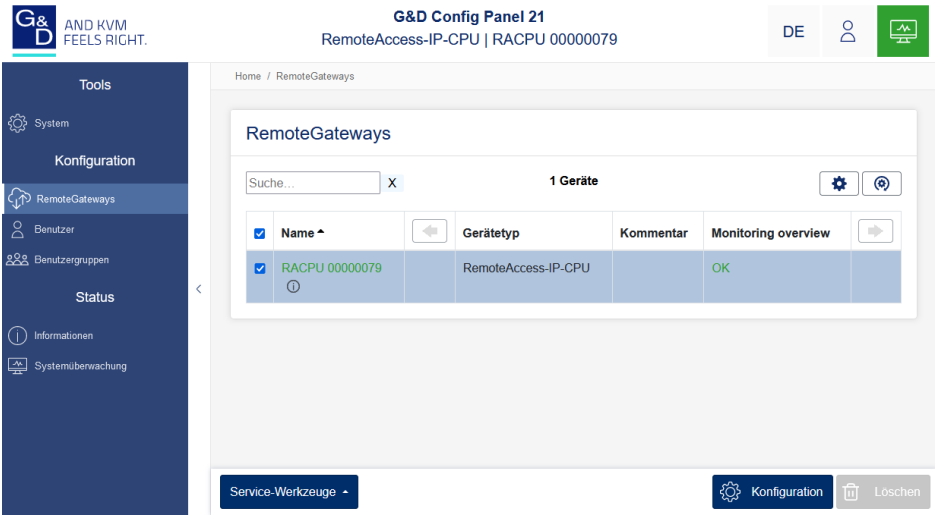
# G&D RemoteAccess-IP-CPU

DE **Webapplikation »Config Panel«**
Konfiguration des Geräts




A9100400-1.20

## 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



**Version 1.20 – 05.09.2025**
Config Panel 21-Version: 1.7.000

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

Telefon +49 (0) 271 23872-0
Telefax +49 (0) 271 23872-120

www.gdsys.com
sales@gdsys.com

# Inhaltsverzeichnis

## Kapitel 1: Grundfunktionen

## Kapitel 2: RemoteGateways

# 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 18
- Google Chrome 137
- Microsoft Edge 134
- Mozilla Firefox 139

## 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: Dynamischer Bezug der Einstellungen

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 Netwerkschnittstelle 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 15 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 3.

**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:

| | |
|---|---|
| **Nutzungsbedingungen zustimmen:** | Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren. |
| | **HINWEIS:** Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde (siehe *Anzeigen von Nutzungsbedingungen* ab Seite 11). |
| **Benutzername:** | Geben Sie Ihren Benutzernamen ein. |
| **Passwort:** | Geben Sie das Passwort Ihres Benutzerkontos ein. |
| **2-Factor Auth Code (TOTP):** | Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein. |
| | **HINWEIS:** Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 46 ff.) und aktiviert wurde (s. Seite 55 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 59).

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:

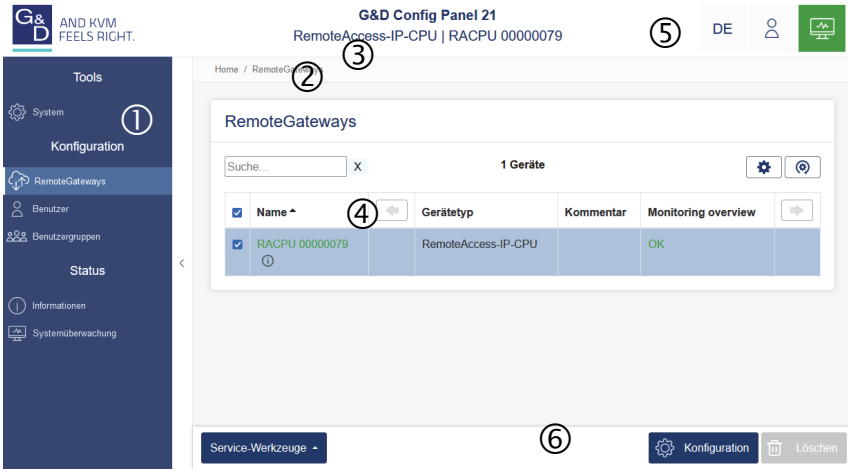



**Abbildung 1: Benutzeroberfläche der Webapplikation**

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

| | |
|---|---|
| **Menü ①:** | Im Menü sind die unterschiedlichen Funktionen der Webapplikation in Themenbereichen zusammengefasst. |
| **Brotkrumen-Navigation ②:** | 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. |
| **Filterfunktion ③:** | 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 *angezeigten* Spalten enthalten. Die Groß-/Kleinschreibung der Namen wird bei der Filterung ignoriert.<br>Um die Filterung aufzuheben, klicken Sie auf **[X]**. |

| | |
|---|---|
| **Hauptansicht ④:** | Nach der Auswahl eines Themenbereichs im Menü werden hier die Inhalte des Themenbereichs dargestellt.<br>Geräte mit aktiviertem *SecureCert-Feature* werden mit einem Schloss-Symbol gekennzeichnet. |
| **Schnellzugriffe ⑤** | **Sprachauswahl:** Die Sprachkennung (beispielsweise **DE** für *Deutsch*) zeigt die derzeit aktive Sprache in der Webapplikation an.<br>Zur Umschaltung der Sprache klicken Sie auf die Sprachkennung. Daraufhin öffnet sich ein Untermenü, das die unterstützten Sprachen und die zugehörigen Kennungen anzeigt.<br>Schalten Sie mit einem Klick auf die gewünschte Sprache die Sprache um.<br>**Benutzer:** Nach einem Klick auf das Benutzersymbol öffnet sich ein Untermenü:<br>▪ Im Untermenü wird der Name des aktiven Benutzers angezeigt.<br>▪ Mit einem Klick auf *Benutzer* gelangen Sie zu den Benutzereinstellungen des aktiven Benutzers.<br>▪ Klicken Sie auf *Abmelden*, um die aktive Sitzung zu beenden.<br>**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).<br>Das Icon *Monitoring-Status* nimmt jeweils die Farbe des *schlechtesten* Monitoring-Wertes an.<br>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:

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

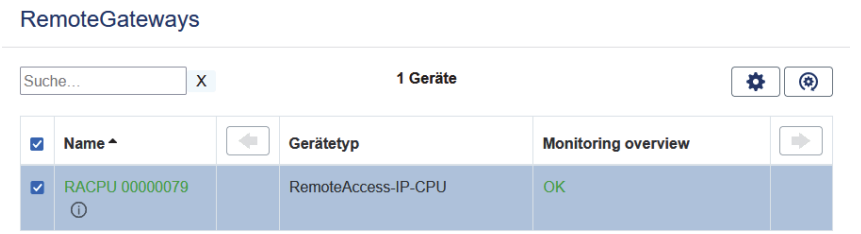



**Abbildung 2: Tabellenspalten (Auswahl) eines RemoteGateways**

**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 Schaltlfäche ( ) 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**.

## Automatisches Logout

Die Funktion *Automatisches Logout* dient dem automatischen Abmelden des Benutzers an der Webapplikation, wenn in einer gewissen Zeit keine Aktivität festzustellen ist.

Zudem kann ausgewählt werden, ob der Benutzer einen Timer (herunterzählende Zeit in Minuten:Sekunden bis zum automatischen Logout) angezeigt bekommt.

Den Zeitraum der Inaktivität können Sie im Bereich von **1** bis **60** Minuten festlegen.

> **HINWEIS:** Zum Deaktivieren der Funktion geben Sie die Ziffer **0** (*Standard*) ein.

**So aktivieren oder deaktivieren Sie die automatische Logout-Funktion:**

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Automatisches Logout**.
3. Geben Sie im Feld **Automatisches Logout des Config Panel (0-60 Minuten)** die Zeit der Inaktivität bis zum automatischen Logout im Bereich von **1** bis **60** Minuten ein.

   > **HINWEIS:** Wird eine Aktivität des Benutzers festgestellt, wird der Timer zurückgesetzt.
   >
   > Mit dem Start eines Updatevorgangs über die Webapplikation wird der Timer ebenfalls zurückgesetzt und läuft erst wieder nach Abschluss des Updatevorgangs.

4. Wählen Sie im Feld **Timer anzeigen** zwischen folgenden Optionen:

| | |
|---|---|
| **An:** | Der Benutzer bekommt den Timer rechts oben in der Webapplikation angezeigt, wenn die Eingabe im Feld **Automatisches Logout des Config Panel (0-60 Minuten)** nicht **0** ist (*Standard*). |
| **Aus:** | Der Benutzer bekommt keinen Timer angezeigt. |

5. Klicken Sie auf **Speichern**.

## Anzeigen von Nutzungsbedingungen

Wenn die Nutzungsbedingungen angezeigt werden, müssen sie vor jedem (erneuten) Gerätezugriff akzeptiert werden.

