebenen übereinstimmt.

- Die Kommunikation verschiedener G&D-Geräte innerhalb eines KVM-Systems wird über die Zertifikate der Geräte abgesichert.

**WICHTIG:** Nur wenn alle Geräte innerhalb eines KVM-Systems Zertifikate der identischen *Certificate Authority* (s. Seite 19) verwenden, können die Geräte mit-einander kommunizieren.

### So wählen Sie das zu verwendende SSL-Zertifikat:

**WICHTIG:** Beenden Sie nach der Aktivierung eines *anderen* Zertifikats die zurzeit aktiven »Config Panel«-Sitzungen und starten Sie neue Sitzungen.

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Zertifikat**.

5. Wählen Sie das zu verwendende Zertifikat aus:

**G&D-Zertifikat #1:** Dieses Zertifikat ist bei *neuen* Geräten ab Werk aktiviert.

**HINWEIS:** Achten Sie darauf, dass Sie innerhalb des KVM-Systems für alle Geräte dasselbe Zertifikat verwenden.

**G&D-Zertifikat #2:** Dieses Zertifikat wird von einigen älteren G&D-Geräten mit integrierter Webapplikation unterstützt.

**Eigenes Zertifikat:** Aktivieren Sie diese Option, wenn Sie ein gekauftes Zertifikat einer Zertifizierungsstelle oder ein selbsterstelltes Zertifikat verwenden möchten.

Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat:

1. Klicken Sie auf **Zertifikat aus Datei importieren** und wählen Sie die zu importierende .pem-Datei im Datei-Dialog aus.

Alternativ kopieren Sie den Klartext des Zertifikats des Servers, den privaten Schlüssel des Servers sowie das Zertifikat der Zertifizierungsstelle in das Textfeld.

2. Klicken Sie auf **Upload und aktivieren**, um das importierte Zertifikat im Gerät zu speichern und zu aktivieren.

6. Klicken Sie auf **Speichern**.

**WICHTIG:** Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation (s. Seite 18 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

## Durchführung von Firmware-Updates

Die Firmware jedes Gerätes des KVM-Systems kann über die Webapplikation aktualisiert werden.

### Firmware-Update eines bestimmten Geräts

**WICHTIG:** Diese Funktion aktualisiert ausschließlich die Firmware des Gerätes, auf welchem die Webapplikation gestartet wurde!

#### So aktualisieren Sie die Firmware eines bestimmten Geräts:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu aktualisierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Firmware-Update**.
4. Klicken Sie auf **Firmware-Dateien bereitstellen**.

**HINWEIS:** Falls sich die Firmware-Datei bereits im internen Gerätespeicher befindet, können Sie diesen Schritt überspringen.

Wählen Sie die Firmware-Datei auf Ihrem lokalen Datenträger und klicken Sie auf **Öffnen**.

**HINWEIS:** Die Mehrfachauswahl von Firmware-Dateien ist bei gleichzeitiger Betätigung der **Shift**- bzw. der **Strg**-Taste mit der linken Maustaste möglich.

Die Firmware-Datei wird auf den internen Gerätespeicher übertragen und kann anschließend für das Update ausgewählt werden.

5. Wählen Sie die zu verwendenden Firmware-Dateien aus dem internen Gerätespeicher und klicken Sie auf **Weiter**.
6. Wählen Sie ggf. die **Zielfersion** der Geräte aus, falls Sie in Schritt 5. mehrere Firmware-Dateien für ein Gerät ausgewählt haben.
7. Schieben Sie den **Aktualisieren**-Schieberegler in den Zeilen aller zu aktualisierenden Geräte nach rechts (grün).
8. Klicken Sie auf **Update starten**.

**WICHTIG:** Schließen Sie **nicht** die Browser-Session, während das Gerät aktualisiert wird! Schalten Sie das Produkt während dem Update **nicht** aus, und trennen Sie es **nicht** von der Stromversorgung.

## Wiederherstellung der Werkseinstellungen

Mit dieser Funktion kann die Werkseinstellung des Gerätes, auf welchem die Webapplikation betrieben wird, wiederhergestellt werden.

### So stellen Sie die Werkseinstellungen wieder her:

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Werkseinstellungen**.
3. Wählen Sie den Umfang der Wiederherstellung aus:

|                                                               |                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Alle Einstellungen zurücksetzen:</b>                       | Alle Einstellungen des Gerätes zurücksetzen.                             |
| <b>Nur Einstellungen des lokalen Netzwerkes zurücksetzen:</b> | Ausschließlich die lokalen Netzwerkeinstellungen zurücksetzen.           |
| <b>Nur Einstellungen der KVM-Anwendungen zurücksetzen:</b>    | Alle Einstellungen außer den lokalen Netzwerkeinstellungen zurücksetzen. |

4. Klicken Sie auf **Werkseinstellungen**.

## Neustart des Gerätes durchführen

Mit dieser Funktion starten Sie das Gerät neu. Vor dem Neustart werden Sie zur Bestätigung aufgefordert, um einen versehentlichen Neustart zu verhindern.

### So führen Sie einen Neustart des Gerätes über die Webapplikation aus:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das gewünschte Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Neustart**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Neustart**.

# Netzwerkfunktionen der Geräte

Die Geräte innerhalb des KVM-Systems verfügen über *separate* Netzwerkfunktionen.

Für das **RemoteAccess-CPU** können Sie u. a. folgende Funktionen konfigurieren:

- Authentifizierung gegenüber Verzeichnisdiensten (LDAP, Active Directory, RADIUS, TACACS+)
- Zeitsynchronisation über einen NTP-Server
- Versendung von Log-Meldungen an Syslog-Server

## NTP-Server

Die Einstellung des Datums und der Uhrzeit eines Gerätes kann wahlweise automatisiert durch die Zeitsynchronisation mit einem NTP-Server (*Network Time Protocol*) oder manuell erfolgen.

### Zeitsynchronisation mit einem NTP-Server

So ändern Sie die Einstellungen bezüglich der NTP-Zeitsynchronisation:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **NTP-Server** und erfassen Sie folgende Daten:

|                                 |                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NTP-Zeitsynchronisation:</b> | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Zeitsynchronisation aus- und einschalten: <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b> (<i>Standard</i>)</li> <li>▪ <b>Aktiviert</b></li> </ul> |
| <b>NTP-Server 1:</b>            | Geben Sie die Adresse eines Zeitserver ein.                                                                                                                                                                                               |
| <b>NTP-Server 2:</b>            | Geben Sie <i>optional</i> die Adresse eines zweiten Zeitserver ein.                                                                                                                                                                       |
| <b>Zeitzone:</b>                | Wählen Sie aus dem Pull-Down-Menü die Zeitzone Ihres Standorts aus.                                                                                                                                                                       |

5. Klicken Sie auf **Speichern**.

## Manuelle Einstellung von Uhrzeit und Datum

So stellen Sie die Uhrzeit und das Datum des Gerätes manuell ein:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **NTP-Server**.

**WICHTIG:** Deaktivieren Sie in diesem Bereich gegebenenfalls die Option **NTP-Zeit-synchronisation**, da andernfalls die manuelle Einstellung von Uhrzeit und Datum nicht möglich ist.

5. Geben Sie im Feld **Uhrzeit** des Abschnitts **Uhrzeit/Datum** die aktuelle Zeit im Format *hh:mm:ss* ein.
6. Geben Sie im Feld **Datum** des Abschnitts **Uhrzeit/Datum** das aktuelle Datum im Format *TT.MM.JJJJ* ein.

**TIPP:** Klicken Sie auf **Lokales Datum übernehmen**, um das aktuelle Systemdatum des Computers, auf welchem die Webapplikation geöffnet wurde, in die Felder *Uhrzeit* und *Datum* zu übernehmen.

