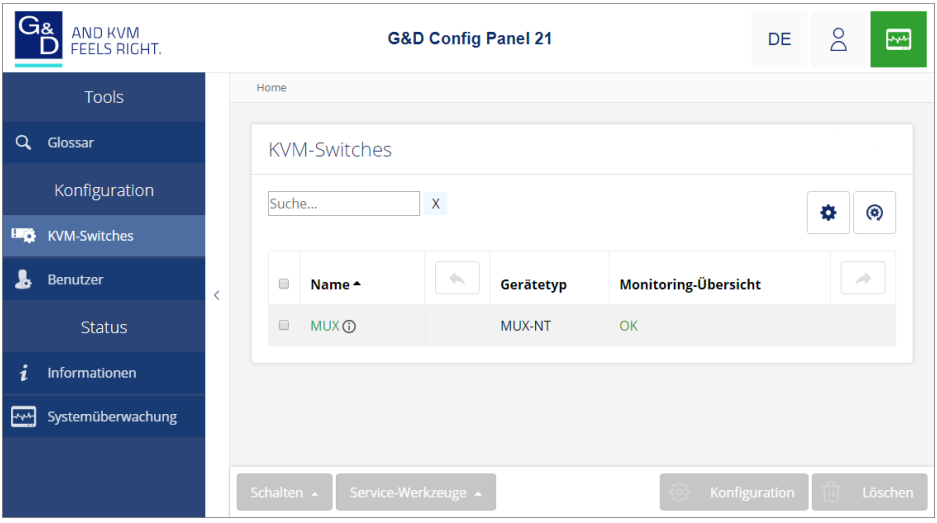
G&D MUX-NT-Serie

DE Webapplikation »Config Panel«
Konfiguration des KVM-Switches



A9100323-1.41

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 1.41 – 20.11.2024
Config Panel 21-Version: 1.6.000

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: KVM-Switches

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

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 128
- Microsoft Edge 127
- Mozilla Firefox 131

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 Netzwerk-einstellungen

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

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

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

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

1. Verbinden Sie die Netzwerkschnittstelle eines beliebigen Rechners mit der Schnittstelle *Network A* des Gerätes. Verwenden Sie hierzu ein Twisted-Pair-Kabel der Kategorie 5 (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* ab Seite 20 beschrieben.

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

6. Entfernen Sie die Twisted-Pair-Kabelverbindung zwischen dem Rechner und dem Gerät.
7. Integrieren Sie das Gerät in das lokale Netzwerk.

Erste Schritte

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

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

Start der Webapplikation

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

So starten Sie die Webapplikation:

1. Geben in der Adresszeile folgende URL ein:

   https://[IP-Adresse des Gerätes]

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

Nutzungsbedingungen zustimmen:	Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren.
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: Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde
(siehe *Anzeigen von Nutzungsbedingungen* ab Seite 12).

HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 49 ff.) und aktiviert wurde (s. Seite 63 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 67).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

HINWEIS: Das voreingestellte *Admin*-Passwort von Geräten mit Produktionsdatum vor Januar 2021 lautet **4658**.

3. Klicken Sie auf **Login**.
4. Klicken Sie auf das Icon **Config Panel 21**.

> **HINWEIS:** Alternativ zum **Config Panel 21** können Sie nach dem Login das Tool **EasyControl** (s. Seite 16) öffnen.

Bedienung der Webapplikation

Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus mehreren Bereichen:

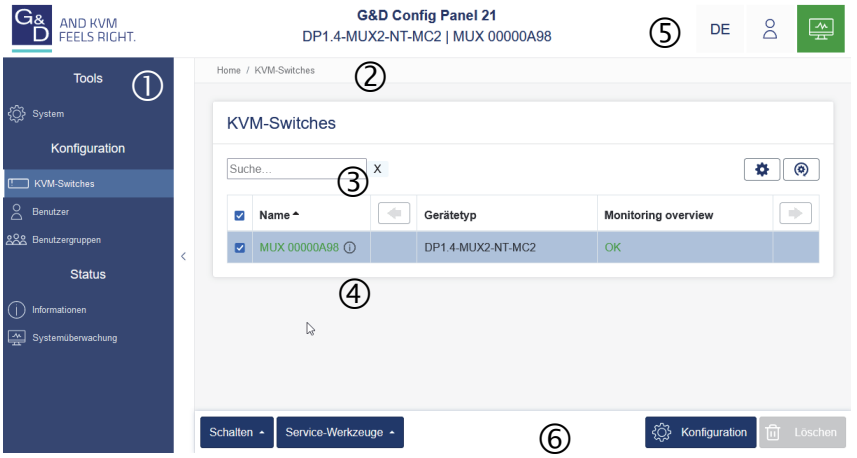


Abbildung 1: Benutzeroberfläche der Webapplikation

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. 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. 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. Um die Filterung aufzuheben, klicken Sie auf **[X]**.
Hauptansicht ④:	Nach der Auswahl eines Themenbereichs im Menü werden hier die Inhalte des Themenbereichs dargestellt.

Schnellzugriffe ⑤	**Sprachauswahl:** Die Sprachkennung (beispielsweise **DE** für *Deutsch*) zeigt die derzeit aktive Sprache in der Webapplikation an. Zur Umschaltung der Sprache klicken Sie auf die Sprachkennung. Daraufhin öffnet sich ein Untermenü, das die unterstützten Sprachen und die zugehörigen Kennungen anzeigt. Schalten Sie mit einem Klick auf die gewünschte Sprache die Sprache um. **Benutzer:** Nach einem Klick auf das Benutzersymbol öffnet sich ein Untermenü: ▪ Im Untermenü wird der Name des aktiven Benutzers angezeigt. ▪ Mit einem Klick auf *Benutzer* gelangen Sie zu den Benutzereinstellungen des aktiven Benutzers. ▪ Klicken Sie auf *Abmelden*, um die aktive Sitzung zu beenden. **Monitoring-Status:** Dieses Icon zeigt Ihnen auf den ersten Blick, ob alle Monitoringwerte im Normbereich sind (grünes Icon) oder mindestens ein Monitoring-Wert auffällig ist (gelbes oder rotes Icon). Das Icon *Monitoring-Status* nimmt jeweils die Farbe des *schlechtesten* Monitoring-Wertes an. Wird das Icon in gelber oder roter Farbe angezeigt, gelangen Sie mit einem Klick auf das Icon in den Dialog *Aktive Alarme*.
Schaltflächen ⑥**:**	Abhängig vom dargestellten Dialog werden in diesem Bereich verschiedene Schaltflächen angezeigt.