**So konfigurieren Sie die Anzeige von Nutzungsbedingungen:**

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Nutzungsbedingungen**.
3. Wählen Sie im Feld **Nutzungsbedingungen anzeigen** zwischen folgenden Optionen:

| | |
|---|---|
| **Aus:** | Bei einer Anmeldung werden *keine* Nutzungsbedinungen angezeigt (*Standard*). |
| **Benutzer-definiert:** | Bei einer Anmeldung werden *individuelle* Nutzungsbedingungen angezeigt. |
| **DoD Notice and Consent Banner:** | Bei einer Anmeldung werden die Nutzungsbedingungen des *US Department of Defense* verwendet (nur auswählbar bei aktiviertem optionalem *SecureCert-Feature*). |

4. Falls Sie im vorherigen Schritt *Benutzerdefiniert* ausgewählt haben, erfassen Sie im Feld **Kurztext** nun den Text, den ein Benutzer vor dem Akzeptieren der Nutzungsbedingungen angezeigt bekommt (**Beispiel**: *Ich habe die Nutzungsbedingungen gelesen und bin hiermit einverstanden*). Dieses Textfeld ist auf 70 Zeichen begrenzt.
5. Im Feld **Langtext** erfassen Sie nun die gewünschten Nutzungsbedingungen. Dieses Textfeld ist auf 1.500 Zeichen begrenzt.
6. Klicken Sie auf **Speichern**.

## Passwort-Komplexität

Zur Einhaltung Ihrer individuellen Passwort-Richtlinien und zur Verbesserung der Sicherheit können Sie die Passwort-Komplexität konfigurieren.

**WICHTIG:** Änderungen im Bereich der Passwort-Komplexität haben **keinen** Einfluss auf bereits bestehende Passwörter, sondern werden nur bei einer Passwort-Änderung (siehe *Änderung des Passworts eines Benutzerkontos* ab Seite 59) und Anlage eines neuen Benutzerkontos (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 54) berücksichtigt. Daher sollten Sie, falls gewünscht, die Passwort-Komplexität möglichst frühzeitig konfigurieren.

**WICHTIG:** Änderungen im Bereich der Passwort-Komplexität haben **keinen** Einfluss auf die Benutzerauthentifizierung mit externen Verzeichnisdiensten. In den Verzeichnisdiensten existieren eigene Konfigurationsoptionen.

**So konfigurieren Sie die Passwort-Komplexität:**

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Passwort-Komplexität**.
3. Geben Sie im Feld **Minimale Passwortlänge** die gewünschte minimale Passwortlänge ein (*Standard*: 3 bzw. 15 bei aktiviertem *SecureCert-Feature*)
4. Geben Sie im Feld **Mindestanzahl Großbuchstaben (z.B. ABCDEF)** die gewünschte Mindestanzahl an Großbuchstaben innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
5. Geben Sie im Feld **Mindestanzahl Kleinbuchstaben (z.B. abcdef)** die gewünschte Mindestanzahl an Kleinbuchstaben innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
6. Geben Sie im Feld **Mindestanzahl Ziffern (z.B. 012345)** die gewünschte Mindestanzahl an Ziffern innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
7. Geben Sie im Feld **Mindestanzahl Sonderzeichen (z.B. !#%&?@)** die gewünschte Mindestanzahl an Sonderzeichen innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
8. Geben Sie im Feld **Mindestanzahl der zu verändernden Zeichen des vorherigen Passworts** die gewünschte Mindestanzahl an unterschiedlichen Zeichen für eine Passwortänderung im Vergleich zum vorherigen Passworts ein (*Standard*: 0 bzw. 8 bei aktiviertem *SecureCert-Feature*)

   **HINWEIS:** Die Mindestanzahl an zu verändernden Zeichen darf nicht größer sein als die minimale Passwortlänge.

9. Klicken Sie auf **Speichern**.

## Anmeldeoptionen

Zur Verbesserung der Sicherheit stehen Ihnen im Bereich der Anmeldeoptionen weitere Konfigurationsmöglichkeiten zur Verfügung.

Sie können festlegen, wie viele Fehlversuche bei der Passworteingabe akzeptiert werden und wie lange ein Benutzer nach dem Überschreiten der Anzahl maximaler Fehlversuche gesperrt wird.

Zudem können Sie in diesem Bereich festlegen, wie viele gleichzeitige Superuser-Sitzungen erlaubt sind.

**So konfigurieren Sie die Anmeldeoptionen:**

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **Anmeldeoptionen**.
3. Geben Sie im Feld **Anzahl der aufeinanderfolgenden ungültigen Anmeldeversuche bis zum Sperrzeitpunkt (0=aus)** die gewünschte Anzahl an maximalen Fehlversuchen bei der Passworteingabe ein
   (*Standard*: 0 = aus/unbegrenzte Anzahl an Fehlversuchen bzw.
   3 bei aktiviertem *SecureCert-Feature*, max. 1.000)
4. Geben Sie im Feld **Sperrzeit (in Minuten)** die gewünschte Sperrzeit in Minuten an, für die ein Nutzer nach dem Überschreiten der Anzahl an maximalen Fehlversuchen bei der Passworteingabe gesperrt wird
   (*Standard*: 1 (wenn max. Fehlversuche > 0) bzw.
   15 bei aktiviertem *SecureCert-Feature*, max. 1.440 Minuten)
5. Geben Sie im Feld **Anzahl gleichzeitiger Sitzungen mit Superuser-Recht beschränken** die gewünschte Anzahl an maximalen Superuser-Sitzungen ein
   (*Standard*: 0 = aus/unbegrenzte Anzahl an Superuser-Sitzungen, max. 1.024)

   **HINWEIS:** Die maximale Anzahl gleichzeitiger Superuser-Sitzungen gilt je Schnittstelle (Gerät/OSD und ConfigPanel).
6. Klicken Sie auf **Speichern**.

## Versionsnummer der Webapplikation und allgemeine Informationen anzeigen

**So zeigen Sie die Versionsnummer der Webapplikation und allgemeine Informationen an:**

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

**TIPP:** Zusätzlich finden Sie hier eine Auflistung der IP-Adressen pro Schnittstelle.

## 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

Die Geräte der *RemoteAccess-IP-CPU*-Serie sind mit zwei Netzwerkschnittstellen ausgestattet:

- **Network/*Schnittstelle A*:** Diese Schnittstelle wird für die Kommunikation mit den virtuellen Computern verwendet.
- **Transmission:** Diese Schnittstelle wird für die Signalübertragung zwischen dem Targetmodul und dem IP-Matrixswitch verwendet.

**HINWEIS:** Die Nutzung der Webapplikation des Geräts und der erweiterten Netzwerkfunktionen (Netzfilter, Syslog, …) kann über beide Schnittstellen erfolgen.

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

## Konfiguration der Netzwerkschnittstellen

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 *Network*-Schnittstelle »*Schnittstelle A*«: **192.168.0.1**
- IP-Adresse der Schnittstelle »*Transmission* «:
  Bezug der Adresse via **DHCPv4** (Fallback: IP-Adresse **172.17.0.10**)
- globale Netzwerkeinstellungen: dynamischer Bezug der Einstellungen

**So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:**

**WICHTIG:** Der Betrieb beider Netzwerkschnittstellen innerhalb eines Subnetzes ist nicht zulässig!

**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!

**WICHTIG:** Die Konfiguration von **IPv6** sollte nur von **technisch erfahrenen Benutzern** vorgenommen werden. IPv6 bietet erweiterte Funktionen und einen größeren Adressraum, bringt jedoch auch **komplexere Anforderungen an Netzwerkstruktur, Sicherheit und Kompatibilität** mit sich. Fehlerhafte Einstellungen können zu **Verbindungsproblemen oder unerwartetem Verhalten im Netzwerkbetrieb** führen. Wenn Sie mit der für IPv6 spezifischen IP-Adressierung und Netzwerktopologie **nicht vertraut** sind, empfehlen wir, sich vor der Aktivierung von IPv6 **genau über die Auswirkungen zu informieren** oder Rücksprache mit Ihrer Netzwerkadministration zu halten.