7. Klicken Sie auf **Speichern**.

## Protokollierung von Syslog-Meldungen

Das Syslog-Protokoll wird zur Übermittlung von Log-Meldungen in Netzwerken verwendet. Die Log-Meldungen werden an einen Syslog-Server übermittelt, welcher die Log-Meldungen vieler Geräte im Rechnernetz protokolliert.

Im Syslog-Standard wurden u. a. acht verschiedene Schweregrade festgelegt, nach welchen die Log-Meldungen zu klassifizieren sind:

|                      |                     |                   |
|----------------------|---------------------|-------------------|
| ▪ <b>0:</b> Notfall  | ▪ <b>3:</b> Fehler  | ▪ <b>6:</b> Info  |
| ▪ <b>1:</b> Alarm    | ▪ <b>4:</b> Warnung | ▪ <b>7:</b> Debug |
| ▪ <b>2:</b> Kritisch | ▪ <b>5:</b> Notiz   |                   |

Über die Webapplikation können Sie die lokale Protokollierung oder den Versand von Syslog-Meldungen an bis zu zwei Syslog-Server konfigurieren.

### Lokale Protokollierung der Syslog-Meldungen

**So konfigurieren Sie die lokale Protokollierung von Syslog-Meldungen:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Syslog** und erfassen Sie im Abschnitt **Syslog lokal** folgende Daten:

|                                                                                                                                                                         |                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syslog lokal:</b>                                                                                                                                                    | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie die lokale Protokollierung von Syslog-Meldungen aus oder ein: <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b></li> <li>▪ <b>Aktiviert</b> (<i>Standard</i>)</li> </ul> |
| <b>Log-Level:</b>                                                                                                                                                       | Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist.<br>Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.                                                  |
| Wählen Sie den Schweregrad <i>2 - Kritisch</i> , so werden für diesen, wie auch für die Schweregrade <i>1 - Alarm</i> und <i>0 - Notfall</i> , Meldungen protokolliert. |                                                                                                                                                                                                                                                             |

5. Klicken Sie auf **Speichern**.

## Versand von Syslog-Meldungen an einen Server

So konfigurieren Sie den Versand von Syslog-Meldungen an einen Server:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Syslog** und erfassen Sie folgende Daten im Abschnitt **Syslog-Server 1** oder **Syslog-Server 2**:

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syslog-Server:</b>            | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie den Versand von Syslog-Meldungen an einen Server aus oder ein: <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b> (<i>Standard</i>)</li> <li>▪ <b>Aktiviert</b></li> </ul>                                                                                                                                                                                                                                                  |
| <b>Log-Level:</b>                | Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist.<br><br>Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.<br><br><div style="border: 1px solid black; padding: 5px; margin-top: 10px;">                     Wählen Sie den Schweregrad <i>2 - Kritisch</i>, so werden für diesen, wie auch für die Schweregrade <i>1 - Alarm</i> und <i>0 - Notfall</i>, Meldungen protokolliert.                 </div> |
| <b>IP-Adresse/<br/>DNS-Name:</b> | Geben Sie die IP-Adresse oder den Namen des Servers an, an welchen die Syslog-Meldungen zu senden sind.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Port:</b>                     | Geben Sie den Port – üblicherweise 514 – an, auf welchem der Syslog-Server eingehende Meldungen annimmt.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Protokoll:</b>                | Wählen Sie das Protokoll – üblicherweise UDP – aus, auf welchem der Syslog-Server eingehende Meldungen annimmt: <ul style="list-style-type: none"> <li>▪ <b>TCP</b></li> <li>▪ <b>UDP</b></li> </ul>                                                                                                                                                                                                                                                                                                          |

5. Klicken Sie auf **Speichern**.

## Lokale Syslog-Meldung einsehen und speichern

Haben Sie die Protokollierung von lokalen Syslog-Meldungen aktiviert, können Sie diese Syslog-Meldung im Informationsdialog aufrufen und gegebenenfalls speichern.

**So können Sie die lokalen Syslog-Meldungen einsehen und ggf. speichern:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Syslog**.
4. Klicken Sie auf **Syslog abrufen**.

Die lokalen Syslog-Meldungen werden jetzt abgerufen und im Textfeld angezeigt.

**TIPP:** Klicken Sie gegebenenfalls auf **Syslog speichern**, um die Meldungen in einer Textdatei zu speichern.

5. Klicken Sie auf das rote **[X]**, um den Dialog zu verlassen.

## Benutzerauthentifizierung mit Verzeichnisdiensten

In unternehmensinternen Netzwerken werden die Benutzerkonten häufig zentral durch einen Verzeichnisdienst verwaltet. Das Gerät kann auf einen solchen Verzeichnisdienst zugreifen und Benutzer gegen den Verzeichnisdienst authentisieren.

**HINWEIS:** Scheitert die Authentifizierung des Benutzerkontos *Admin* durch den Verzeichnisdienst, wird das Benutzerkonto gegen die Datenbank des Gerätes authentifiziert!

Der Verzeichnisdienst wird ausschließlich zur Authentifizierung eines Benutzers verwendet. Die Vergabe von Rechten erfolgt durch die Datenbank des KVM-Systems. Hierbei wird zwischen folgenden Szenarien unterschieden:

- **Das Benutzerkonto existiert im Verzeichnisdienst und im KVM-System.**

Der Benutzer kann sich mit dem im Verzeichnisdienst gespeicherten Passwort anmelden. Nach erfolgreicher Anmeldung werden dem Benutzer die Rechte des gleichnamigen Kontos im KVM-System zugewiesen.

**HINWEIS:** Das Passwort, mit dem sich der Benutzer erfolgreich angemeldet hat, wird in die Datenbank des KVM-Systems übernommen.

■ **Das Benutzerkonto existiert im Verzeichnisdienst, aber nicht im KVM-System**

Ein Benutzer, der erfolgreich gegen den Verzeichnisdienst authentifiziert wurde, aber kein gleichnamiges Konto in der Datenbank des KVM-Systems besitzt, wird mit den Rechten des Benutzers *RemoteAuth* ausgestattet.

Ändern Sie ggf. die Rechte dieses speziellen Benutzerkontos, um die Berechtigung von Benutzern ohne eigenes Konto einzustellen.

**TIPP:** Deaktivieren Sie den Benutzer *RemoteAuth*, um die Anmeldung von Benutzern ohne eigenes Benutzerkonto im KVM-System zu verhindern.

■ **Das Benutzerkonto existiert im KVM-System, aber nicht im Verzeichnisdienst**

Ist der Verzeichnisdienst erreichbar, meldet dieser, dass das Benutzerkonto nicht existiert. Der Zugang zum KVM-System wird dem Benutzer verwehrt.

Ist der Server nicht erreichbar, aber der Fallback-Mechanismus aktiviert, kann sich der Benutzer mit dem im KVM-System gespeicherten Passwort anmelden.

**WICHTIG:** Um zu vermeiden, dass bei Ausfall der Verbindung zum Verzeichnisdienst die Anmeldung eines im Verzeichnisdienst gesperrten oder deaktivierten Benutzers möglich ist, beachten Sie folgende Sicherheitsregeln:

- Wird im Verzeichnisdienst ein Benutzerkonto deaktiviert oder gelöscht, ist diese Aktion auch in der Benutzerdatenbank des KVM-Systems durchzuführen!
- Aktivieren Sie den Fallback-Mechanismus nur in begründeten Ausnahmefällen.

**WICHTIG:** Bei Verwendung der Zwei-Faktor-Authentifizierung (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* ab Seite 34) kann der Fallback-Mechanismus **nicht** genutzt werden.