Häufig verwendete Schaltflächen

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

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. Erst nach einem Klick auf **Speichern** oder **Abbrechen** werden die Daten permanent gespeichert oder verworfen.

Tabellenspalten konfigurieren

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

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

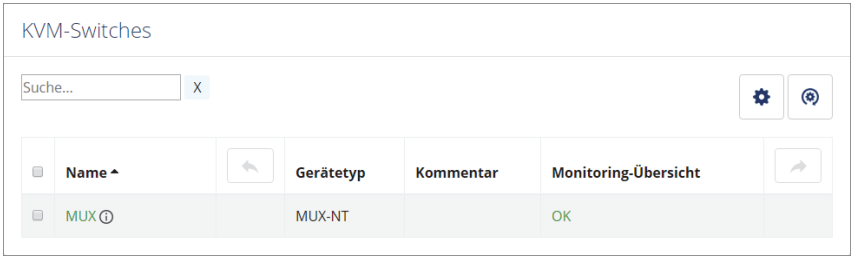


Abbildung 2: Tabellenspalten (Auswahl) eines KVM-Switches

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.

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 67) und Anlage eines neuen Benutzerkontos (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 62) 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)
4. Geben Sie im Feld **Mindestanzahl Großbuchstaben (z.B. ABCDEF)** die gewünschte Mindestanzahl an Großbuchstaben innerhalb eines Passworts ein (*Standard*: 0
5. Geben Sie im Feld **Mindestanzahl Kleinbuchstaben (z.B. abcdef)** die gewünschte Mindestanzahl an Kleinbuchstaben innerhalb eines Passworts ein (*Standard*: 0)
6. Geben Sie im Feld **Mindestanzahl Ziffern (z.B. 012345)** die gewünschte Mindestanzahl an Ziffern innerhalb eines Passworts ein (*Standard*: 0)
7. Geben Sie im Feld **Mindestanzahl Sonderzeichen (z.B. !#%&?@)** die gewünschte Mindestanzahl an Sonderzeichen innerhalb eines Passworts ein (*Standard*: 0)
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)

   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.

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, 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), max. 1.440 Minuten)
5. Klicken Sie auf **Speichern**.

Versionsnummer der Webapplikation anzeigen

So zeigen Sie die Versionsnummer der Webapplikation an:

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

Webapplikation beenden

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

> **WICHTIG:** Verwenden Sie immer die *Abmelden*-Funktion nach Abschluss Ihrer Arbeit mit der Webapplikation.
>
> Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die Webapplikation:

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

Kanalumschaltung via EasyControl

Das integrierte Umschalt-Tool **EasyControl** können Sie einsetzen, um den aufgeschalteten Kanal zu visualisieren und die schnelle Umschaltung (auch via Touchscreen-Gerät) zuzulassen.

Alle Benutzer mit der Berechtigung **Config Panel Login** (s. Seite 74) können das Umschalt-Tool verwenden.

Start des Umschalt-Tools »EasyControl«

So starten Sie das Umschalt-Tool:

1. Geben in der Adresszeile folgende URL ein:

   https://[IP-Adresse des Gerätes]

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

Nutzungs-bedingungen 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 12).
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 49 ff.) und aktiviert wurde (s. Seite 63 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 67).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

HINWEIS: Das voreingestellte *Admin*-Passwort von Geräten mit Produktionsdatum vor Januar 2021 lautet **4658**.

3. Klicken Sie auf **Login**.
4. Klicken Sie auf das Icon **EasyControl**.

Umschalten des aktiven KVM-Kanals

Die Bedienoberfläche besteht aus drei Schaltflächen zur Umschaltung zwischen den drei Kanälen des KVM-Switches.

Bei Verwendung des Standard-Farbschema kennzeichnet ein grüner Rahmen den derzeit aufgeschalteten Kanal.

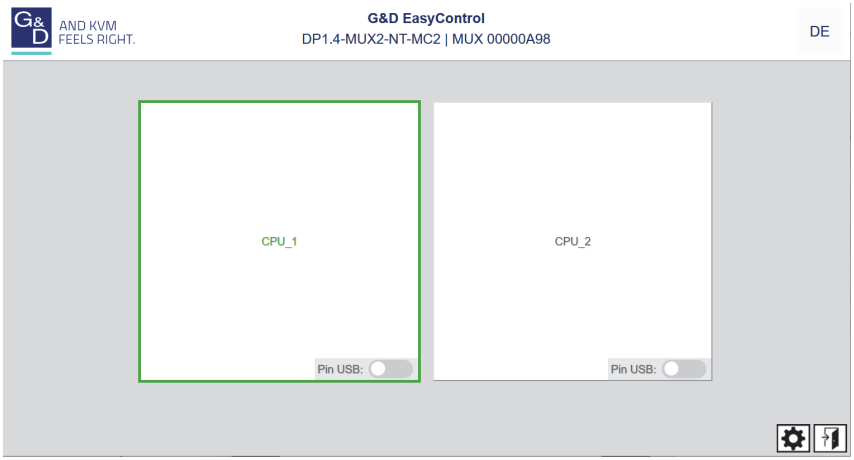


Abbildung 4: Benutzeroberfläche des Umschalt-Tools »EasyControl«

So schalten Sie auf einen anderen KVM-Kanal um:

- Klicken Sie auf die Schaltfläche des auszuschaltenenden Kanals.

Geräte an USB 3.0-Schnittstellen permanent umschalten

Mit der USB-Haltefunktion können Sie die, an die Schnittstelle »USB 3.0 Devices« angeschlossenen Geräte, permanent auf einen bestimmten Kanal aufschalten. Die permanente Schaltung dieser Geräte wird bei späteren Umschaltungen des KVM-Kanals beibehalten.

So schalten Sie die Geräte an den USB 3.0-Schnittstellen permanent auf einen bestimmten Kanal:

- Schieben Sie den Schieberegler **Pin USB** des Kanals, dessen USB 3.0-Schnittstellen permanant aufgeschaltet bleiben sollen, nach *rechts*.

So beenden Sie die permanente Schaltung der Geräte an den USB 3.0-Schnittstellen:

- Schieben Sie den Schieberegler **Pin USB** des Kanals, dessen USB 3.0-Schnittstellen permanant aufgeschaltet sind, nach *links*.