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** oder **Transmission** folgende Daten:

> **HINWEIS:** Jede Netzwerkschnittstelle erhält neben ihrer Bezeichnung eine eindeutige **Zone-ID**, die ihre Schnittstellennummer angibt. Diese wird benötigt, um bei der Verwendung von *IPv6-Link-Local-Adressen* die jeweilige Schnittstelle eindeutig zu identifizieren.

| | |
|---|---|
| **Betriebsmodus:** | Wählen Sie den Betriebsmodus aus:<br>▪ **Aus:** Netzwerkschnittstelle ausschalten.<br>▪ **Statisch IPv4:** Es wird eine statische IPv4-Adresse zugeteilt.<br>▪ **DHCPv4:** Bezug der IPv4-Adresse von einem DHCP-Server. |
| **IPv4-Adresse:** | Geben Sie die IPv4-Adresse der Schnittstelle an (nur bei Auswahl des Betriebsmodus *Statisch IPv4).* |
| **Netzmaske:** | Geben Sie die Netzmaske des Netzwerkes an (nur bei Auswahl des Betriebsmodus *Statisch IPv4*). |
| **IPv6:** | Klicken Sie auf den Schieberegler, um IPv6 zu aktivieren (grün/rechts = aktiviert).<br>**HINWEIS:** Bei der Aktivierung von IPv6 wird gemäß RFC 4921 standardmäßig eine link-lokale IPv6-Adresse anhand der MAC-Adresse der Schnittstelle generiert. Diese link-lokale IPv6-Adresse ist vom Anwender nicht veränderbar.<br>Klicken Sie auf den Schieberegler, um IPv6 zu deaktivieren (grau/links = deaktiviert (*Standard*)). |
| **IPv6-Adresse:** | Geben Sie die statische IPv6-Adresse der Schnittstelle an. |
| **Subnetz-präfixlänge:** | Geben Sie die Präfixlänge (*Standard*: 64) gemäß den Notationsregeln nach RFC 5952 für die Schnittstelle 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 Einstellungen**.
5. Erfassen Sie folgende Daten und klicken Sie anschließend auf **Speichern**:

| | |
|---|---|
| **Betriebsmodus:** | Wählen Sie den gewünschten Betriebsmodus:<br>▪ **Statisch:** Verwendung von statischen Einstellungen.<br>▪ **Dynamisch:** Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6). |
| **Host-Name:** | Geben Sie den Host-Namen des Gerätes ein. |
| **Domäne:** | Geben Sie die Domäne an, welcher das Gerät angehören soll. |
| **Gateway IPv4:** | Geben Sie die IPv4-Adresse des Gateways an. |
| **Gateway IPv6:** | Geben Sie die IPv6-Adresse des Gateways an. |
| **DNS-Server 1:** | Geben Sie die IP-Adresse des DNS-Servers an..<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **DNS-Server 2:** | Geben Sie *optional* die IP-Adresse eines weiteren DNS-Servers an..<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **Priorisierung von IPv6:** | Klicken Sie auf den Schieberegler, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (grün/rechts = IPv6 wird bevorzugt.<br>Klicken Sie auf den Schieberegler, falls IPv6 nicht bevorzugt werden soll (grau/links = IPv6 wird nicht bevorzugt, *Standard*). |

| | |
|---|---|
| **Verwende IPv6 Stateless Address Auto-configuration (SLAAC):** | Klicken Sie auf den Schieberegler, falls SLAAC verwendet werden soll (grün/rechts = SLAAC wird verwendet, *Standard*, wenn *SecureCert-Feature* nicht aktiviert ist).<br>Klicken Sie auf den Schieberegler, falls SLAAC nicht verwendet werden soll (grau/links = SLAAC wird nicht verwendet, *Standard* bei aktiviertem *SecureCert-Feature*). |
| **ICMP Echo-Reply auf Echo-Request einer Multicast-/ Anycast-Adresse senden (IPv6):** | Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests beantwortet werden sollen (grün/rechts = Echo-Requests werden beantwortet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests nicht beantwortet werden sollen (grau/links = Echo-Requests werden nicht beantwortet). |
| **ICMP-Destination-Unreachable-Nachrichten senden (IPv6):** | Klicken Sie auf den Schieberegler, falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann (grün/rechts = Fehlermeldung wird gesendet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls keine ICMPv6-Fehlermeldungen gesendet werden sollen (grau/links = Fehlermeldung wird nicht gesendet). |
| **Redirect-Meldungen verarbeiten (IPv6):** | Klicken Sie auf den Schieberegeler, falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen (grün/rechts = Redirect-Meldungen werden verarbeitet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls Redirect-Meldungen nicht verarbeitet werden sollen (grau/links = Redirect-Meldungen werden nicht verarbeitet). |
| **Duplicate Address Detection (IPv6):** | Klicken Sie auf den Schieberegler, falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird (grün/rechts = es wird auf doppelte Adressen geprüft, *Standard*).<br>Klicken Sie auf den Schieberegler, falls nicht auf doppelt IPv6-Adressen geprüft werden soll (grau/links = es wird nicht auf doppelte Adressen geprüft). |

## Status der Netzwerkschnittstellen auslesen

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

**So ermitteln Sie den Status der Netzwerkschnittstellen:**

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. In den Abschnitten **Schnittstelle A** und **Transmission** werden Ihnen folgende Daten angezeigt:

> **HINWEIS:** Die Netzwerkschnittstelle erhält neben ihrer Bezeichnung eine eindeutige **Zone-ID**, die ihre Schnittstellennummer angibt. Diese wird benötigt, um bei der Verwendung von *IPv6-Link-Local-Adressen* die jeweilige Schnittstelle eindeutig zu identifizieren.

| | |
|---|---|
| **Link detected:** | Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**). |
| **Auto-negotiation:** | Die Übertragungsgeschwindigkeit und das Duplex-Verfahren wurden automatisch (**ja**) oder manuell vom Administrator konfiguriert (**nein**). |
| **Speed:** | Übertragungsgeschwindigkeit |
| **Duplex:** | Duplexverfahren (**full** bzw. **half**) |

6. Klicken Sie auf **Schließen**.

# 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.

**HINWEIS:** Sobald eine Netzfilterregel verwendet wird, greift die *Default-DROP-Poliy*.

Falls *bestimmte* IP-Adressen akzeptiert werden sollen, reicht es aus, ihnen die Filterregel *Accept* zuzuordnen. Datenpakete über *alle* anderen IP-Adressen werden aufgrund der *Default-DROP-Policy* nicht verarbeitet (*„gedroppt“*).

**WICHTIG:** Falls Datenpakete nur über *bestimmte* IP-Adressen *nicht* verarbeitet (*„gedroppt“*) werden sollen, ist diesen IP-Adressen die Filterregel *Drop* zuzuordnen. Anschließend muss den IP-Adressen, die akzeptiert werden sollen, die Filterregel *Accept* zugeordnet werden, da weitere Datenpakete über weitere IP-Adressen aufgrund der *Default-DROP-Policy* ansonsten ebenfalls nicht verarbeitet (*„gedroppt“*) werden. Falls *alle* anderen IP-Adressen akzeptiert werden sollen, kann die *Accept*-Regel auf *alle* IP-Adressen (**0.0.0.0/0**) angewendet werden.

## 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:

| | |
|---|---|
| **Schnittstelle:** | Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen:<br>▪ **Alle**<br>▪ **Schnittstelle A**<br>▪ **Transmission** |
| **Option:** | Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist:<br>▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.<br>▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. |
| **IP-Adresse/ Präfixlänge:** | Geben Sie die IP-Adresse des Hosts oder durch Verwendung des Feldes **Präfixlänge** das Netzsegment an.<br>**Beispiele IPv4:**<br>▪ **192.168.150.187/32:** nur die IP-Adresse 192.168.150.187 Wird nur eine IP-Adresse ohne Angabe einer Präfixlänge eingetragen, setzt das System im Hintergrund automatisch **/32** als Präfix.<br>▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x<br>▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x<br>▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x<br>▪ **0.0.0.0/0:** alle IPv4-Adressen<br>**Beispiele IPv6:**<br>▪ **2001:db8::222:4dff:fe84:3cb6/128:** nur diese IP-Adresse Wird nur eine IP-Adresse ohne Angabe einer Präfixlänge eingetragen, setzt das System im Hintergrund automatisch **/128** als Präfix.<br>▪ **fe80::/64:** alle link-lokalen IP-Adressen<br>▪ **2001:db8::/64:** IP-Adressen des Raums 2001:db8::/64<br>▪ **::/0:** alle IPv6-Adressen |

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

**HINWEIS:** Geben Sie link-lokale IPv6-Adressen hier gegebenenfalls ohne Zone-ID ein.

| | |
|---|---|
| **MAC-Adresse:** | Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.<br>**HINWEIS:** Innerhalb einer Regel können wahlweise die *IP-Adresse* und/ oder eine *MAC-Adresse* angegeben werden. |
| **Filterregel:** | ▪ **Drop:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden *nicht* verarbeitet.<br>▪ **Accept:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet. |
| **Service:** | Wählen Sie einen bestimmten Service, für den diese Regel exklusiv angewendet wird oder wählen Sie (**Alle**). |

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.