**So konfigurieren Sie die Authentifizierung von Benutzerkonten:**

**HINWEIS:** Wird kein Verzeichnisdienst eingesetzt, werden die Benutzerkonten durch das Gerät verwaltet.

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Authentifizierung**.

5. Erfassen Sie im Abschnitt **Authentifizierungsdienst** folgende Daten:

**Authentifizierungs-server:** Wählen Sie die Option **Lokal**, wenn die Benutzerverwaltung durch das KVM-System erfolgen soll.

Möchten Sie einen bestimmten externen Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus:

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

Erfassen Sie nach der Auswahl eines externen Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers in der sich öffnenden entsprechenden Dialogmaske.

**HINWEIS:** Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 41).

**Fallback:** Aktivieren Sie diese Option, falls die lokale Benutzerverwaltung des KVM-Systems verwendet werden soll, wenn der Verzeichnisdienst temporär nicht verfügbar ist.

**WICHTIG:** Um zu vermeiden, dass bei Ausfall der Verbindung zum Verzeichnisdienst die Anmeldung eines im Verzeichnisdienst gesperrten oder deaktivierten Benutzers möglich ist, beachten Sie folgende Sicherheitsregeln:

- Wird im Verzeichnisdienst ein Benutzerkonto deaktiviert oder gelöscht, ist diese Aktion auch in der Benutzerdatenbank des KVM-Systems durchzuführen!
- Aktivieren Sie den Fallback-Mechanismus nur in begründeten Ausnahmefällen.

**WICHTIG:** Bei Verwendung der Zwei-Faktor-Authentifizierung (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* auf Seite 34) kann der Fallback-Mechanismus **nicht** genutzt werden.

6. Klicken Sie auf **Speichern**.

## Einrichtung der Zwei-Faktor-Authentifizierung am Gerät

Die standardmäßige Benutzer-Authentifizierung erfolgt über eine Passwort-Abfrage. Um die Sicherheit zu erhöhen, kann durch die Zwei-Faktor-Authentifizierung (2FA) ein zweiter, besitzbasierter Faktor abgefragt werden. Hierbei kommt ein Time-Based-One-Time-Password (TOTP) zum Einsatz, wobei es sich um ein zeitlich begrenzt gültiges und nur einmalig nutzbares Passwort handelt. Es können Authenticator-Apps oder Hardware-Tokens verwendet werden.

Für den Einsatz der 2FA ist zunächst die Unterstützung am jeweiligen Gerät zu aktivieren.

**WICHTIG:** Wenn Sie keinen Zugriff auf Ihren besitzbasierten Faktor mehr haben oder er kaputt geht, verlieren Sie den Zugang zum System. Sorgen Sie für diesen Fall vor, indem Sie z. B. bei Verwendung des internen OTP-Servers die Notfall-Codes geschützt an einem sicheren Ort aufbewahren und die Einstellungen so wählen, dass das Risiko eines Zugriffsverlusts minimiert wird (siehe *Aktivierung der Zwei-Faktor-Authentifizierung* ab Seite 42).

### So aktivieren Sie die 2FA am Gerät:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Doppelklicken Sie auf das zu konfigurierende Gerät.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **2-Faktor-Authentifizierung (2FA)**.

5. Erfassen Sie im Abschnitt 2-Faktor-Authentifizierung folgende Daten:

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>2FA-Unterstützung:</b>                             | <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b> (<i>Standard</i>)</li> <li>▪ <b>Aktiviert</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>OTP-Server:</b>                                    | <p>Wählen Sie die Option <b>Intern</b> (<i>Standard</i>), wenn ein interner, im Gerät bereitgestellter Authentifizierungsserver zum Einsatz kommen soll.</p> <p>Möchten Sie einen bestimmten externen Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus:</p> <ul style="list-style-type: none"> <li>▪ <b>LDAP</b></li> <li>▪ <b>Active Directory</b></li> <li>▪ <b>Radius</b></li> <li>▪ <b>TACACS+</b></li> </ul> <p>Erfassen Sie nach der Auswahl eines externen Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers in der sich öffnenden entsprechenden Dialogmaske.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>HINWEIS:</b> Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe <i>Anlegen eines neuen Benutzerkontos</i> ab Seite 41).</p> </div> |
| <b>Login nur für Benutzer mit konfigurierter 2FA:</b> | <p>Kommt der interne OTP-Server zum Einsatz, kann festgelegt werden, ob ein Login von Benutzern ohne eine aktivierte 2FA zulässig ist (<i>Standard</i>) oder verhindert werden soll. Mit dieser Option kann z. B. eine Übergangszeit zur Einrichtung der OTPs ermöglicht werden.</p> <ul style="list-style-type: none"> <li>▪ <b>Nein</b> (<i>Standard</i>)</li> <li>▪ <b>Ja</b></li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>WICHTIG:</b> Kommt ein externer Verzeichnisdienst zum Einsatz wird für <b>jedes</b> Benutzerprofil der zweite Faktor beim Login verlangt.</p> </div>                                                                                                                                                                                                                                                                                                  |

6. Klicken Sie auf **Speichern**.

**WICHTIG:** Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 27). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 28).

Informationen zur Aktivierung der Zwei-Faktor-Authentifizierung finden Sie auf Seite 42 ff.

# Monitoring-Funktionen

## Alle Monitoring-Werte einsehen

Die Liste aller Monitoring-Werte können Sie im Themenbereich **RemoteGateways** einsehen.

**So öffnen Sie die Liste aller Monitoring-Werte:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu prüfende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Monitoring**.

Die angezeigte Tabelle enthält eine Auflistung aller verfügbaren Monitoring-Werte.

4. Klicken Sie auf **Schließen**.

## Monitoring-Werte deaktivieren

Jeden Monitoring-Wert können Sie *separat* ein- und ausschalten. Alternativ können Sie alle Monitoring-Werte *gemeinsam* ein- oder ausschalten.

Die deaktivierten Monitoring-Werte werden *nicht* in der Webapplikation angezeigt.

**WICHTIG:** Zu deaktivierten Monitoring-Werte erscheinen *keine* Warnungen in der Webapplikation!

### So (de)aktivieren Sie einen *einzelnen* Monitoring-Wert:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Monitoring**.
4. Schalten Sie den Schieberegler in der Spalte **Aktiviert** des gewünschten Monitoring-Wertes nach rechts (aktiviert) oder nach links (deaktiviert).
5. Klicken Sie auf **Speichern**.

### So (de)aktivieren Sie *alle* Monitoring-Werte:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Monitoring**.
4. Schalten Sie das Kontrollkästchen im Spaltenkopf **Aktiviert** an oder aus, um alle Werte gemeinsam an- oder auszuschalten.
5. Klicken Sie auf **Speichern**.

## Erweiterte Funktionen zur Verwaltung der kritischen Geräte

Das Icon **Monitoring-Status** (siehe *Die Benutzeroberfläche* auf Seite 5) zeigt Ihnen auf den ersten Blick, ob alle Monitoringwerte im Normbereich sind (grünes Icon) oder mindestens ein Monitoring-Wert auffällig ist (gelbes oder rotes Icon).

Das Icon *Monitoring-Status* nimmt jeweils die Farbe des *schlechtesten* Monitoring-Wertes an.

### Auflistung der kritischen Monitoring-Werte einsehen

Wird das Icon **Monitoring-Status** in gelber oder roter Farbe angezeigt, gelangen Sie mit einem Klick auf das Icon in den Dialog **Aktive Alarme**.

Im Dialog *Aktive Alarme* werden die kritischen Werte aufgelistet.

### Alarm eines kritischen Gerätes bestätigen

Viele Alarm-Meldungen erfordern ein sofortiges Handeln des Administrators. Andere Alarm-Meldungen hingegen (beispielsweise der Ausfall der redundanten Stromversorgung) weisen auf möglicherweise unkritische Sachverhalte hin.