Farbschema des Umschalt-Tools ändern

HINWEIS: Das ausgewählte Farbschema wird in den Benutzereinstellungen des aktiven Benutzers gespeichert. Bei der nächsten Verwendung des Umschalt-Tools wird das zuvor ausgewählte Farbschema angewendet.

So ändern Sie das anzuwendende Farbschema des Umschalt-Tools:

1. Klicken Sie rechts unten auf das Zahnradsymbol.
2. Klicken Sie auf die Schaltfläche des gewünschten Farbschemas (**Skin 1**, **Skin 2** oder **Skin 3**).
3. Jedes Farbschema liegt in einer Variante für helle und dunkle Arbeitsumgebungen vor. Wählen Sie die gewünschte Variante aus:

Bright:	Variante für helle Arbeitsumgebungen anwenden
Dark:	Variante für dunkle Arbeitsumgebungen anwenden

4. Klicken Sie erneut auf das Zahnradsymbol, um die Einstellungen zu schließen.

Umbenennung der Kanal-Kanäle

WICHTIG: Ausschließlich Benutzer mit **Superuser**-Berechtigung können die Namen der einzelnen KVM-Kanäle im Umschalt-Tool editieren.

So ändern Sie die Namen der KVM-Kanäle:

1. Klicken Sie rechts unten auf das Zahnradsymbol ([⚙]).
2. Editieren Sie die Namen in den Feldern **Kanal x**.
3. Klicken Sie auf **Speichern**.
4. Klicken Sie erneut auf das Zahnradsymbol, um die Einstellungen zu schließen.

Beenden des Umschalt-Tools »EasyControl«

So beenden Sie das Umschalt-Tool:

1. Klicken Sie auf das **Exit**-Symbol ([⏻]) rechts unten.

Grundkonfiguration der Webapplikation

Netzwerkeinstellungen

Das Gerät ist mit zwei Netzwerkschnittstellen (*Network A* und *Network B*) ausgestattet. Die Netzwerkschnittstellen erlauben die Integration eines Gerätes in bis zu zwei separate Netzwerke.

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

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. Klicken Sie im Menü auf **KVM-Switches**.
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 **Schnittstelle B** folgende Daten:

Betriebsmodus:	Wählen Sie den Betriebsmodus der **Schnittstelle A** bzw. **Schnittstelle B** aus: ▪ **Aus:** Netzwerkschnittstelle ausschalten. ▪ **Statisch:** Es wird eine statische IP-Adresse zugeteilt. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server. In der Drop-Down-Liste wird der Text **Link-Aggregation aktiv** angezeigt, falls die Schnittstelle zu einer Netzwerkschnittstellen-Gruppe hinzugefügt wurde. Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall im Bereich »Link-Aggregation«.
IP-Adresse:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die IP-Adresse der Schnittstelle an
Netzmaske:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die Netzmaske des Netzwerkes an.

6. Klicken Sie auf **Speichern**.

Konfiguration der globalen Netzwerkeinstellungen

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

So konfigurieren Sie die globalen Netzwerkeinstellungen:

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

Betriebsmodus:	Wählen Sie den gewünschten Betriebsmodus: ▪ **Statisch:** Verwendung von statischen Einstellungen. ▪ **DHCP:** Bezug der Einstellungen von einem DHCP-Server.
Host-Name:	Geben Sie den Host-Namen des Gerätes ein. **WICHTIG:** Falls bei aktiviertem DHCP der DHCP-Server selbst keinen Host-Namen vergibt, wird der hier erfasste Host-Name verwendet. Ansonsten wird der vom DHCP-Server bezogene Host-Name verwendet.
Im Betriebsmodus *DHCP* werden die folgenden Einstellungen automatisch bezogen. Eine Eingabe ist nicht möglich.	
Domäne:	Geben Sie die Domäne an, welcher das Gerät angehören soll.
Gateway:	Geben Sie die IP-Adresse des Gateways an.
DNS-Server 1:	Geben Sie die IP-Adresse des DNS-Servers an.
DNS-Server 2:	Geben Sie *optional* die IP-Adresse eines weiteren DNS-Servers an.

6. Klicken Sie auf **Speichern**.

Ausfallsicherheit der Netzwerkverbindung durch Link-Aggregation erhöhen

In der Standardeinstellung können beide Netzwerkschnittstellen parallel eingesetzt werden, um beispielsweise aus zwei verschiedenen Netzwerksegmenten auf die Webapplikation zuzugreifen.

Zur Erhöhung der Ausfallsicherheit können die Netzwerkschnittstellen via *Link-Aggregation* zu einer Gruppe zusammengefasst werden. Innerhalb der Gruppe ist stets nur eine Schnittstelle aktiv. Eine andere Schnittstelle wird nur aktiv, falls die aktive Schnittstelle ausfällt.

Zur Überwachung der Schnittstellen stehen zwei verschiedene Modi zur Verfügung:

- **MII-Modus:** Der Carrier-Status der Netzwerkschnittstelle wird über das *Media Independent Interface* überwacht. In diesem Modus wird lediglich die Funktionalität der Netzwerkschnittstelle geprüft.

- **ARP-Modus:** Über das *Address-Resolution-Protokoll* werden Anfragen an ein ARP-Target im Netzwerk gesendet. Die Antwort des ARP-Targets bestätigt sowohl die Funktionalität der Netzwerkschnittstelle, als auch eine einwandfreie Netzwerkverbindung zum ARP-Target.

Ist das ARP-Target zwar mit dem Netzwerk verbunden, aber temporär offline, können die Anfragen nicht beantwortet werden. Bestimmen Sie daher mehrere ARP-Targets, um auch bei Ausfall eines ARP-Targets eine Rückmeldung mindestens eines Targets zu erhalten.

HINWEIS: Die Kombination des **MII-** und des **ARP-Modus** ist nicht möglich!

So konfigurieren Sie die Einstellungen einer Netzwerkschnittstellen-Gruppe:

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

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Link-Aggregation**.

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

Name:	Geben Sie den gewünschten Namen der Netzwerkschnittstellen-Gruppe ein.
Betriebsmodus:	Wählen Sie den Betriebsmodus der Netzwerkschnittstellen-Gruppe aus: ▪ **Aus:** Link-Aggregation ausschalten. *Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall im Bereich »Schnittstellen«.* ▪ **Statisch:** Es wird eine statische IP-Adresse zugeteilt. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server.
IP-Adresse:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die IP-Adresse der Schnittstelle an.
Netzmaske:	Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die Netzmaske des Netzwerkes an.