| | |
|---|---|
| **Schnittstelle:** | Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen:<br>▪ **Alle**<br>▪ **Schnittstelle A**<br>▪ **Transmission** |
| **Option:** | Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist:<br>▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.<br>▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. |
| **IP-Adresse/ Präfixlänge:** | Geben Sie die IP-Adresse des Hosts oder durch Verwendung des Feldes **Präfixlänge** das Netzsegment an.<br>**Beispiele IPv4:**<br>▪ **192.168.150.187/32:** nur die IP-Adresse 192.168.150.187 Wird nur eine IP-Adresse ohne Angabe einer Präfixlänge eingetragen, setzt das System im Hintergrund automatisch **/32** als Präfix.<br>▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x<br>▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x<br>▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x<br>▪ **0.0.0.0/0:** alle IPv4-Adressen<br>**Beispiele IPv6:**<br>▪ **2001:db8::222:4dff:fe84:3cb6/128:** nur diese IP-Adresse Wird nur eine IP-Adresse ohne Angabe einer Präfixlänge eingetragen, setzt das System im Hintergrund automatisch **/128** als Präfix.<br>▪ **fe80::/64:** alle link-lokalen IP-Adressen<br>▪ **2001:db8::/64:** IP-Adressen des Raums 2001:db8::/64<br>▪ **::/0:** alle IPv6-Adressen |

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

**HINWEIS:** Geben Sie link-lokale IPv6-Adressen hier gegebenenfalls ohne Zone-ID ein.

| | |
|---|---|
| **MAC-Adresse:** | Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist.<br>**HINWEIS:** Innerhalb einer Regel können wahlweise die *IP-Adresse* und/ oder eine *MAC-Adresse* angegeben werden. |
| **Filterregel:** | ▪ **Drop:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden *nicht* verarbeitet.<br>▪ **Accept:** Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet. |
| **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/Prorität 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 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.

**Ein Zertifikat wird grundsätzlich in 5 Schritten erstellt:**

1. Erzeugen eines privaten Schlüssels
2. Erstellen einer Certificate Signing Request (CSR)
3. Übermitteln der CSR an die Zertifizierungsstelle (CA)
4. Erhalt des signierten Zertifikats von der CA
5. Erstellen der PEM-Datei

## 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 28) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 32) 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 (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 Zertifkat 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 Zertifkats 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 (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 Zertifikatwiderruf 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 req -x509 -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.

**WICHTIG:** Falls Sie die Zertifikate nicht, wie in den vorherigen Abschnitten erläutert, erstellen, sondern eigene Zertifikate mit Zertifikatserweiterungen verwenden, ist der einzugebene Befehl entsprechend anzupassen bzw. zu erweitern.

**BEISPIEL:** Nutzen Sie beispielsweise die *Extended Key Usage*, um die erlaubte Verwendung des Schlüssels einzuschränken, so muss mindestens die Extension *serverAuth* und *clientAuth* aktiviert bzw. berücksichtigt werden:

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

**TIPP:** Um zu prüfen, welche Zertifikatserweiterungen verwendet werden, verwenden Sie:

```
openssl x509 -text -in ca.crt
```

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

   b. Windows

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

2. Durch die Kopieroperation(en) wird die Datei *gdcd.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 28) verwenden, können die Geräte miteinander kommunizieren.

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

**HINWEIS:** Durch die Auswahl und Aktivierung eines *anderen* Zertifikates werden alle aktiven Sitzungen der Webapplikation beendet!

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.<br>**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.<br>Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat:<br>1. Klicken Sie auf **Zertifikat aus Datei importieren** und wählen Sie die zu importierende .pem-Datei im Datei-Dialog aus.<br>Alternativ kopieren Sie den Klartext des Zertifikats des Servers, den privaten Schlüssel des Servers sowie das Zertifikat der Zertifizierungsstelle in das Textfeld.<br>2. Klicken Sie auf **Upload und aktivieren**, um das importierte Zertifikat im Gerät zu speichern und zu aktivieren. |

3. Klicken Sie auf **Speichern**.

**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.

# Durchführung von Firmware-Updates

Die Firmware des Gerätes kann über die Webapplikation aktualisiert werden.

## Firmware-Update des Gerätes

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

**So aktualisieren Sie die Firmware des Gerätes:**

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 **Zielversion** 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 Gerät während des Updates **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:

| | |
|---|---|
| **Alle Einstellungen zurücksetzen:** | Alle Einstellungen des Gerätes zurücksetzen. |
| **Nur Einstellungen des lokalen Netzwerkes zurücksetzen:** | Ausschließlich die lokalen Netzwerk-einstellungen zurücksetzen. |
| **Nur Einstellungen der KVM-Anwendungen zurücksetzen:** | 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 **Ja**.

# Netzwerkfunktionen der Geräte

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

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

- Authentifizierung gegenüber Verzeichnisdiensten (LDAP, Active Directory, RADIUS)
- 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:

| | |
|---|---|
| **Allgemein** | |
| **NTP-Zeitsynchronisation:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Zeitsynchronisation aus- und einschalten:<br>▪ **Deaktiviert** (*Standard*)<br>▪ **Aktiviert** |
| **Zeitzone:** | Wählen Sie aus dem Pull-Down-Menü die Zeitzone Ihres Standorts aus. |
| **NTP-Server 1** | |
| **Adresse:** | Geben Sie die Adresse eines Zeitservers ein. |
| **Authentifizierung:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Authentifizierung aus- und einschalten:<br>▪ **Deaktiviert** (*Standard*)<br>▪ **SHA1** |
| **Schlüssel-ID:** | Geben Sie nach Aktivierung der Authentifizierung die Schlüssel-ID ein, die für die Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. |
| **Schlüssel** | Geben Sie den Schlüssel in Form von bis zu 40 Hexadezimalstellen ein. |
| **NTP-Server 2** | |
| **Adresse:** | Geben Sie *optional* die Adresse eines zweiten Zeitservers ein. |
| **Authentifizierung:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Authentifizierung aus- und einschalten:<br>▪ **Deaktiviert** (*Standard*)<br>▪ **SHA1** |
| **Schlüssel-ID:** | Geben Sie nach Aktivierung der Authentifizierung die Schlüssel-ID ein, die für die Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann. |
| **Schlüssel** | Geben Sie den Schlüssel in Form von bis zu 40 Hexadezimalstellen ein. |

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-Zeitsynchronisation**, 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:

- **0:** Notfall
- **1:** Alarm
- **2:** Kritisch
- **3:** Fehler
- **4:** Warnung
- **5:** Notiz
- **6:** Info
- **7:** Debug

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

**BEISPIEL:** Bei Verwendung des Schweregrads 6 (*Standard*) werden beispielsweise folgende Ereignisse mit Zeitstempel nach ISO8601 und weitere Informationen protokolliert:

- Benutzeranmeldung: Welcher Benutzer hat sich an welchem Gerät angemeldet und ist der Benutzer bereits an einem anderen Gerät angemeldet (usercount N)
- Anmelde-Fehlversuch: An welchem Gerät hat ein fehlerhafter Loginversuch stattgefunden (bereits bei Verwendung des Schweregrads 5)
- Benutzerrechte-Änderung: Welcher Benutzer hat über welches Gerät eine Veränderung von Rechten vorgenommen
- Fehlgeschlagenes (Auto-)Backup: Für welches Gerät ist ein (Auto-)Backup fehlgeschlagen (bereits bei Verwendung des Schweregrads 3)

**HINWEIS:** Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.

## 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:

| | |
|---|---|
| **Syslog lokal:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie die lokale Protokollierung von Syslog-Meldungen aus oder ein:<br>▪ **Deaktiviert**<br>▪ **Aktiviert** (*Standard*) |
| **Log-Level:** | Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist (*Standard*: 6 - Info).<br>Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert. |

Wählen Sie den Schweregrad *2 - Kritisch*, so werden für diesen, wie auch für die Schweregrade *1 - Alarm* und *0 - Notfall*, 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**:

| | |
|---|---|
| **Syslog-Server:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie den Versand von Syslog-Meldungen an einen Server aus oder ein:<br>▪ **Deaktiviert** (*Standard*)<br>▪ **Aktiviert** |
| **Log-Level:** | 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.<br>Wählen Sie den Schweregrad *2 - Kritisch*, so werden für diesen, wie auch für die Schweregrade *1 - Alarm* und *0 - Notfall*, Meldungen protokolliert. |
| **IP-Adresse/ DNS-Name:** | Geben Sie die IP-Adresse oder den FQDN des Zielservers für die Syslog-Meldungen an. |
| **Port:** | Geben Sie den Port – üblicherweise 514 – an, auf dem der Syslog-Server eingehende Meldungen annimmt. |
| **Protokoll:** | Wählen Sie das Protokoll – üblicherweise UDP – aus, auf dem der Syslog-Server eingehende Meldungen annimmt:<br>▪ **TCP**<br>▪ **UDP** |

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 (Option)* ab Seite 46) 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:

**Authentifizierungsserver:** 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**

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 54).