In einem solchen Fall, kann die Alarm-Meldung eines Wertes bestätigt werden. Der Wert wird dadurch von **Alarm** (rot) auf **Warnung** (gelb) zurückgestuft.

#### So bestätigen Sie die Monitoring-Meldungen eines Gerätes:

1. Klicken Sie auf das rote Icon **Monitoring-Status** rechts oben.
2. Markieren Sie den zu bestätigenden Alarm.
3. Klicken Sie auf **Bestätigen**.

# Benutzer und Gruppen

## Effizienter Einsatz der Rechteverwaltung

Die Webapplikation verwaltet maximal 256 Benutzerkonten sowie die gleiche Anzahl an Benutzergruppen. Jeder Benutzer des Systems kann Mitglied von bis zu 20 Benutzergruppen sein.

Sowohl einem Benutzerkonto als auch einer Benutzergruppe können verschiedene Rechte innerhalb des Systems zugeordnet werden.

**TIPP:** Bei entsprechender Planung und Umsetzung der Benutzergruppen sowie der zugeordneten Rechte, ist es möglich, die Rechteverwaltung nahezu vollständig über die Benutzergruppen zu erledigen.

Änderungen an den Rechten der Benutzer können so besonders schnell und effizient durchgeführt werden.

## Das Effektivrecht

Welche Berechtigung ein Benutzer für eine bestimmte Operation hat, wird anhand des Effektivrechts des Benutzers ermittelt.

**WICHTIG:** Das Effektivrecht ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

**BEISPIEL:** Der Benutzer *Muster* ist Mitglied der Gruppen *Office* und *TargetConfig*.

Die folgende Tabelle zeigt die Rechte des Benutzerkontos und der zugeordneten Gruppen sowie das daraus abgeleitete Effektivrecht:

| Recht                   | Benutzer<br><i>Muster</i> | Gruppe<br><i>Office</i> | Gruppe<br><i>TargetConfig</i> | Effektivrecht |
|-------------------------|---------------------------|-------------------------|-------------------------------|---------------|
| Config Panel Login      | Nein                      | Ja                      | Ja                            | Ja            |
| Eigenes Passwort ändern | Nein                      | Ja                      | Nein                          | Ja            |

Das Effektivrecht der Rechte und resultieren aus den Rechten der Benutzergruppen.

In den Dialogmasken der Webapplikation wird hinter jeder Einstellung zusätzlich das Effektivrecht angezeigt.

**TIPP:** Klicken Sie in den Dialogen der Benutzerkonfiguration auf **i**, um eine Auflistung der dem Benutzerkonto zugeordneten Gruppen sowie der dort vergebenen Rechte zu erhalten.

## Effizienter Einsatz der Benutzergruppen

Durch den Einsatz von Benutzergruppen ist es möglich, für mehrere Benutzer mit identischen Kompetenzen, ein gemeinsames Rechteprofil zu erstellen und die Benutzerkonten der Mitgliederliste der Gruppe hinzuzufügen. Dies erspart die individuelle Konfiguration der Rechte der Benutzerkonten dieser Personen und erleichtert die Administration der Rechte innerhalb des Systems.

Werden die Rechte über Benutzergruppen gesteuert, so werden im Benutzerprofil ausschließlich die allgemeinen Daten des Benutzers sowie benutzerbezogene Einstellungen gespeichert.

Bei der Ersteinrichtung des Systems ist es empfehlenswert, verschiedene Gruppen für Anwender mit unterschiedlichen Kompetenzen einzurichten (z. B. *Office* und *IT*) und die entsprechenden Benutzerkonten zuzuordnen.

Ist eine weitere Differenzierung zwischen den Kompetenzen der Anwender erforderlich, können weitere Gruppen eingerichtet werden.

**BEISPIEL:** Sollen einige Benutzer der Gruppe *Office* die Berechtigung zum *Monitoring-Alarm bestätigen* erhalten, bieten sich folgende Möglichkeiten an, dies mit Benutzergruppen zu realisieren:

- Sie erstellen eine Benutzergruppe (z. B. *Office\_Monitoring*), mit den identischen Einstellungen der Gruppe *Office*. Das Recht *Monitoring-Alarm bestätigen* wird abschließend *aktiviert*. Ordnen Sie dieser Gruppe die entsprechenden Benutzerkonten zu.
- Sie erstellen eine Benutzergruppe (z. B. *Monitoring*) und setzen ausschließlich das Recht *Monitoring-Alarm bestätigen* auf *aktiviert*. Ordnen Sie dieser Gruppe die entsprechenden Benutzerkonten – *zusätzlich* zur Gruppe *Office* – zu.

In beiden Fällen erhält der Benutzer durch die Gruppen das Effektivrecht *Ja* für das *Monitoring-Alarm bestätigen*.

**HINWEIS:** Möchten Sie einem Benutzer der Gruppe ein erweitertes Recht zuordnen, kann dies alternativ auch direkt im Benutzerprofil geändert werden.

## Verwaltung von Benutzerkonten

Durch die Verwendung von Benutzerkonten besteht die Möglichkeit, die Rechte des Benutzers individuell festzulegen. Zusätzlich zu den Rechten können im persönlichen Profil einige benutzerbezogene Einstellungen festgelegt werden.

**WICHTIG:** Der Administrator sowie alle Benutzer mit aktiviertem *Superuser*-Recht sind berechtigt, Benutzer anzulegen, zu löschen und die Rechte sowie die benutzerbezogenen Einstellungen zu editieren.

## Anlegen eines neuen Benutzerkontos

Die Webapplikation verwaltet maximal 256 Benutzerkonten. Jedes Benutzerkonto verfügt über individuelle Login-Daten, Rechte und benutzerbezogene Einstellungen für das KVM-System.

### So erstellen Sie ein neues Benutzerkonto:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**.
3. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

|                                                                                                                                                                                                                    |                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Name:</b>                                                                                                                                                                                                       | Geben Sie den gewünschten Benutzernamen ein.                                                                               |
| <b>HINWEIS:</b> Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe <i>Benutzerauthentifizierung mit Verzeichnisdiensten</i> ab Seite 31). |                                                                                                                            |
| <b>Passwort:</b>                                                                                                                                                                                                   | Geben Sie das Passwort des Benutzerkontos ein.                                                                             |
| <b>Passwort bestätigen:</b>                                                                                                                                                                                        | Wiederholen Sie das oben eingegebene Passwort.                                                                             |
| <b>Klartext:</b>                                                                                                                                                                                                   | Aktivieren Sie ggf. dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können. |
| <b>Vollständiger Name:</b>                                                                                                                                                                                         | Geben Sie hier – falls gewünscht – den vollständigen Namen des Benutzers ein.                                              |
| <b>Kommentar:</b>                                                                                                                                                                                                  | Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto.                                        |
| <b>Aktiviert:</b>                                                                                                                                                                                                  | Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.                                                |
| <b>HINWEIS:</b> Ist das Benutzerkonto deaktiviert, wird dem Benutzer der Zugriff auf das KVM-System verweigert.                                                                                                    |                                                                                                                            |

4. Klicken Sie auf **Speichern**.

**WICHTIG:** Unmittelbar nach der Erstellung verfügt das Benutzerkonto über keinerlei Rechte innerhalb des KVM-Systems.

5. Falls die Zwei-Faktor-Authentifizierung am Gerät aktiviert ist (s. Seite 34), sind im Folgenden die Einstellungen für das Benutzerkonto vorzunehmen (s. Seite 42).

## Aktivierung der Zwei-Faktor-Authentifizierung

**HINWEIS:** Für die Verwendung der Zwei-Faktor-Authentifizierung (2FA) muss zunächst die Einrichtung am Gerät erfolgen (s. Seite 34).