6. Erfassen Sie im Abschnitt **Parameter** folgende Daten:

Primärer Follower:	Wählen Sie, ob der Datenverkehr bevorzugt über die Schnittstelle *Network A* (**Schnittstelle A**) bzw. *Network B* (**Schnittstelle B**) erfolgen soll. Sobald die ausgewählte Schnittstelle verfügbar ist, wird diese Schnittstelle für den Datenverkehr verwendet. Wählen Sie die Option **Keiner**, wird der Datenverkehr über eine beliebige Schnittstelle gesendet. Eine Umschaltung erfolgt nur, wenn die aktive Schnittstelle ausfällt.
Link-Monitoring:	Wählen Sie, ob der **MII-** oder der **ARP-Modus** (s. Erläuterung oben) zum Monitoring der Schnittstelle verwendet werden soll.
MII-Down-Delay:	Wartezeit in Millisekunden, bevor eine ausgefallene Netzwerkschnittstelle deaktiviert wird. Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.
MII-Up-Delay:	Wartezeit in Millisekunden, bevor eine wiederhergestellte Netzwerkschnittstelle aktiviert wird. Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.
ARP-Intervall:	Geben Sie das Intervall (100 bis 10.000 Millisekunden) ein, nach welchem eine Prüfung auf eingegangene ARP-Pakete der Netzwerkschnittstellen erfolgt.

ARP-Validierung:	Die Validierung stellt sicher, dass das ARP-Paket für eine bestimmte Netzwerkschnittstelle von einem der angegebenen ARP-Targets generiert wurde. Wählen Sie, ob bzw. welche der eingehenden ARP-Pakete validiert werden sollen: ▪ **Keine:** Die ARP-Pakete werden nicht validiert (Standard). ▪ **Aktiv:** Ausschließlich die ARP-Pakete der aktiven Netzwerkschnittstelle werden validiert. ▪ **Backup:** Ausschließlich die ARP-Pakete der inaktiven Netzwerkschnittstelle werden validiert. ▪ **Alle:** Die ARP-Pakete aller Netzwerkschnittstellen der Gruppe werden validiert.
ARP-Target:	Die Tabelle enthält eine Liste aller konfigurierten ARP-Targets. Verwenden Sie die Schaltflächen **Hinzufügen**, **Ändern** und **Löschen**, um die ARP-Targets zu verwalten.

7. Klicken Sie auf **Speichern**.

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 **KVM-Switches**.
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 **Schnittstelle B** werden Ihnen folgende Daten angezeigt:

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

6. Klicken Sie auf **Speichern**.

Netzfilterregeln einrichten und administrieren

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

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

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

Neue Netzfilterregel erstellen

So erstellen Sie eine neue Netzfilterregel:

1. Klicken Sie im Menü auf **KVM-Switches**.
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: ▪ **Alle** ▪ **Schnittstelle A** ▪ **Schnittstelle B** ▪ **Link-Aggregation group**
Option:	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: ▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. ▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.

IP-Adresse/ Netzmaske:	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes **Netzmaske** – den Adressraum der IP-Adressen ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x ▪ **0.0.0.0/0:** alle IP-Adressen **HINWEIS:** Innerhalb einer Regel können wahlweise die *IP-Adresse* und/ oder eine *MAC-Adresse* angegeben werden.
MAC-Adresse:	Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist. **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. ▪ **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 **KVM-Switches**.
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: ▪ **Alle** ▪ **Schnittstelle A** ▪ **Schnittstelle B** ▪ **Link-Aggregation group**
Option:	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: ▪ **Normal:** Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. ▪ **Invertiert:** Die Regel gilt für Datenpakete, deren Absenderinformation *nicht* der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.
IP-Adresse/ Netzmaske:	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes **Netzmaske** – den Adressraum der IP-Adressen ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x ▪ **0.0.0.0/0:** alle IP-Adressen

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

MAC-Adresse:	Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist. 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. ▪ **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 **KVM-Switches**.
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 **KVM-Switches**.
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 (s. Seite 30 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

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

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

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

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

Besonderheiten für komplexe KVM-Systeme

Falls innerhalb eines KVM-Systems verschiedene G&D-Geräte miteinander kommunizieren sollen, ist bei der Erstellung von Zertifikaten für diese Geräte das identische *Certificate Authority*-Zertifikat (s. Seite 31) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 35) 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 Zertifikats im Gerät erfolgreich geprüft werden.

Erzeugen eines beliebigen Zertifikats

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

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

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

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

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

So erstellen Sie die Zertifikatsanforderung:

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

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

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

   Nachfolgend sind die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (eg, city)	Siegen
Organization Name (eg, company)	Guntermann & Drunck GmbH
Organizational Unit Name (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 31) verwenden, können die Geräte mit-einander kommunizieren.

So wählen Sie das zu verwendende SSL-Zertifikat:

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

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

5. Wählen Sie das zu verwendende Zertifikat aus:

G&D-Zertifikat #1:	Dieses Zertifikat ist bei *neuen* Geräten ab Werk aktiviert. **HINWEIS:** Achten Sie darauf, dass Sie innerhalb des KVM-Systems für alle Geräte dasselbe Zertifikat verwenden.
G&D-Zertifikat #2:	Dieses Zertifikat wird von einigen älteren G&D-Geräten mit integrierter Webapplikation unterstützt.
Eigenes Zertifikat:	Aktivieren Sie diese Option, wenn Sie ein gekauftes Zertifikat einer Zertifizierungsstelle oder ein selbsterstelltes Zertifikat verwenden möchten. Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat: ▪ Klicken Sie auf **Zertifikat aus Datei importieren** und wählen Sie die zu importierende .pem-Datei im Datei-Dialog aus. Alternativ kopieren Sie den Klartext des Zertifikats des Servers, den privaten Schlüssel des Servers sowie das Zertifikat der Zertifizierungsstelle in das Textfeld. ▪ Klicken Sie auf **Upload und aktivieren**, um das importierte Zertifikat im Gerät zu speichern und zu aktivieren.

6. Klicken Sie auf **Speichern**.

WICHTIG: Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation (s. Seite 30 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

Durchführung von Firmware-Updates

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

Firmware-Update eines bestimmten Geräts

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

So aktualisieren Sie die Firmware eines bestimmten Geräts:

1. Klicken Sie im Menü auf **KVM-Switches**.
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 Produkt während dem Update **nicht** aus, und trennen Sie es **nicht** von der Stromversorgung.