**TIPP:** Erfassen Sie bei Verwendung von *LDAP* oder *Active Directory* im Feld **Base DN/SearchScope** den Pfad, ab dem die jeweilige Suche gestartet werden soll. Dies spart Zeit und verhindert eine unnötig lange Suche.

**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 (Option)* auf Seite 46) kann der Fallback-Mechanismus **nicht** genutzt werden.

6. Klicken Sie auf **Speichern**.

## Einrichtung der Zwei-Faktor-Authentifizierung am Gerät (Option)

Die standardmäßige Benutzer-Authentifizierung erfolgt über eine Passwort-Abfrage. Um die Sicherheit zu erhöhen, kann durch die kostenpflichtige 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 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 55).

**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:

| | |
|---|---|
| **2FA-Unterstützung:** | ▪ **Deaktiviert** (*Standard*)<br>▪ **Aktiviert** |
| **OTP-Server:** | Wählen Sie die Option **Intern** (*Standard*), wenn ein interner, im Gerät bereitgestellter Authentifizierungsserver zum Einsatz kommen soll.<br>Möchten Sie einen bestimmten externen Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus:<br>▪ **LDAP**<br>▪ **Active Directory**<br>▪ **Radius**<br>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* ab Seite 54).

| | |
|---|---|
| **Login nur für Benutzer mit konfigurierter 2FA:** | Kommt der interne OTP-Server zum Einsatz, kann festgelegt werden, ob ein Login von Benutzern ohne eine aktivierte 2FA zulässig ist (*Standard*) oder verhindert werden soll. Mit dieser Option kann z. B. eine Übergangszeit zur Einrichtung der OTPs ermöglicht werden.<br>▪ **Nein** (*Standard*)<br>▪ **Ja** |

**WICHTIG:** Kommt ein externer Verzeichnisdienst zum Einsatz wird für **jedes** Benutzerprofil der zweite Faktor beim Login verlangt.

6. Klicken Sie auf **Speichern**.

**WICHTIG:** Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 37). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 39).

Informationen zur Aktivierung der Zwei-Faktor-Authentifizierung finden Sie auf Seite 55 ff.

# Monitoring-Funktionen

In den Themenbereichen **RemoteGateways** und **Systemüberwachung** können Sie die aktuellen Monitoring-Werte der Geräte des KVM-Systems einsehen.

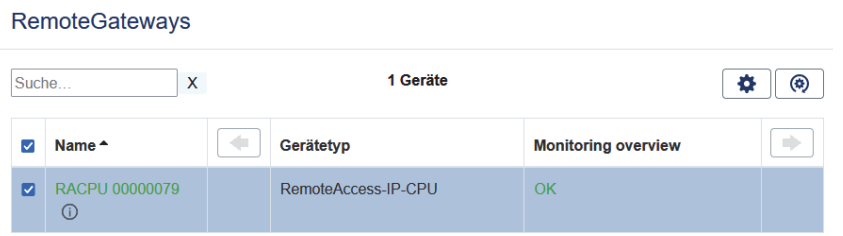



**Abbildung 4: Detailansicht einer exemplarischen Monitoring-Tabelle**

Die, für die Tabellenansicht (siehe *Tabellenspalten konfigurieren* auf Seite 7) konfigurierten Werte, werden in der Tabelle aufgelistet.

Anhand der Farbe können Sie sofort erkennen, ob der Status einwandfrei (grüne Darstellung) oder auffällig (rote Darstellung) ist. Der ausgegebene Text in der Spalte gibt zusätzlich Auskunft über den aktuellen Zustand.

## 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-Werten 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 1.024 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 *RechnermodulConfig*.

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

| Recht | Benutzer *Muster* | Gruppe *Office* | Gruppe *Rechnermodul-Config* | Effektivrecht |
|---|---|---|---|---|
| **Config Panel Login** | Nein | Ja | **Ja** | **Ja** |
| **Eigenes Passwort ändern** | Nein | **Ja** | Nein | **Ja** |

Das Effektivrecht der Rechte *Config Panel Login* und *Eigenes Passwort ändern* 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 1.024 Benutzerkonten. Jedes Benutzerkonto verfügt über individuelle Login-Daten, Rechte und benutzerbezogene Einstellungen für das KVM-System.

**WICHTIG:** Falls individuelle Passwort-Richtlinien berücksichtigt werden sollen, müssen Sie die Konfiguration der Passwort-Komplexität vor der Anlage eines neuen Benutzerkontos vornehmen (siehe *Passwort-Komplexität* auf Seite 12).

**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:

| | |
|---|---|
| **Name:** | Geben Sie den gewünschten Benutzernamen ein.<br>**HINWEIS:** Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Benutzerauthentifizierung mit Verzeichnisdiensten* ab Seite 43). |
| **Passwort:** | Geben Sie das Passwort des Benutzerkontos ein. |
| **Passwort bestätigen:** | Wiederholen Sie das oben eingegebene Passwort. |
| **Klartext:** | Aktivieren Sie ggf. dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können. |
| **Vollständiger Name:** | Geben Sie hier – falls gewünscht – den vollständigen Namen des Benutzers ein. |
| **Kommentar:** | Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto. |
| **Aktiviert:** | Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.<br>**HINWEIS:** 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 46), sind im Folgenden die Einstellungen für das Benutzerkonto vorzunehmen (s. Seite 55).

## Aktivierung der Zwei-Faktor-Authentifizierung

**HINWEIS:** Für die Verwendung der Zwei-Faktor-Authentifizierung (2FA) muss zunächst die Einrichtung am Gerät erfolgen (s. Seite 46).

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 (Option)* ab Seite 46), 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 67), oder der Anwender muss mit dem entsprechenden Benutzerprofil angemeldet sein (s. Seite 67) und über das Recht *Eigenes Passwort ändern* (s. Seite 68) verfügen.

**WICHTIG:** Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 37). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 39).

**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:

| | |
|---|---|
| **Schlüssel:** | Beim Wechsel des Parameters **2FA für diesen Benutzer** von **Deaktiviert** auf **Aktiviert**, wird automatisch ein Schlüssel generiert und angezeigt.<br>**WICHTIG:** Eine Eingabe muss im **Base32-Format** erfolgen.<br>Klicken Sie auf **Generieren**, um einen neuen Schlüssel zu erhalten. |
| **Hash-Algorithmus:** | ▪ **SHA1**<br>▪ **SHA256** (*Standard*)<br>▪ **SHA512** |
| **Gültigkeitsdauer (Sek.):** | Erfassen Sie hier, wie lange der 2-Faktor-Authentifizierungscode (TOTP) gültig sein soll. Der eingegebene Wert muss zwischen **10** und **200** Sekunden liegen (*Standard*: 30 Sekunden).<br>**TIPP:** Es ist sinnvoll, die Gültigkeitsdauer nicht zu klein zu wählen, da es durch evtl. nicht synchronisierte Zeit ansonsten zu Zugriffsproblemen kommen könnte. |
| **Länge des 2-Factor Auth Code (TOTP):** | ▪ **6 Stellen** (*Standard*)<br>▪ **8 Stellen** |
| **Fensterbreite des 2-Factor Auth Code (TOTP):** | Mit der Fensterbreite legen Sie fest, wie viele vorherige 2-Faktor-Authentifizierungscodes (TOTP) neben dem aktuellen gültig sind. Es ist hierbei nicht möglich zukünftige 2-Faktor-Authentifizierungscodes (TOTP) zu erlauben. Der eingegebene Wert muss zwischen 1 und 20 liegen (*Standard*: 1).<br>**TIPP:** Um durch evtl. nicht synchronisierte Zeit auftretende Zugriffsprobleme zu vermeiden, kann es sinnvoll sein, mehrere vorherige 2-Faktor-Authentifizierungscodes (TOTP) zuzulassen. |
| **QR-Code zeigen & Sicherheits-schlüssel kopieren:** | 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. |
| **Verifikations-code:** | 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.

Der 2-Faktor-Authentifizierungscode (TOTP) 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 60).

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 62).

Nachdem die 2FA im Benutzerkonto erfolgreich aktiviert wurde, wird beim Login (siehe *Start der Webapplikation* auf Seite 4) zusätzlich zur Eingabe des Benutzernamens und des Passwortes der 2-Faktor-Authentifizierungscode (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 43).

## 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 67)
oder das Recht *Eigenes Passwort ändern*
(siehe *Berechtigung zur Änderung des eigenen Passworts* ab Seite 68).

**HINWEIS:** Bei der Änderung des Passworts werden ggf. die festgelegten Passwort-Richtlinien (siehe *Passwort-Komplexität* auf Seite 12) berücksichtigt.