Wird der interne OTP-Server für die 2FA genutzt, kann diese für fast jedes Benutzerprofil (Ausnahme: Benutzer *RemoteAuth*) aktiviert werden. Zur Aktivierung werden neben dem eigentlichen Schlüssel, welcher automatisch generiert werden kann, weitere steuernde Parameter zur Generierung des Sicherheitsschlüssels herangezogen. Der Schlüssel und die steuernden Parameter können vom Benutzer modifiziert werden. Dies ist für die Einrichtung von Hardware-Tokens notwendig. Wenn Authenticator-Apps zum Einsatz kommen, müssen die Parameter in der Regel nicht modifiziert werden.

**WICHTIG:** Kommt ein externer Verzeichnisdienst zum Einsatz (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* ab Seite 34), wird für jedes Benutzerprofil innerhalb der Datenbank die 2FA automatisch aktiviert. Somit ist ein Login am Gerät nur möglich, sofern der externe OTP-Server die identischen Benutzerprofile bereithält und den zweiten Faktor erfolgreich validiert.

**WICHTIG:** Um die 2FA für ein Benutzerprofil zu aktivieren oder zu deaktivieren, benötigt der Anwender Superuser-Rechte (s. Seite 52), oder der Anwender muss mit dem entsprechenden Benutzerprofil angemeldet sein (s. Seite 52) und über das Recht *Eigenes Passwort ändern* (s. Seite 53) verfügen.

**WICHTIG:** Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 27). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 28).

**HINWEIS:** Die 2FA kann für fast alle Benutzerprofile aktiviert werden. Einzige Ausnahme stellt hier der Benutzer *RemoteAuth* dar.

### So aktivieren Sie die 2FA im Benutzerkonto:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Klicken Sie in der Zeile **2-Faktor-Authentifizierung** auf **Bearbeiten**.
4. Wählen Sie **Aktiviert** im Abschnitt **2FA für diesen Benutzer** aus.

## 5. Erfassen Sie im Menü folgende Daten:

|                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Schlüssel:</b>                                                                                                                                                                                                                                        | Beim Wechsel des Parameters <b>2FA für diesen Benutzer</b> von <b>Deaktiviert</b> auf <b>Aktiviert</b> , wird automatisch ein Schlüssel generiert und angezeigt.                                                                                                                                                                 |
| <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <b>WICHTIG:</b> Eine Eingabe muss im <b>Base32-Format</b> erfolgen.     </div>                                                                                                      |                                                                                                                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                                                                          | Klicken Sie auf <b>Generieren</b> , um einen neuen Schlüssel zu erhalten.                                                                                                                                                                                                                                                        |
| <b>Hash-Algorithmus:</b>                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>▪ <b>SHA1</b></li> <li>▪ <b>SHA256</b> (<i>Standard</i>)</li> <li>▪ <b>SHA512</b></li> </ul>                                                                                                                                                                                              |
| <b>Gültigkeitsdauer (Sek.):</b>                                                                                                                                                                                                                          | Erfassen Sie hier, wie lange das Einmal-Passwort gültig sein soll. Der eingetragene Wert muss zwischen <b>10</b> und <b>200</b> Sekunden liegen ( <i>Standard: 30 Sekunden</i> ).                                                                                                                                                |
| <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <b>TIPP:</b> Es ist sinnvoll, die Gültigkeitsdauer nicht zu klein zu wählen, da es durch evtl. nicht synchronisierte Zeit ansonsten zu Zugriffsproblemen kommen könnte.     </div>  |                                                                                                                                                                                                                                                                                                                                  |
| <b>Länge des Einmal-Passworts:</b>                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>▪ <b>6 Stellen</b> (<i>Standard</i>)</li> <li>▪ <b>8 Stellen</b></li> </ul>                                                                                                                                                                                                               |
| <b>Fensterbreite des Einmal-Passworts:</b>                                                                                                                                                                                                               | Mit der Fensterbreite legen Sie fest, wie viele vorherige Einmal-Passwörter neben dem aktuellen gültig sind. Es ist hierbei <b>nicht</b> möglich zukünftige Einmal-Passwörter zu erlauben. Der eingetragene Wert muss zwischen <b>1</b> und <b>20</b> liegen ( <i>Standard: 1</i> ).                                             |
| <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <b>TIPP:</b> Um durch evtl. nicht synchronisierte Zeit auftretende Zugriffsprobleme zu vermeiden, kann es sinnvoll sein, mehrere vorherige Einmal-Passwörter zuzulassen.     </div> |                                                                                                                                                                                                                                                                                                                                  |
| <b>QR-Code zeigen &amp; Sicherheits-schlüssel kopieren:</b>                                                                                                                                                                                              | Durch Klicken des Buttons werden die getätigten Eingaben validiert. Es wird ein Sicherheitsschlüssel generiert und ein QR-Code angezeigt, der den generierten Sicherheitsschlüssel beinhaltet und zum Einscannen mit einer Authenticator-App verwendet werden kann. Der Sicherheitsschlüssel wird in die Zwischenablage kopiert. |
| <b>Verifikations-code:</b>                                                                                                                                                                                                                               | Erfassen Sie hier den Verifikationscode, den Sie über einen verwendeten Hardware-Token oder eine eingesetzte Authenticator-App erhalten. In diesem Feld ist nur die Eingabe von Ziffern zulässig.                                                                                                                                |

6. Klicken Sie auf **Speichern**.

**WICHTIG:** Nach erfolgreicher Aktivierung der 2FA bei Verwendung des internen OTP-Servers erscheint in der Zeile **2-Faktor-Authentifizierung** der zusätzliche Button **Notfall-Codes**. Wenn Sie diesen Button anklicken, werden Ihnen fünf Notfall-Codes angezeigt. Durch diese Notfall-Codes wird ein Zugriff zum Benutzerkonto jeweils **einmalig** ermöglicht. Diese Codes laufen zeitlich **nicht** ab. Die Codes sollten geschützt an einem sicheren Ort aufbewahrt werden. Die Notfall-Codes sind z. B. bei Verlust eines Hardware-Tokens einsetzbar, um weiterhin Zugriff auf das System zu haben.

Klicken Sie auf **Neue Codes erhalten**, falls Sie fünf neue Codes erstellen wollen.

**HINWEIS:** Ein Benutzer, der erfolgreich gegen den Verzeichnisdienst authentifiziert wurde, aber kein gleichnamiges Konto in der Datenbank des KVM-Systems besitzt, wird mit den Rechten des Benutzers *RemoteAuth* ausgestattet. Das OTP wird über den konfigurierten, externen OTP-Server validiert.

Ändern Sie ggf. die Rechte dieses speziellen Benutzerkontos, um die Berechtigung von Benutzern ohne eigenes Konto einzustellen (siehe *Änderung der Rechte eines Benutzerkontos* ab Seite 46).

Deaktivieren Sie den Benutzer *RemoteAuth*, um die Anmeldung von Benutzern ohne eigenes Benutzerkonto im KVM-System zu verhindern (siehe *Aktivierung oder Deaktivierung eines Benutzerkontos* auf Seite 48).

Nachdem die 2FA im Benutzerkonto erfolgreich aktiviert wurde, wird beim Login (siehe *Start der Webapplikation* auf Seite 4) zusätzlich zur Eingabe des Benutzer-  
namens und des Passwortes das Einmal-Passwort (TOTP) abgefragt.

## Änderung des Namens eines Benutzerkontos

### So ändern Sie den Namen eines Benutzerkontos:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Geben Sie im Feld **Name** den gewünschten Benutzernamen ein.
4. *Optional:* Geben Sie im Feld **Vollständiger Name** den vollständigen Namen des Benutzers ein.
5. Klicken Sie auf **Speichern**.