Wiederherstellung der Werkseinstellungen

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

So stellen Sie die Werkseinstellungen wieder her:

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

Alle Einstellungen zurücksetzen:	Alle Einstellungen des Gerätes zurücksetzen.
Nur Einstellungen des lokalen Netzwerkes zurücksetzen:	Ausschließlich die lokalen Netzwerkeinstellungen 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 **KVM-Switches**.
2. Klicken Sie auf das gewünschte Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Neustart**.
4. Bestätigen Sie die Sicherheitsabfrage mit **Neustart**.

Netzwerkfunktionen der Geräte

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

Für können Sie u. a. folgende Funktionen konfigurieren:

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

NTP-Server

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

Zeitsynchronisation mit einem NTP-Server

So ändern Sie die Einstellungen bezüglich der NTP-Zeitsynchronisation:

1. Klicken Sie im Menü auf **KVM-Switches**.
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: ▪ **Deaktiviert** (*Standard*) ▪ **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: ▪ **Deaktiviert** (*Standard*) ▪ **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: ▪ **Deaktiviert** (*Standard*) ▪ **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 **KVM-Switches**.
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 **KVM-Switches**.
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: ▪ **Deaktiviert** ▪ **Aktiviert** (*Standard*)
Log-Level:	Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist (*Standard*: 6 - Info). 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 **KVM-Switches**.
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: ▪ **Deaktiviert** (*Standard*) ▪ **Aktiviert**
Log-Level:	Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist. 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.
IP-Adresse/ DNS-Name:	Geben Sie die IP-Adresse oder den Namen des Servers an, an welchen die Syslog-Meldungen zu senden sind.
Port:	Geben Sie den Port – üblicherweise 514 – an, auf welchem der Syslog-Server eingehende Meldungen annimmt.
Protokoll:	Wählen Sie das Protokoll – üblicherweise UDP – aus, auf welchem der Syslog-Server eingehende Meldungen annimmt: ▪ **TCP** ▪ **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 **KVM-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie Eintrag **Syslog**.
4. Klicken Sie auf **Syslog abrufen**.

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

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

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

Benutzerauthentifizierung mit Verzeichnisdiensten

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

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

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

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

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

- **Das Benutzerkonto existiert im Verzeichnisdienst, aber nicht im KVM-System**
  Ein Benutzer, der erfolgreich gegen den Verzeichnisdienst authentifiziert wurde, aber kein gleichnamiges Konto in der Datenbank des KVM-Systems besitzt, wird mit den Rechten des Benutzers *RemoteAuth* ausgestattet.
  Ändern Sie ggf. die Rechte dieses speziellen Benutzerkontos, um die Berechtigung von Benutzern ohne eigenes Konto einzustellen.

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

- **Das Benutzerkonto existiert im KVM-System, aber nicht im Verzeichnisdienst**
  Ist der Verzeichnisdienst erreichbar, meldet dieser, dass das Benutzerkonto nicht existiert. Der Zugang zum KVM-System wird dem Benutzer verwehrt.
  Ist der Server nicht erreichbar, aber der Fallback-Mechanismus aktiviert, kann sich der Benutzer mit dem im KVM-System gespeicherten Passwort anmelden.

  WICHTIG: Um zu vermeiden, dass bei Ausfall der Verbindung zum Verzeichnisdienst die Anmeldung eines im Verzeichnisdienst gesperrten oder deaktivierten Benutzers möglich ist, beachten Sie folgende Sicherheitsregeln:
  - Wird im Verzeichnisdienst ein Benutzerkonto deaktiviert oder gelöscht, ist diese Aktion auch in der Benutzerdatenbank des KVM-Systems durchzuführen!
  - Aktivieren Sie den Fallback-Mechanismus nur in begründeten Ausnahmefällen.

  WICHTIG: Bei Verwendung der Zwei-Faktor-Authentifizierung (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* ab Seite 49) 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 **KVM-Switches**.
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**
- **TACACS+**

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

HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 62).

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* auf Seite 49) kann der Fallback-Mechanismus **nicht** genutzt werden.

6. Klicken Sie auf **Speichern**.

Einrichtung der Zwei-Faktor-Authentifizierung am Gerät

Die standardmäßige Benutzer-Authentifizierung erfolgt über eine Passwort-Abfrage. Um die Sicherheit zu erhöhen, kann durch die Zwei-Faktor-Authentifizierung (2FA) ein zweiter, besitzbasierter Faktor abgefragt werden. Hierbei kommt ein Time-Based-One-Time-Password (TOTP) zum Einsatz, wobei es sich um ein zeitlich begrenzt gültiges 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 63).

So aktivieren Sie die 2FA am Gerät:

1. Klicken Sie im Menü auf **KVM-Switches**.
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*) ▪ **Aktiviert**
OTP-Server:	Wählen Sie die Option **Intern** (*Standard*), wenn ein interner, im Gerät bereitgestellter Authentifizierungsserver zum Einsatz kommen soll. Möchten Sie einen bestimmten externen Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus: ▪ **LDAP** ▪ **Active Directory** ▪ **Radius** ▪ **TACACS+** Erfassen Sie nach der Auswahl eines externen Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers in der sich öffnenden entsprechenden Dialogmaske.
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. ▪ **Nein** (*Standard*) ▪ **Ja**

HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Anlegen eines neuen Benutzerkontos* ab Seite 62).

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 40). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 42).

Informationen zur Aktivierung der Zwei-Faktor-Authentifizierung finden Sie auf Seite 63 ff.

Monitoring-Funktionen

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

Die folgende Abbildung zeigt beispielsweise die Monitoringwerte *Status*, *Main power* und *Temperature* eines Gerätes:

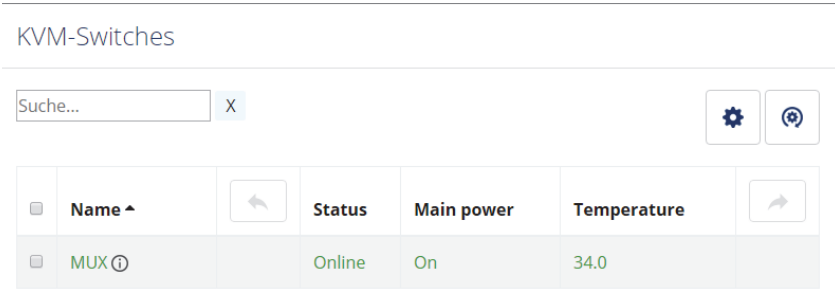


Abbildung 5: Detailansicht einer exemplarischen Monitoring-Tabelle

Die, für die Tabellenansicht (siehe *Tabellenspalten konfigurieren* auf Seite 8) 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 **KVM-Switches** einsehen.