**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:

| | |
|---|---|
| **Aktuelles Passwort:** | Geben Sie das bisherige Passwort ein.<br>**HINWEIS:** Bei Benutzern mit aktiviertem Superuser-Recht (s. Seite 67 ff.) ist in diesem Feld keine Eingabe notwendig. |
| **Passwort:** | Geben Sie das neue Passwort ein. |
| **Passwort bestätigen:** | Wiederholen Sie das neue Passwort. |
| **Klartext:** | Aktivieren Sie dieses Kontrollkästchen, um die eingegebenen Passwörter im Klartext sehen und prüfen zu können. |
| **Verifikationscode:** | Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.<br>**HINWEIS:** Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 46 ff.) und aktiviert wurde (s. Seite 55 ff.). |

4. Klicken Sie auf **Speichern**.

## Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

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

**System-Rechte**

| Bezeichnung | Berechtigung | Seite |
|---|---|---|
| **Superuser-Recht** | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 67 |
| **Config Panel Login** | Login mit der Webapplikation *ConfigPanel* | Seite 67 |
| **Eigenes Passwort ändern** | Änderung des eigenen Passworts | Seite 68 |
| **Monitoring-Alarm bestätigen** | Bestätigung eines Monitoring-Alarms | Seite 68 |

## 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 1.024 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:

| | |
|---|---|
| **Name:** | Geben Sie den gewünschten Benutzernamen ein. |
| **Kommentar:** | Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto. |
| **Aktiviert:** | 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 liste die verschiedenen Berechtigungen auf. Weiterführende Hinweise zu den Rechten finden Sie auf den angegebenen Seiten.

**System-Rechte**

| Bezeichnung | Berechtigung | Seite |
|---|---|---|
| **Superuser-Recht** | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 67 |
| **Config Panel Login** | Login mit der Webapplikation *ConfigPanel* | Seite 67 |
| **Eigenes Passwort ändern** | Änderung des eigenen Passworts | Seite 68 |
| **Monitoring-Alarm bestätigen** | Bestätigung eines Monitoring-Alarms | Seite 68 |

## 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:

| | |
|---|---|
| **Aktiviert:** | Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte erlaubt |
| **Deaktiviert:** | 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:

| | |
|---|---|
| **Aktiviert:** | Zugriff auf die Webapplikation erlaubt |
| **Deaktiviert:** | 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:

| | |
|---|---|
| **Aktiviert:** | Passwortänderung des eigenen Benutzerkontos erlaubt |
| **Deaktiviert:** | 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:

| | |
|---|---|
| **Aktiviert:** | Bestätigung von Monitoring-Alarmen erlaubt |
| **Deaktiviert:** | 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 Gerätes:**

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:

| | |
|---|---|
| **Auto-Backup:** | Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Auto-Backup-Funktion aus- und einschalten:<br>▪ **Deaktiviert** (*Standard*)<br>▪ **Aktiviert** |
| **Dateiname-Präfix:** | Geben Sie das Dateiname-Präfix ein.<br>**HINWEIS:** Bei Aktivierung der Auto-Backup-Funktion wird das Feld Dateiname-Präfix automatisch mit der **UID** des Geräts gefüllt. Diesen Eintrag können Sie überschreiben.<br>**WICHTIG:** Es sind ausschließlich Buchstaben (groß- und kleingeschrieben), Ziffern (0 bis 9) und die Zeichen - und _ zugelassen. Das Präfix darf maximal 25 Zeichen enthalten. |
| **Backup-Passwort:** | *Optional:* Erfassen Sie ein Passwort zur Sicherung der Backup-Dateien.<br>**WICHTIG:** Doppelte Anführungszeichen („ und “) sind hier **nicht** zugelassen. |
| **Backup-Umfang:** | Wählen Sie den Umfang der zu speichernden Daten: Sie können wahlweise die **Netzwerkeinstellungen** und/oder die **Anwendungseinstellungen** sichern. |

| | |
|---|---|
| **Pfad:** | Erfassen Sie den Pfad für die Speicherung der Backup-Dateien.<br>**WICHTIG:** Die Syntax der Pfadangabe unterscheidet sich je nach gewähltem Protokoll.<br>Bei Verwendung des Protokolls **NFS** ist die URL-Schreibweise für NFS gemäß RFC 2224 anzuwenden - unter Berücksichtigung der allgemeinen URL-Notation aus RFC 3986.<br>Bei Verwendung des Protokolls **CIFS** muss die URL-Schreibweise gemäß RFC 3986 verwendet werden.<br>**WICHTIG:** Abweichend von den Vorgaben in RFC 2224 und RFC 3986 dürfen Protokoll, Port, Benutzername und Passwort **nicht** im Parameter Pfad angegeben werden. Diese Informationen werden ausschließlich aus den separaten Parametern **Protokoll**, **Port**, **Benutzer** und **Passwort** übernommen.<br>**Beispiele:**<br>▪ **NFS:** *name:/verzeichnis1/verzeichnis2*<br>▪ **CIFS:** *//name/verzeichnis1/verzeichnis2* |
| **Protokoll:** | Wählen Sie zwischen den folgenden Protokollen:<br>▪ **NFS** (*Standard*)<br>▪ **CIFS** |
| **Port:** | Geben Sie den Port ein. Dieses Feld wird je nach Auswahl im Feld *Protokoll* automatisch gefüllt:<br>▪ **2049** (bei Auswahl *NFS*)<br>▪ **445** (bei Auswahl *CIFS*) |
| **Benutzer:** | *Optional:* Erfassen Sie den Namen des Benutzers. |
| **Passwort:** | *Optional:* Erfassen Sie ein Passwort zur Sicherung der Freigabe. |
| **Uhrzeit:** | Erfassen Sie folgende Daten:<br>▪ **Stunde** (Zahlen *0* bis *23*)<br>▪ **Minute** (Zahlen *0* bis *59*) |
| **Auswahl des Tages:** | Es stehen Ihnen die folgenden Auswahlmöglichkeiten zur Verfügung:<br>▪ **1.** bis **31. Tag des Monats**<br>▪ **Alle auswählen** (jeder Tag des Monats) |

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:** Ob der Test erfolgreich war, sehen Sie in den Syslog-Meldungen (siehe *Protokollierung von Syslog-Meldungen* ab Seite 40).

**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 Gerätes 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.

> **WICHTIG:** Das *SecureCert-Feature* kann nur zusammen mit einem Neugerät beauftragt werden und ist **nicht** nachträglich aktivierbar!

**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.

   > **HINWEIS:** 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**.

# Einrichtung der KVM-over-IP™-Verbindung

Die Signalübertragung zwischen dem Rechnermodul und dem IP-Matrixswitch erfolgt mittels G&Ds **KVM-over-IP™**-Technologie über ein Gigabit-Ethernet (Layer 3).

**HINWEIS:** Die **Transmission**-Schnittstelle des Rechnermoduls wird für die Signalübertragung zwischen dem Rechnermodul und dem IP-Matrixswitch verwendet.

Die **Network**-Schnittstelle *Schnittstelle A* wird für die Kommunikation mit den virtuellen Computern verwendet.

Der Zugriff auf die Webapplikation des Rechnermoduls ist über beide Schnittstellen möglich.

Erst nach der Ersteinrichtung der KVM-over-IP™-Verbindung zwischen dem Rechnermodul und dem IP-Matrixswitch kann das Rechnermodul mit dem IP-Matrixswitch verwendet werden.

Im Auslieferungszustand ist folgende Einstellung der *Transmission*-Schnittstelle voreingestellt:

- IP-Adresse der *Transmission*-Schnittstelle:
  Bezug der Adresse via **DHCPv4** (Fallback: IP-Adresse 172.17.0.10)

Im Auslieferungszustand ist folgende Einstellung der *Network*-Schnittstelle voreingestellt:

- IP-Adresse der *Network*-Schnittstelle *Schnittstelle A*: 192.168.0.1

# KVM-over-IP-Verbindung konfigurieren

## Konfiguration der Netzwerkschnittstelle

**So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:**

**WICHTIG:** Der Betrieb beider Netzwerkschnittstellen innerhalb eines Subnetzes ist nicht zulässig!

**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. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **Netzwerk**.
5. Wählen Sie den Bereich **Schnittstellen**.