**HINWEIS:** Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Benutzerauthentifizierung mit Verzeichnisdiensten* ab Seite 31).

## Änderung des Passworts eines Benutzerkontos

**HINWEIS:** Voraussetzung für die Änderung des Passworts eines Benutzerkontos ist das aktivierte *Superuser*-Recht (siehe *Berechtigung zum uneingeschränkten Zugriff (Superuser)* ab Seite 52) oder das Recht *Eigenes Passwort ändern* (siehe *Berechtigung zur Änderung des eigenen Passworts* ab Seite 53).

### So ändern Sie das Passwort eines Benutzerkontos:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Ändern Sie folgende Daten innerhalb der Dialogmaske:

|                             |                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Passwort:</b>            | Geben Sie das neue Passwort ein.                                                                                      |
| <b>Passwort bestätigen:</b> | Wiederholen Sie das oben eingegebene Passwort.                                                                        |
| <b>Klartext:</b>            | Aktivieren Sie dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können. |

4. Klicken Sie auf **Speichern**.

## Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

Die folgende Tabelle listet die verschiedenen Berechtigungen auf. Weiterführende Hinweise zu den Rechten finden Sie auf den angegebenen Seiten.

| Bezeichnung                        | Berechtigung                                                      | Seite    |
|------------------------------------|-------------------------------------------------------------------|----------|
| <b>Eigenes Passwort ändern</b>     | Änderung des eigenen Passworts                                    | Seite 53 |
| <b>Superuser-Recht</b>             | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 52 |
| <b>Config Panel Login</b>          | Login mit der Webapplikation <i>ConfigPanel</i>                   | Seite 52 |
| <b>Monitoring-Alarm bestätigen</b> | Bestätigung eines Monitoring-Alarms                               | Seite 53 |

## Änderung der Gruppenzugehörigkeit eines Benutzerkontos

**HINWEIS:** Jeder Benutzer des Systems kann Mitglied von bis zu 20 Benutzergruppen sein.

### So ändern Sie die Gruppenzugehörigkeit eines Benutzerkontos:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Mitgliedschaft**.
4. Schalten Sie den Schieberegler der Gruppe, der der Benutzer hinzugefügt werden soll, in der Spalte **Mitglied** nach rechts (aktiviert).

**TIPP:** Verwenden Sie ggf. das *Suchen*-Feld, um die im Auswahlfenster anzuzeigenden Benutzergruppen einzugrenzen.

5. Schalten Sie den Schieberegler der Gruppe, aus der der Benutzer entfernt werden soll, in der Spalte **Mitglied** nach links (deaktiviert).

**TIPP:** Verwenden Sie ggf. das *Suchen*-Feld, um die im Auswahlfenster anzuzeigenden Benutzergruppen einzugrenzen.

6. Klicken Sie auf **Speichern**.

## Aktivierung oder Deaktivierung eines Benutzerkontos

**WICHTIG:** Ist das Benutzerkonto deaktiviert, wird dem Benutzer der Zugriff auf das KVM-System verweigert.

### So aktivieren oder deaktivieren Sie ein Benutzerkonto:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Benutzerkonto zu aktivieren.  
Möchten Sie den Zugang zum System mit diesem Benutzerkonto sperren, so deaktivieren Sie das Kontrollkästchen.
4. Klicken Sie auf **Speichern**.

### Löschen eines Benutzerkontos

#### So löschen Sie ein Benutzerkonto:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu löschende Benutzerkonto und anschließend auf **Löschen**.
3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

## Verwaltung von Benutzergruppen

Durch den Einsatz von *Benutzergruppen* ist es möglich, für mehrere Benutzer mit identischen Kompetenzen ein gemeinsames Rechteprofil zu erstellen und die Benutzerkonten als Mitglieder dieser Gruppe hinzuzufügen.

Dies erspart die individuelle Konfiguration der Rechte von Benutzerkonten dieser Personen und erleichtert die Administration der Rechte innerhalb des KVM-Systems.

**HINWEIS:** Der Administrator sowie alle Benutzer mit aktiviertem *Superuser*-Recht sind berechtigt, Benutzergruppen anzulegen, zu löschen und die Rechte sowie die Mitgliederliste zu editieren.

### Anlegen einer neuen Benutzergruppe

Innerhalb des Systems können Sie bis zu 256 Benutzergruppen erstellen.

**So erstellen Sie eine neue Benutzergruppe:**

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf **Benutzergruppe hinzufügen**.
3. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

|                   |                                                                                     |
|-------------------|-------------------------------------------------------------------------------------|
| <b>Name:</b>      | Geben Sie den gewünschten Benutzernamen ein.                                        |
| <b>Kommentar:</b> | Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto. |
| <b>Aktiviert:</b> | Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.         |

**HINWEIS:** Ist die Benutzergruppe deaktiviert, wirken sich die Rechte der Gruppe *nicht* auf die zugeordneten Mitglieder aus.

4. Klicken Sie auf **Speichern**.

**WICHTIG:** Unmittelbar nach der Erstellung verfügt die Benutzergruppe über keinerlei Rechte innerhalb des Systems.

## Änderung des Namens einer Benutzergruppe

So ändern Sie den Namen einer Benutzergruppe:

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Geben Sie im Feld **Name** den gewünschten Gruppennamen ein.
4. Klicken Sie auf **Speichern**.

## Änderung der Rechte einer Benutzergruppe

Den verschiedenen Benutzergruppen können differenzierte Berechtigungen erteilt werden.

Die folgende Tabelle listet die verschiedenen Berechtigungen auf. Weiterführende Hinweise zu den Rechten finden Sie auf den angegebenen Seiten.

| Bezeichnung                        | Berechtigung                                                      | Seite    |
|------------------------------------|-------------------------------------------------------------------|----------|
| <b>Eigenes Passwort ändern</b>     | Änderung des eigenen Passworts                                    | Seite 53 |
| <b>Superuser-Recht</b>             | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 52 |
| <b>Config Panel Login</b>          | Login mit der Webapplikation <i>ConfigPanel</i>                   | Seite 52 |
| <b>Monitoring-Alarm bestätigen</b> | Bestätigung eines Monitoring-Alarms                               | Seite 53 |

## Mitgliederverwaltung einer Benutzergruppe

### So verwalten Sie die Mitglieder einer Benutzergruppe:

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Mitglieder**.
4. Schalten Sie den Schieberegler der in die Gruppe aufzunehmenden Benutzer in der Spalte **Mitglied** nach rechts (aktiviert).

**TIPP:** Verwenden Sie ggf. das *Suchen*-Feld, um die im Auswahlfenster anzuzeigenden Benutzer einzugrenzen.

5. Schalten Sie den Schieberegler der aus der Gruppe zu entfernenden Benutzer in der Spalte **Mitglied** nach links (deaktiviert).

**TIPP:** Verwenden Sie ggf. das *Suchen*-Feld, um die im Auswahlfenster anzuzeigenden Benutzer einzugrenzen.

6. Klicken Sie auf **Speichern**.

## Aktivierung oder Deaktivierung einer Benutzergruppe

### So aktivieren oder deaktivieren Sie eine Benutzergruppe:

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Aktivieren Sie die Benutzergruppe mit dem Schieberegler **Aktiviert**.  
Möchten Sie den Mitgliedern der Benutzergruppe den Zugang zum KVM-System sperren, so deaktivieren Sie das Kontrollkästchen.
4. Klicken Sie auf **Speichern**.

## Löschen einer Benutzergruppe

### So löschen Sie eine Benutzergruppe:

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf die zu löschende Benutzergruppe und anschließend auf **Löschen**.
3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

## System-Rechte

### Berechtigung zum uneingeschränkten Zugriff (Superuser)

Das *Superuser*-Recht erlaubt einem Benutzer den uneingeschränkten Zugriff auf die Konfiguration des KVM-Systems.