So öffnen Sie die Liste aller Monitoring-Werte:

1. Klicken Sie im Menü auf **KVM-Switches**.
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 **KVM-Switches**.
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 **KVM-Switches**.
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 6) 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**.

Geräteüberwachung via SNMP

Das *Simple Network Management Protocol* (SNMP) wird zur Überwachung und Steuerung von Computern und Netzwerkgeräten verwendet.

Praktischer Einsatz des SNMP-Protokolls

Zur Überwachung und Steuerung von Computern und Netzwerkgeräten wird in einem Netzwerk ein *Network Management System* (NMS) betrieben, das die Daten der zu überwachenden Geräte von deren *Agents* anfordert und sammelt.

WICHTIG: Chinesische und kyrillische Zeichen werden von vielen Network-Management-Systemen nicht unterstützt.

Stellen Sie daher sicher, dass die verwendeten Passwörter solche Zeichen nicht enthalten!

HINWEIS: Ein *Agent* ist ein Programm, das auf dem überwachten Gerät läuft und dessen Status ermittelt. Über SNMP werden die ermittelten Daten an das *Network Management System* übermittelt.

Erkennt ein *Agent* ein schwerwiegendes Ereignis auf dem Gerät, kann er selbstständig ein *Trap*-Paket an das *Network Management System* senden. So wird sichergestellt, dass der Administrator kurzfristig über das Ereignis informiert wird.

Konfiguration des SNMP-Agents

So konfigurieren Sie den SNMP-Agent:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **SNMP-Agent**.

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

Status:	Durch Auswahl des entsprechenden Eintrags schalten Sie den SNMP-Agent aus (**Deaktiviert**) oder ein (**Aktiviert**).
Protokoll:	Wählen Sie das Protokoll (**TCP** oder **UDP**) – üblicherweise UDP – aus, über welches die SNMP-Pakete übertragen werden sollen.
Port:	Geben Sie den Port – üblicherweise 161 – an, auf welchem *eingehende* SNMP-Pakete akzeptiert werden.
SysContact:	Geben Sie die Kontaktdaten (beispielweise Durchwahl oder E-Mail-Adresse) des Administrators ein.
SysName:	Geben Sie den Namen des Gerätes ein.
SysLocation:	Geben Sie den Standort des Gerätes ein.

6. Möchten Sie Pakete der Protokollversion **SNMPv2c** verarbeiten, erfassen Sie im gleichnamigen Abschnitt die auf der folgenden Seite aufgeführten Daten.

Access:	Aktivieren Sie den lesenden Zugriff (**View**), schreibenden Zugriff (**Full**) oder verweigern Sie den Zugriff (**No**) über das *SNMPv2c*-Protokoll.
Source:	Geben Sie die IP-Adresse oder den Adressraum der Adressen eingehender SNMP-Pakete ein. **Beispiele:** ▪ **192.168.150.187:** nur die IP-Adresse 192.168.150.187 ▪ **192.168.150.0/24:** IP-Adressen des Raums 192.168.150.x ▪ **192.168.0.0/16:** IP-Adressen des Raums 192.168.x.x ▪ **192.0.0.0/8:** IP-Adressen des Raums 192.x.x.x
Read-only community:	Geben Sie die Bezeichnung einer bestimmten *Community* ein, welche auch im *Network Management System* gewählt wurde.

WICHTIG: Das Passwort (*Community*) der Pakete der Protokollversion *SNMPv2c* wird unverschlüsselt übertragen und kann daher leicht abgehört werden!

Verwenden Sie ggf. die Protokollversion *SNMPv3* (s. u.) und einen hohen *Security-Level*, um eine sichere Übertragung der Daten zu erreichen.

7. Möchten Sie Pakete der Protokollversion **SNMPv3** verarbeiten, erfassen Sie im gleichnamigen Abschnitt folgende Daten:

Access:	Aktivieren Sie den lesenden Zugriff (**View**) oder verweigern Sie den Zugriff (**No**) über das *SNMPv3*-Protokoll.
Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem *Network Management System* an.
Authentifizierungs-protokoll:	Wählen Sie das im *Network Management System* aktivierte Authentifizierungs-Protokoll aus: ▪ **SHA-1** ▪ **SHA-224** ▪ **SHA-256** ▪ **SHA-384** ▪ **SHA-512** (*Standard*) ▪ **MD5.** **HINWEIS:** Da inzwischen bekannt ist, dass **MD5** keine Kollisionsresistenz bietet, wird von der Verwendung abgeraten.
Authentifizierungs-passwort:	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem *Network Management System* an.
Security-Level:	Wählen Sie zwischen einer der folgenden Optionen: ▪ **noAuthNoPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll deaktiviert ▪ **authNoPriv:** Benutzer-Authentifizierung aktiviert, *Privacy*-Protokoll deaktiviert ▪ **authPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll aktiviert
Privacy-Protokoll:	Wählen Sie das im *Network Management System* aktivierte Privacy-Protokoll aus: ▪ **AES128** ▪ **AES192** ▪ **AES256** (*Standard*) ▪ **DES.** **HINWEIS:** Aufgrund der geringen Schlüssellänge von **DES** wird von der Verwendung abgeraten.
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem *Network Management System* an.

Engine-ID-Methode:	Wählen Sie, nach welcher Methode die **SnmpEngineID** vergeben werden soll: ▪ **Random:** Die *SnmpEngineID* wird bei jedem Neustart des Gerätes neu vergeben. ▪ **Fix:** Die *SnmpEngineID* entspricht der MAC-Adresse der ersten Netzwerkschnittstelle des Gerätes. ▪ **User:** Der im Feld *Engine-ID* eingetragene String wird als *SnmpEngineID* verwendet.
Engine-ID	Bei Verwendung der *Engine-ID-Methode* **User** geben Sie hier den String ein, der als *Engine-ID* verwendet wird.