6. Erfassen Sie im **Schnittstelle A** oder **Transmission** folgende Daten:

> **HINWEIS:** Jede Netzwerkschnittstelle erhält neben ihrer Bezeichnung eine eindeutige **Zone-ID**, die ihre Schnittstellennummer angibt. Diese wird benötigt, um bei der Verwendung von *IPv6-Link-Local-Adressen* die jeweilige Schnittstelle eindeutig zu identifizieren.

| | |
|---|---|
| **Betriebsmodus:** | Wählen Sie den Betriebsmodus aus:<br>▪ **Aus:** Netzwerkschnittstelle ausschalten.<br>▪ **Statisch IPv4:** Es wird eine statische IPv4-Adresse zugeteilt.<br>▪ **DHCPv4:** Bezug der IPv4-Adresse von einem DHCP-Server. |
| **IPv4-Adresse:** | Geben Sie die IPv4-Adresse der Schnittstelle an (nur bei Auswahl des Betriebsmodus *Statisch IPv4).* |
| **Netzmaske:** | Geben Sie die Netzmaske des Netzwerkes an (nur bei Auswahl des Betriebsmodus *Statisch IPv4*). |
| **IPv6:** | Klicken Sie auf den Schieberegler, um IPv6 zu aktivieren (grün/rechts = aktiviert).<br>**HINWEIS:** Bei der Aktivierung von IPv6 wird gemäß RFC 4921 standardmäßig eine link-lokale IPv6-Adresse anhand der MAC-Adresse der Schnittstelle generiert. Diese link-lokale IPv6-Adresse ist vom Anwender nicht veränderbar.<br>Klicken Sie auf den Schieberegler, um IPv6 zu deaktivieren (grau/links = deaktiviert (*Standard*)). |
| **IPv6-Adresse:** | Geben Sie die statische IPv6-Adresse der Schnittstelle an. |
| **Subnetz-präfixlänge:** | Geben Sie die Präfixlänge (*Standard*: 64) gemäß den Notationsregeln nach RFC 5952 für die Schnittstelle an. |

7. Klicken Sie auf **Speichern**.

## Konfiguration der globalen Netzwerkeinstellungen

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

**So konfigurieren Sie die globalen Netzwerkeinstellungen:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **Netzwerk**.
5. Wählen Sie den Bereich **Globale Einstellungen**.
6. Erfassen Sie folgende Daten:

| | |
|---|---|
| **Betriebsmodus:** | Wählen Sie den gewünschten Betriebsmodus:<br>▪ **Statisch:** Verwendung von statischen Einstellungen.<br>▪ **Dynamisch:** Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6). |
| **Host-Name:** | Geben Sie den Host-Namen des Gerätes ein. |
| **Domäne:** | Geben Sie die Domäne an, welcher das Gerät angehören soll. |
| **Gateway IPv4:** | Geben Sie die IPv4-Adresse des Gateways an. |
| **Gateway IPv6:** | Geben Sie die IPv6-Adresse des Gateways an. |
| **DNS-Server 1:** | Geben Sie die IP-Adresse des DNS-Servers an..<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **DNS-Server 2:** | Geben Sie *optional* die IP-Adresse eines weiteren DNS-Servers an..<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **Priorisierung von IPv6:** | Klicken Sie auf den Schieberegler, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (grün/rechts = IPv6 wird bevorzugt.<br>Klicken Sie auf den Schieberegler, falls IPv6 nicht bevorzugt werden soll (grau/links = IPv6 wird nicht bevorzugt, *Standard*). |

| | |
|---|---|
| **Verwende IPv6 Stateless Address Auto-configuration (SLAAC):** | Klicken Sie auf den Schieberegler, falls SLAAC verwendet werden soll (grün/rechts = SLAAC wird verwendet, *Standard*, wenn *SecureCert-Feature* nicht aktiviert ist).<br>Klicken Sie auf den Schieberegler, falls SLAAC nicht verwendet werden soll (grau/links = SLAAC wird nicht verwendet, *Standard* bei aktiviertem *SecureCert-Feature*). |
| **ICMP Echo-Reply auf Echo-Request einer Multicast-/ Anycast-Adresse senden (IPv6):** | Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests beantwortet werden sollen (grün/rechts = Echo-Requests werden beantwortet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests nicht beantwortet werden sollen (grau/links = Echo-Requests werden nicht beantwortet). |
| **ICMP-Destination-Unreachable-Nachrichten senden (IPv6):** | Klicken Sie auf den Schieberegler, falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann (grün/rechts = Fehlermeldung wird gesendet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls keine ICMPv6-Fehlermeldungen gesendet werden sollen (grau/links = Fehlermeldung wird nicht gesendet). |
| **Redirect-Meldungen verarbeiten (IPv6):** | Klicken Sie auf den Schieberegeler, falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen (grün/rechts = Redirect-Meldungen werden verarbeitet, *Standard*).<br>Klicken Sie auf den Schieberegler, falls Redirect-Meldungen nicht verarbeitet werden sollen (grau/links = Redirect-Meldungen werden nicht verarbeitet). |
| **Duplicate Address Detection (IPv6):** | Klicken Sie auf den Schieberegler, falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird (grün/rechts = es wird auf doppelte Adressen geprüft, *Standard*).<br>Klicken Sie auf den Schieberegler, falls nicht auf doppelt IPv6-Adressen geprüft werden soll (grau/links = es wird nicht auf doppelte Adressen geprüft). |

7. Klicken Sie auf **Speichern**.

## Konfiguration der KVM-over-IP-Verbindung

**So konfigurieren Sie die KVM-over-IP-Verbindung:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Erfassen Sie im Abschnitt **Konfiguration** folgende Daten:

| | |
|---|---|
| **Control-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein (*Standard*: 18246). |
| **Communication-Port (K, M, msic):** | Geben Sie die Nummer des zu verwendenden Ports ein (*Standard*: 18245). |
| **Data-Port (AR, V):** | Geben Sie die Nummer des zu verwendenden Ports ein (*Standard*: 18244). |

6. Wählen Sie in der Zeile **Verbindungsaufbau über eigenes Zertifikat**, ob der Verbindungsaufbau zur Gegenstelle mit einem Zertifikat geschützt werden soll:

**WICHTIG:** Ein Verbindungsaufbau ist nur möglich, wenn die Gegenstelle dasselbe Zertifikat verwendet!

| | |
|---|---|
| **Deaktiviert:** | Der Verbindungsaufbau wird *nicht* durch ein Zertifikat geschützt.. |
| **Aktiviert, Netzwerk-Zertifikat verwenden:** | Das Netzwerk-Zertifikat wird für den Verbindungsaufbau verwendet<br>(siehe *Erstellung eines SSL-Zertifikats* auf Seite 27). |
| **Aktiviert, separates Zertifikat verwenden:** | Ein gekauftes Zertifikat einer Zertifizierungsstelle oder ein selbsterstelltes Zertifikat werden für den Verbindungsaufbau verwendet<br>(siehe *Erstellung eines SSL-Zertifikats* auf Seite 27).<br>Klicken Sie auf **Zertifikat hochladen** und wählen Sie die zu importierende .pem-Datei im Datei-Dialog aus. Klicken Sie auf **Upload und aktivieren**, um das Zertifikat zu speichern und zu aktivieren. |

7. Klicken Sie auf **Speichern**.

# Erweiterte Einstellungen der KVM-over-IP-Verbindung

## Bandbreite limitieren

In der Standardeinstellung verwendet das Gerät die maximal zur Verfügung stehende Bandbreite des Gigabit-Ethernets. Mittels manuellem Bandbreiten-Management können Sie die Übertragung an unterschiedliche Bandbreitenanforderungen anpassen.

**So stellen Sie das Bandbreiten-Limit der KVM-over-IP-Verbindung ein:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Geben Sie in der Zeile **Max. Bandbreite** des Abschnitts **Verbindungseinstellungen** das Bandbreiten-Limit in MBit/sec für die KVM-over-IP-Verbindung ein.

   **HINWEIS:** Der Wert **0** deaktiviert das Limit.

6. Klicken Sie auf **Speichern**.

## Klassifizierung der IP-Pakete (DiffServ)

Für QoS-Zwecke (Quality of Service; deutsch: Dienstgüte) haben Sie die Möglichkeit, **Differentiated Services Codepoints** (DSCP) zur Klassifizierung der IP-Pakete zu verwenden.

Mittels dieser Klassifizierung können Sie die Datenpakete beispielsweise durch einen Switch priorisieren.

Für die IP-Pakete der Keyboard, Maus und Steuerdaten (**Communication**-Datenpakete) sowie die IP-Pakete der Video-, Audio und RS232-Daten (**Data**-Datenpakete) können Sie je einen DSCP festlegen.

**So konfigurieren Sie die DSCPs der IP-Datenpakete:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Erfassen Sie im Abschnitt **Verbindungseinstellungen** folgende Daten:

| | |
|---|---|
| **DiffServ Communication:** | Bestimmen Sie den **Differentiated Services Codepoint** (DSCP) der zur Klassifizierung der IP-Pakete der **Communication**-Datenpakete verwendet wird. |
| **DiffServ Data:** | Bestimmen Sie den **Differentiated Services Codepoint** (DSCP) der zur Klassifizierung der IP-Pakete der **Data**-Datenpakete verwendet wird. |

**HINWEIS:** Berücksichtigen Sie, dass einige Netzwerkswitches für *alle* Datenpakete automatisch die Service-Klasse **Network Control** (DSCP-Name: CS6) vergeben.

In solchen Umgebungen darf die Option **DSCP 48** nicht ausgewählt werden!