**HINWEIS:** Die Informationen über die zuvor zugewiesenen Rechte des Benutzers bleiben bei der Aktivierung des *Superuser*-Rechtes weiterhin gespeichert und werden bei Entzug des Rechtes wieder aktiviert.

#### So ändern Sie die Berechtigung zum uneingeschränkten Zugriff:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Superuser-Recht** zwischen folgenden Optionen:

|                     |                                                                                       |
|---------------------|---------------------------------------------------------------------------------------|
| <b>Aktiviert:</b>   | Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte erlaubt   |
| <b>Deaktiviert:</b> | Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte untersagt |

5. Klicken Sie auf **Speichern**.

### Berechtigung zum Login in die Webapplikation

#### So ändern Sie die Berechtigung zum Login mit der Webapplikation:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Config Panel Login** zwischen folgenden Optionen:

|                     |                                          |
|---------------------|------------------------------------------|
| <b>Aktiviert:</b>   | Zugriff auf die Webapplikation erlaubt   |
| <b>Deaktiviert:</b> | Zugriff auf die Webapplikation untersagt |

5. Klicken Sie auf **Speichern**.

## Berechtigung zur Änderung des eigenen Passworts

So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Eigenes Passwort ändern** zwischen folgenden Optionen:

|                     |                                                       |
|---------------------|-------------------------------------------------------|
| <b>Aktiviert:</b>   | Passwortänderung des eigenen Benutzerkontos erlaubt   |
| <b>Deaktiviert:</b> | Passwortänderung des eigenen Benutzerkontos untersagt |

5. Klicken Sie auf **Speichern**.

## Berechtigung zur Bestätigung eines Monitoring-Alarms

So ändern Sie die Berechtigung zur Bestätigung eines Monitoring-Alarms:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Monitoring-Alarm bestätigen** zwischen folgenden Optionen:

|                     |                                              |
|---------------------|----------------------------------------------|
| <b>Aktiviert:</b>   | Bestätigung von Monitoring-Alarmen erlaubt   |
| <b>Deaktiviert:</b> | Bestätigung von Monitoring-Alarmen untersagt |

5. Klicken Sie auf **Speichern**.

# Erweiterte Funktionen des KVM-Systems

## Identifizierung eines Gerätes durch Aktivierung der Identification-LED

Einige Geräte sind mit einer *Identification*-LED ausgestattet.

Über die Webapplikation können Sie die LEDs der Geräte ein- bzw. ausschalten, um die Geräte beispielsweise innerhalb eines Racks zu identifizieren.

**So (de)aktivieren Sie die *Identification*-LED eines Gerätes:**

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie den Eintrag **Ident-LED**.
4. Klicken Sie auf **LED an** bzw. **LED aus**.
5. Klicken Sie auf das rote **[X]**, um den Dialog zu verlassen.

## Sicherung der Konfigurationseinstellungen

Konfigurationseinstellungen können über die Backup-Funktion gesichert werden. Das Wiederherstellen der gesicherten Daten ist über die Restore-Funktion möglich.

**So sichern Sie die Konfigurationseinstellungen des :**

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Backup & Restore**.
3. Klicken Sie auf den Reiter **Backup**.
4. *Optional:* Erfassen Sie ein **Passwort** zur Sicherung der Backup-Datei und/oder einen **Kommentar**.
5. Wählen Sie den Umfang der zu speichernden Daten: Sie können wahlweise die **Netzwerkeinstellungen** und/oder die **Anwendungseinstellungen** sichern.
6. Klicken Sie auf **Backup**.

**WICHTIG:** Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

## Sicherung der Konfigurationseinstellungen mit der Auto-Backup-Funktion

Das Gerät kann in einem definierten Intervall ein automatisches Backup auf einem Netzlaufwerk erstellen. Somit müssen Sie kein manuelles Backup anlegen nachdem eine Konfigurationsoption geändert wurde. Das Wiederherstellen der gesicherten Daten ist auch hierbei über die Restore-Funktion möglich.

### So verwenden Sie die Auto-Backup-Funktion:

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Auto-Backup**.
3. Nehmen Sie die folgenden Einstellungen vor:

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Auto-Backup:</b>      | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Auto-Backup-Funktion aus- und einschalten: <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b> (<i>Standard</i>)</li> <li>▪ <b>Aktiviert</b></li> </ul>                                                                                                                                                                        |
| <b>Dateiname-Präfix:</b> | Geben Sie das Dateiname-Präfix ein.<br><b>HINWEIS:</b> Bei Aktivierung der Auto-Backup-Funktion wird das Feld Dateiname-Präfix automatisch mit der <b>UID</b> des Geräts gefüllt. Diesen Eintrag können Sie überschreiben.<br><b>WICHTIG:</b> Es sind ausschließlich Buchstaben (groß- und kleingeschrieben), Ziffern (0 bis 9) und die Zeichen - und _ zugelassen. Das Präfix darf maximal 25 Zeichen enthalten. |
| <b>Backup-Passwort:</b>  | <i>Optional:</i> Erfassen Sie ein Passwort zur Sicherung der Backup-Dateien.<br><b>WICHTIG:</b> Doppelte Anführungszeichen („ und “) sind hier <b>nicht</b> zugelassen.                                                                                                                                                                                                                                           |
| <b>Backup-Umfang:</b>    | Wählen Sie den Umfang der zu speichernden Daten: Sie können wahlweise die <b>Netzwerkeinstellungen</b> und/oder die <b>Anwendungseinstellungen</b> sichern.                                                                                                                                                                                                                                                       |
| <b>Pfad:</b>             | Erfassen Sie den Pfad für die Speicherung der Backup-Dateien.<br><b>WICHTIG:</b> Die Syntax der Pfadangabe unterscheidet sich je nach gewähltem Protokoll.<br><b>Beispiele:</b> <ul style="list-style-type: none"> <li>▪ <b>NFS:</b> <i>name:/verzeichnis1/verzeichnis2</i></li> <li>▪ <b>CIFS:</b> <i>//name/verzeichnis1/verzeichnis2</i></li> </ul>                                                            |

|                           |                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protokoll:</b>         | Wählen Sie zwischen den folgenden Protokollen: <ul style="list-style-type: none"> <li>▪ <b>NFS</b> (<i>Standard</i>)</li> <li>▪ <b>CIFS</b></li> </ul>                                                                                          |
| <b>Port:</b>              | Geben Sie den Port ein. Dieses Feld wird je nach Auswahl im Feld <i>Protokoll</i> automatisch gefüllt: <ul style="list-style-type: none"> <li>▪ <b>2049</b> (bei Auswahl <i>NFS</i>)</li> <li>▪ <b>445</b> (bei Auswahl <i>CIFS</i>)</li> </ul> |
| <b>Benutzer:</b>          | <i>Optional:</i> Erfassen Sie den Namen des Benutzers.                                                                                                                                                                                          |
| <b>Passwort:</b>          | <i>Optional:</i> Erfassen Sie ein Passwort zur Sicherung der Freigabe.                                                                                                                                                                          |
| <b>Uhrzeit:</b>           | Erfassen Sie folgende Daten: <ul style="list-style-type: none"> <li>▪ <b>Stunde</b> (Zahlen 0 bis 23)</li> <li>▪ <b>Minute</b> (Zahlen 0 bis 59)</li> </ul>                                                                                     |
| <b>Auswahl des Tages:</b> | Es stehen Ihnen die folgenden Auswahlmöglichkeiten zur Verfügung: <ul style="list-style-type: none"> <li>▪ <b>1. bis 31. Tag des Monats</b></li> <li>▪ <b>Alle auswählen</b> (jeder Tag des Monats)</li> </ul>                                  |

4. Klicken Sie auf **Speichern & Testen** oder **Speichern**.

**TIPP:** Nutzen Sie **Speichern & Testen** und überprüfen Sie, ob ein Backup erfolgreich mit den gewünschten Parametern gespeichert wurde.