8. Klicken Sie auf **Speichern**.

Hinzufügen und Konfiguration von SNMP-Traps

So fügen Sie einen neuen Trap hinzu oder bearbeiten einen vorhandenen Trap:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den Reiter **Netzwerk**.
3. Wählen Sie den Bereich **SNMP-Trap**.
4. Klicken Sie auf **Hinzufügen** bzw. auf **Bearbeiten**.
5. Erfassen Sie im Abschnitt **Global** folgende Daten:

Server:	Geben Sie die IP-Adresse des *Network Management Servers* ein.
Protokoll:	Wählen Sie das Protokoll (**TCP** oder **UDP**) – üblicherweise UDP – aus, über welches die SNMP-Pakete übertragen werden sollen.
Port:	Geben Sie den Port – üblicherweise 162 – an, auf welchem *ausgehende* SNMP-Pakete übertragen werden.
Versuche:	Geben Sie die Anzahl der Versand-Wiederholungen eines *SNMP Informs* an. **HINWEIS:** Eine Eingabe ist nur möglich, wenn im Feld *Notification type* die Option *Inform* gewählt wurde.
Timeout:	Geben Sie das Timeout (in Sekunden) ein, nach welchem die erneute Aussendung eines *SNMP Informs* erfolgt, wenn keine Bestätigung erfolgt. **HINWEIS:** Eine Eingabe ist nur möglich, wenn im Feld *Notification type* die Option *Inform* gewählt wurde.

Log-Level:	Wählen Sie den Schweregrad eines Ereignisses aus, ab welchem ein SNMP-Trap zu versenden ist. Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.

HINWEIS: Wählen Sie den Schweregrad *2 - Kritisch*, so werden bei Ereignissen dieses, wie auch der Schweregrade *1 - Alarm* und *0 - Notfall*, SNMP-Traps ausgesendet.

Version:	Wählen Sie, ob die Traps gemäß der Protokollversion *SNMPv2c* (**v2c**) oder *SNMPv3* (**v3**) erstellt und versendet werden.
Benachrichtigungsart:	Wählen Sie, ob die Ereignisse als *Trap*- oder *Inform*-Paket versendet werden.

HINWEIS: *Inform*-Pakete erfordern eine Bestätigung des *Network Management Systems*. Liegt diese nicht vor, wird die Übertragung wiederholt.

6. Haben Sie sich im letzten Schritt für die Protokollversion **SNMPv2c** entschieden, erfassen Sie im gleichnamigen Abschnitt die Bezeichnung der *Community*, welche auch im *Network Management System* gewählt wurde.

WICHTIG: Das Passwort (*Community*) der Pakete der Protokollversion *SNMPv2c* wird unverschlüsselt übertragen und kann daher leicht abgehört werden!

Verwenden Sie ggf. die Protokollversion *SNMPv3* (s. u.) und einen hohen *Security-Level*, um eine sichere Übertragung der Daten zu erreichen.

7. Haben Sie sich in Schritt 5. für die Protokollversion **SNMPv3** entschieden, erfassen Sie im gleichnamigen Abschnitt folgende Daten:

Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem *Network Management System* an.
Authentifizierungsprotokoll:	Wählen Sie das im *Network Management System* aktivierte Authentifizierungs-Protokoll aus: ▪ **SHA-1** ▪ **SHA-224** ▪ **SHA-256** ▪ **SHA-384** ▪ **SHA-512** (*Standard*) ▪ **MD5.**

HINWEIS: Da inzwischen bekannt ist, dass **MD5** keine Kollisionsresistenz bietet, wird von der Verwendung abgeraten.

Authentifizierungspasswort:	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem *Network Management System* an.

Security-Level:	Wählen Sie zwischen einer der folgenden Optionen: ▪ **noAuthNoPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll deaktiviert ▪ **authNoPriv:** Benutzer-Authentifizierung aktiviert, *Privacy*-Protokoll deaktiviert ▪ **authPriv:** Benutzer-Authentifizierung und *Privacy*-Protokoll aktiviert
Privacy-Protokoll:	Wählen Sie das im *Network Management System* aktivierte Privacy-Protokoll aus: ▪ **AES128** ▪ **AES192** ▪ **AES256** (*Standard*) ▪ **DES.** **HINWEIS:** Aufgrund der geringen Schlüssellänge von **DES** wird von der Verwendung abgeraten.
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem *Network Management System* an.
Engine-ID:	Geben Sie die *Engine-ID* des Trap-Receivers ein.

8. Klicken Sie auf **Speichern**.

So löschen Sie einen vorhandenen Trap:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den Reiter **Netzwerk**.
3. Wählen Sie den Bereich **SNMP-Trap**.
4. Klicken Sie in der Zeile des zu löschenden Receivers auf **Löschen**.
5. Klicken Sie auf **Speichern**.

XML-Steuerung des KVM-Switches (Remote-Control)

Die XML-Steuerung erlaubt die Steuerung des KVM-Switches über Drittherstellergeräte (beispielsweise AMX® und Crestron®). Der KVM-Switch verarbeitet die vom Drittherstellergerät über die Ethernet-Schnittstelle empfangenen XMLBefehle.

HINWEIS: Die detaillierte Erläuterung der Funktionen und Konfigurationseinstellungen erfolgt im separaten Handbuch »Installation und Bedienung«.

Benutzer und Gruppen

Effizienter Einsatz der Rechteverwaltung

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

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

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

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

Das Effektivrecht

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

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

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

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

Recht	Benutzer *Muster*	Gruppe *Office*	Gruppe *TargetConfig*	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 *Monitoring-Alarm bestätigen*.

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

Verwaltung von Benutzerkonten

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

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

Anlegen eines neuen Benutzerkontos

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

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 13).

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.
	HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Benutzerauthentifizierung mit Verzeichnisdiensten* ab Seite 46).
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.
	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 49), sind im Folgenden die Einstellungen für das Benutzerkonto vorzunehmen (s. Seite 63).

Aktivierung der Zwei-Faktor-Authentifizierung

HINWEIS: Für die Verwendung der Zwei-Faktor-Authentifizierung (2FA) muss zunächst die Einrichtung am Gerät erfolgen (s. Seite 49).

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

WICHTIG: Kommt ein externer Verzeichnisdienst zum Einsatz (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* ab Seite 49), 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 74), oder der Anwender muss mit dem entsprechenden Benutzerprofil angemeldet sein (s. Seite 74) und über das Recht *Eigenes Passwort ändern* (s. Seite 75) verfügen.