6. Klicken Sie auf **Speichern**.

## Signale (de)aktivieren

In der Standardeinstellung werden neben Keyboard-, Video- und Mausdaten auch die Audio-Daten übertragen.

**So (de)aktivieren Sie die Übertragung des Audio-Signals:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Erfassen Sie im Abschnitt **Abschaltbare Signale** folgende Daten:

| | |
|---|---|
| **Audio:** | Wählen **Aktiviert** oder **Deaktiviert**. |

6. Klicken Sie auf **Speichern**.

## Zurücksetzen der KVM-over-IP-Verbindung des Rechnermoduls

Ein Rechnermodul, das mit einer IP-Matrix verbunden wurde, speichert die Pairingdaten der IP-Matrix *permanent* ab.

**So löschen Sie die Pairingdaten des Rechnermoduls:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Klicken Sie im Abschnitt **Remote** auf **Reset connection**.

## Beschränkung der KVM-over-IP-Gegenstellen (UID-Locking)

In der Standardeinstellung eines Rechnermoduls darf *jede* IP-Matrix eine KVM-over-IP-Verbindung zum Rechnermodul aufbauen.

**TIPP:** Aktivieren Sie die Funktion **UID-Locking**, falls Sie den Verbindungsaufbau nur *bestimmten* IP-Matrixswitches erlauben möchten.

**So (de)aktivieren Sie das UID-Locking:**

1. Starten Sie die Webapplikation des **Rechnermoduls**.
2. Klicken Sie im Menü auf **RemoteGateways**.
3. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
4. Klicken Sie auf den Reiter **KVM-Verbindung**.
5. Tätigen Sie im Abschnitt **UID-Locking** die gewünschten Einstellungen:

| | |
|---|---|
| **UID-Locking:** | Nur die in der Liste angegebenen Gegenstellen dürfen eine KVM-over-IP-Verbindung herstellen (**Aktiviert**) oder alle Gegenstellen dürfen eine Verbindung aufbauen (**Deaktiviert**). |
| **Verbundene Geräte-UIDs:** | Aktivieren Sie bei eingeschaltetem UID-Locking den **Erlaubt**-Schieberegler in der Zeile jedes Gerätes, das eine Verbindung zum Rechnermodul aufbauen darf. |
| **IP-Matrix hinzufügen:** | Klicken Sie auf diese Schaltfläche und geben Sie die UID der IP-Matrix ein, die eine Verbindung mit diesem Rechnermodul herstellen darf. Klicken Sie abschließend auf **Speichern**. |
| **Entfernen:** | Klicken Sie auf eine erlaubte IP-Matrix und anschließend auf **Entfernen**, um die Erlaubnis zu widerrufen. |

6. Klicken Sie auf **Speichern**.

# Verwendete Netzwerk-Ports und Protokolle

Die folgenden Netzwerk-Ports und Protokolle können bei KVM-over-IP von G&D verwendet werden.

**WICHTIG:** Stellen Sie sicher, dass diese Ports und Protokolle in Ihrem Netzwerk nicht blockiert sind.

**HINWEIS:** Es ist möglich, dass weitere Ports verwendet werden.

| Port | Service | Type | Beschreibung | Anmerkung |
|---|---|---|---|---|
| - | IGMP | IGMP | IGMP Multicast | nicht veränderbar |
| - | L2 Multicast | | 01:0F:F4.. Device Finder | nicht veränderbar |
| - | IPSec | ESP | IPSec Encapsulating Security Payload | nicht veränderbar |
| - | IPSec | AH | IPSec Authentication Header | nicht veränderbar |
| **22** | SSH | TCP | optional Kommunikation RemoteAccess-IP-CPU und RemoteTargets | veränderbar |
| **67** | DHCP | UDP | DHCP-Server | nicht veränderbar |
| **68** | DHCP | UDP | DHCP-Client | nicht veränderbar |
| **80** | http | TCP | zum Öffnen der Webapplikation (Weiterleitung auf https) | deaktivierbar, falls Weiterleitung nicht benötigt bzw. gewünscht wird |
| **123** | NTP | UDP | für Zeitsynchronisation | nicht veränderbar (s. Seite 37) |
| **161** | SNMP | UDP | optional SNMP agent | veränderbar |
| **162** | SNMP-Traps | UDP/ TCP | optional SNMP agent | veränderbar |

| | | | | |
|---|---|---|---|---|
| **389** | LDAP | UDP/ TCP | optional Kommunikation Authentifizierungsservice | nicht veränderbar (s. Seite 43) |
| **443** | https | SSL/ TCP | zum Öffnen der Webapplikation | nicht veränderbar |
| **445** | CIFS | TCP | für Auto-Backup-Funktion | veränderbar (s. Seite 71) |
| **514** | Syslog | UDP/ TCP | optional Syslog server 1/ Syslog server 2 | veränderbar (s. Seite 42) |
| **636** | Active Directory | UDP/ TCP | optional Kommunikation Authentifizierungsservice | nicht veränderbar (s. Seite 43) |
| **1812** | Radius | UDP/ TCP | optional Kommunikation Authentifizierungsservice | nicht veränderbar (s. Seite 43) |
| **2049** | NFS | UDP/ TCP | für Auto-Backup-Funktion | veränderbar (s. Seite 71) |
| **3389** | RDP | TCP | optional Kommunikation RemoteAccess-IP-CPU und RemoteTargets | veränderbar |
| **5900** | VNC | TCP | optional Kommunikation RemoteAccess-IP-CPU | veränderbar |
| **6137** | U2-LAN | UDP | optional Kommunikation U2-LAN | nicht veränderbar |
| **18244** | KMV-over-IP | TCP | KVM-over-IP: Data-Port (Video) | veränderbar (s. Seite 81) |
| **18245** | KVM-over-IP | TCP | KVM-over-IP: Communication Port (K, M, misc) | veränderbar (s. Seite 81) |
| **18246** | KVM-over-IP | TCP | KVM-over-IP: Control Port und IPSec Internet Key Exchange (IKE) | veränderbar (s. Seite 81) |
| **27994** | Remote-Port | UDP/ TCP | optional Remote control access, z. B. IP Control API | veränderbar |
| **27996** | Database communica-tion | TCP | optional Remote control access, z. B. MatrixGuard | veränderbar |

| | | | | |
|---|---|---|---|---|
| **37996** | Database communica-tion | TCP | interne Kommunikation | nicht veränderbar |

# 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

Über das Konfigurationsmenü können Sie eine Ansicht mit verschiedenen Statusinformationen aufrufen.

**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** | |
|---|---|
| **Name:** | Name des Geräts |
| **Geräte-ID:** | physikalische ID des Geräts |
| **Status:** | aktueller Status (**Online** oder **Offline**) des Geräts |
| **Klasse:** | Geräteklasse |

| **Hardware-Informationen** | |
|---|---|
| **Firmware name:** | Bezeichnung der Firmware |
| **Firmware rev.:** | Firmware-Version |
| **Hardware rev.:** | Hardware-Revision |
| **IP-Adresse Network:** | IP-Adresse(n) der Schnittstelle *Network* |
| **IP-Adresse Transmission:** | IP-Adresse(n) der Schnittstelle *Transmission* |
| **MAC Network:** | MAC-Adresse der Schnittstelle *Network* |
| **MAC Transmission:** | MAC-Adresse der Schnittstelle *Transmission* |
| **Serial number:** | Seriennummer des Geräts |

| **Aktive Features** |
|---|
| In diesem Bereich werden alle aktivierten Zusatzfunktionen aufgelistet. |

| **Link-Status** | |
|---|---|
| **Link detected:** | Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**). |
| **Auto-negotiation:** | Die Übertragungsgeschwindigkeit und das Duplex-Verfahren wurden automatisch (**ja**) oder manuell vom Administrator konfiguriert (**nein**). |
| **Speed:** | Übertragungsgeschwindigkeit |
| **Duplex:** | Duplexverfahren (**full** bzw. **half**) |

**HINWEIS:** Zusätzlich werden die *Monitoring*-Informationen des Gerätes angezeigt.

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

# NOTIZEN

# NOTIZEN

# NOTIZEN

# G&D. FEELS RIGHT.

**Headquarters | Hauptsitz**

**Guntermann & Drunck GmbH Systementwicklung**

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

**US Office**

G&D North America Inc.
4540 Kendrick Plaza Drive | Suite 100
Houston, TX 77032 | United States
Phone +1-346-620-4362
sales.us@gdsys.com

**Middle East Office**

Guntermann & Drunck GmbH
Dubai Studio City | DSC Tower
12th Floor, Office 1208 | Dubai, UAE
Phone +971 4 5586178
sales.me@gdsys.com

**APAC Office**

Guntermann & Drunck GmbH
60 Anson Road #17-01
Singapore 079914
Phone +65 9685 8807
sales.apac@gdsys.com