**WICHTIG:** Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

## Wiederherstellung der Konfigurationseinstellungen

So stellen Sie die Konfigurationseinstellungen des wieder her:

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Backup & Restore**.
3. Klicken Sie auf den Reiter **Restore**.
4. Klicken Sie auf **Datei auswählen** und öffnen Sie eine zuvor erstellte Backup-Datei.
5. Prüfen Sie anhand der Informationen der Felder **Erstellungsdatum** und **Kommentar** des Dialogs, ob es sich um die gewünschte Backup-Datei handelt.
6. Wählen Sie den Umfang der zu wiederherzustellenden Daten: Sie können wahlweise die **Netzwerkeinstellungen** und/oder die **Anwendungseinstellungen** wiederherstellen.

**HINWEIS:** Falls während der Sicherung der Daten einer der Bereiche ausgelassen wurde, ist dieser Bereich nicht anwählbar.

**HINWEIS:** Falls bei der Sicherung der Daten ein Passwort eingegeben wurde, wird dieses hier abgefragt.

7. Klicken Sie auf **Restore**.

**WICHTIG:** Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

## Freischaltung kostenpflichtiger Zusatzfunktionen

Bei Erwerb einer kostenpflichtigen Funktion erhalten Sie einen Feature-Key.

Hierbei handelt es sich um eine Datei, die einen Schlüssel zur Freischaltung der von Ihnen gekauften Funktion(en) erhält.

Durch den Import der Datei in die Webapplikation wird/werden die gekaufte(n) Funktion(en) freigeschaltet.

### So importieren Sie einen Feature-Key zur Freischaltung gekaufter Funktionen:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Features**.
4. Klicken Sie auf **Feature-Key aus Datei importieren...** und importieren Sie den Feature-Key (Datei) über den Datei-Dialog.

Der Klartext des Feature-Keys wird nach dem Laden im Textfeld angezeigt.

|                                                                                                              |
|--------------------------------------------------------------------------------------------------------------|
| <b>HINWEIS:</b> Alternativ können Sie den Klartext-Inhalt des Feature-Keys manuell in das Textfeld kopieren. |
|--------------------------------------------------------------------------------------------------------------|

5. Klicken Sie auf **Speichern**.

# 2 RemoteGateways

Im Menü *RemoteGateways* der Webapplikation können Sie verschiedene Einstellungen konfigurieren und Statusinformationen des Gerätes einsehen.

## Grundkonfiguration der RemoteGateways

### Änderung des Namens eines RemoteGateways

So ändern Sie den Namen eines RemoteGateways:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Geben Sie im Feld **Name** des Abschnitts **Gerät** den gewünschten Namen ein.
5. Klicken Sie auf **Speichern**.

### Änderung des Kommentares eines RemoteGateways

Im Listenfeld der Webapplikation wird neben dem Namen eines RemoteGateways auch der erfasste Kommentar angezeigt.

**TIPP:** Verwenden Sie das Kommentarfeld beispielsweise um den Standort des RemoteGateways zu vermerken.

So ändern Sie den Kommentar eines RemoteGateways:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Geben Sie im Feld **Kommentar** des Abschnitts **Gerät** einen beliebigen Kommentar ein.
5. Klicken Sie auf **Speichern**.

# Erweiterte Funktionen für RemoteGateways

## Konfigurationseinstellungen übertragen (Gerät ersetzen)

Wird ein Rechnermodul durch ein anderes Modul ersetzt, können Sie die Konfigurationseinstellungen des bisherigen Moduls auf das neue übertragen. Nach der Übertragung der Konfigurationseinstellungen ist das neue Modul unmittelbar einsatzbereit.

**WICHTIG:** Das Gerät, dessen Einstellungen übertragen werden, wird anschließend aus dem KVM-System gelöscht.

### So übertragen Sie die Konfigurationseinstellungen eines Moduls:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das *neue* Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Gerät ersetzen**.
4. Wählen Sie das *alte* Geräte aus der Liste aus, dessen Konfigurationseinstellungen Sie übertragen möchten.
5. Klicken Sie auf **Speichern**.

## Monitoring-Werte konfigurieren

Im Bereich *Monitoring* können Sie die zu überwachenden Monitoring-Werte festlegen und den Status dieser Werte ablesen.

### Auswahl der zu überwachenden Monitoring-Werte

Das KVM-System überwacht standardmäßig eine Vielzahl verschiedener Werte des Geräts.

Falls von Ihnen gewünscht, können Sie die Auswertung und Überwachung der Eigenschaften eingrenzen.

#### So verwalten Sie die zu überwachenden Monitoring-Werte:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Monitoring**.
4. (De)aktivieren Sie die einzelnen Monitoring-Werte in dem Sie den Regler nach *links* schieben (**aus**) oder nach *rechts* schieben (**an**).

**HINWEIS:** Um *alle* Werte aus- oder einzuschalten können Sie das Kontrollkästchen im Kopf der Spalten **Aktiviert** verwenden.

5. Klicken Sie auf **Speichern**.

## Statusinformationen des Geräts einsehen

So können Sie die Statusinformationen einsehen:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Informationen**.
4. Im jetzt erscheinenden Dialog werden Ihnen folgende Informationen angezeigt:

| RemoteGateways                                                                                |                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name:</b>                                                                                  | Name des Geräts                                                                                                                                        |
| <b>Geräte-ID:</b>                                                                             | physikalische ID des Geräts                                                                                                                            |
| <b>Status:</b>                                                                                | aktueller Status ( <b>Online</b> oder <b>Offline</b> ) des Geräts                                                                                      |
| <b>Klasse:</b>                                                                                | Gerätekategorie                                                                                                                                        |
| Hardware-Informationen                                                                        |                                                                                                                                                        |
| <b>Firmware name:</b>                                                                         | Bezeichnung der Firmware                                                                                                                               |
| <b>Firmware rev.:</b>                                                                         | Firmware-Version                                                                                                                                       |
| <b>Hardware rev.:</b>                                                                         | Hardware-Revision                                                                                                                                      |
| <b>IP-Adresse:</b>                                                                            | IP-Adresse der Schnittstelle                                                                                                                           |
| <b>MAC :</b>                                                                                  | MAC-Adresse der Schnittstelle                                                                                                                          |
| <b>Serial number:</b>                                                                         | Seriennummer des Geräts                                                                                                                                |
| Aktive Features                                                                               |                                                                                                                                                        |
| In diesem Bereich werden alle aktivierten Zusatzfunktionen aufgelistet.                       |                                                                                                                                                        |
| Link-Status                                                                                   |                                                                                                                                                        |
| <b>Link detected:</b>                                                                         | Verbindung zum Netzwerk hergestellt ( <b>ja</b> ) oder unterbrochen ( <b>nein</b> ).                                                                   |
| <b>Auto-negotiation:</b>                                                                      | Die Übertragungsgeschwindigkeit und das Duplex-Verfahren wurden automatisch ( <b>ja</b> ) oder manuell vom Administrator konfiguriert ( <b>nein</b> ). |
| <b>Speed:</b>                                                                                 | Übertragungsgeschwindigkeit                                                                                                                            |
| <b>Duplex:</b>                                                                                | Duplexverfahren ( <b>full</b> bzw. <b>half</b> )                                                                                                       |
| <b>HINWEIS:</b> Zusätzlich werden die <i>Monitoring</i> -Informationen des Gerätes angezeigt. |                                                                                                                                                        |

5. Klicken Sie auf **Schließen**, um die Ansicht zu schließen.











## 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