WICHTIG: Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 40). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 42).

HINWEIS: Die 2FA kann für fast alle Benutzerprofile aktiviert werden. Einzige Ausnahme stell 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. **WICHTIG:** Eine Eingabe muss im **Base32-Format** erfolgen. Klicken Sie auf **Generieren**, um einen neuen Schlüssel zu erhalten.
Hash-Algorithmus:	▪ **SHA1** ▪ **SHA256** (*Standard*) ▪ **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). **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*) ▪ **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). **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 & Sicherheitsschlüssel 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.
Verifikationscode:	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 68).

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 70).

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 46).

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 74)
oder das Recht *Eigenes Passwort ändern*
(siehe *Berechtigung zur Änderung des eigenen Passworts* ab Seite 75).

HINWEIS: Bei der Änderung des Passworts werden ggf. die festgelegten Passwort-Richtlinien (siehe *Passwort-Komplexität* auf Seite 13) 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. **HINWEIS:** Bei Benutzern mit aktiviertem Superuser-Recht (s. Seite 74 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. **HINWEIS:** Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 49 ff.) und aktiviert wurde (s. Seite 63 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 74
Config Panel Login	Login mit der Webapplikation *ConfigPanel*	Seite 74
EasyControl Login	Zugriff auf das *EasyControl*-Tool	Seite 75
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 75
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 75

Änderung der Gruppenzugehörigkeit eines Benutzerkontos

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

So ändern Sie die Gruppenzugehörigkeit eines Benutzerkontos:

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

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

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

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

6. Klicken Sie auf **Speichern**.

Aktivierung oder Deaktivierung eines Benutzerkontos

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

So aktivieren oder deaktivieren Sie ein Benutzerkonto:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Benutzerkonto zu aktivieren.

   Möchten Sie den Zugang zum System mit diesem Benutzerkonto sperren, so deaktivieren Sie das Kontrollkästchen.
4. Klicken Sie auf **Speichern**.

Löschen eines Benutzerkontos

So löschen Sie ein Benutzerkonto:

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

Verwaltung von Benutzergruppen

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

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

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

Anlegen einer neuen Benutzergruppe

Innerhalb des Systems können Sie bis zu 256 Benutzergruppen erstellen.

So erstellen Sie eine neue Benutzergruppe:

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

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 74
Config Panel Login	Login mit der Webapplikation *ConfigPanel*	Seite 74
EasyControl Login	Zugriff auf das *EasyControl*-Tool	Seite 75
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 75
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 75

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 zum Zugriff auf das EasyControl-Tool

So ändern Sie die Berechtigung zum Zugriff auf das *EasyControl*-Tool:

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 **EasyControl Login** zwischen folgenden Optionen:

Ja:	Zugriff auf das *EasyControl*-Tool erlaubt
Nein:	Zugriff auf das *EasyControl*-Tool 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 **KVM-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät.
3. Öffnen Sie das Menü **Service-Werkzeuge** und wählen Sie den Eintrag **Ident-LED**.
4. Klicken Sie auf **LED an** bzw. **LED aus**.
5. Klicken Sie auf das rote **[X]**, um den Dialog zu verlassen.

Sicherung der Konfigurationseinstellungen

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

So sichern Sie die Konfigurationseinstellungen des :

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

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

Sicherung der Konfigurationseinstellungen mit der Auto-Backup-Funktion

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

So verwenden Sie die Auto-Backup-Funktion:

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

Auto-Backup:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Auto-Backup-Funktion aus- und einschalten: ▪ **Deaktiviert** (*Standard*) ▪ **Aktiviert**
Dateiname-Präfix:	Geben Sie das Dateiname-Präfix ein. **HINWEIS:** Bei Aktivierung der Auto-Backup-Funktion wird das Feld Dateiname-Präfix automatisch mit der **UID** des Geräts gefüllt. Diesen Eintrag können Sie überschreiben. **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. **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. **WICHTIG:** Die Syntax der Pfadangabe unterscheidet sich je nach gewähltem Protokoll. **Beispiele:** ▪ **NFS:** *name:/verzeichnis1/verzeichnis2* ▪ **CIFS:** *//name/verzeichnis1/verzeichnis2*

Protokoll:	Wählen Sie zwischen den folgenden Protokollen: ▪ **NFS** (*Standard*) ▪ **CIFS**
Port:	Geben Sie den Port ein. Dieses Feld wird je nach Auswahl im Feld *Protokoll* automatisch gefüllt: ▪ **2049** (bei Auswahl *NFS*) ▪ **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: ▪ **Stunde** (Zahlen *0* bis *23*) ▪ **Minute** (Zahlen *0* bis *59*)
Auswahl des Tages:	Es stehen Ihnen die folgenden Auswahlmöglichkeiten zur Verfügung: ▪ **1.** bis **31. Tag des Monats** ▪ **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 43).

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

Wiederherstellung der Konfigurationseinstellungen

So stellen Sie die Konfigurationseinstellungen des wieder her:

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

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

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

7. Klicken Sie auf **Restore**.

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

HINWEIS: Nach dem Restore wird der Benutzer aus der Webapplikation abgemeldet.

8. Melden Sie sich nach Abschluss des Restore erneut in der Webapplikation an (siehe *Seite 4*) und führen Sie einen Neustart des Geräts aus (siehe *Seite 39*).

Freischaltung kostenpflichtiger Zusatzfunktionen

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

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

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

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

1. Klicken Sie im Menü auf **KVM-Switches**.
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 KVM-Switches

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

Grundkonfiguration der KVM-Switches

Änderung des Namens eines KVM-Switches

So ändern Sie den Namen eines KVM-Switches:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Geben Sie im Feld **Name** des Abschnitts **Gerät** den gewünschten Namen des KVM-Switches ein.
4. Klicken Sie auf **Speichern**.

Änderung des Kommentares eines KVM-Switches

Im Listenfeld der Webapplikation wird neben dem Namen eines KVM-Switches auch der erfasste Kommentar angezeigt.

> **TIPP:** Verwenden Sie das Kommentarfeld beispielsweise um den Standort des KVM-Switches zu vermerken.

So ändern Sie den Kommentar eines KVM-Switches:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Geben Sie im Feld **Kommentar** des Abschnitts **Gerät** einen beliebigen Kommentar ein.
4. Klicken Sie auf **Speichern**.

Einen KVM-Switch aus dem KVM-System löschen

Wird ein – zuvor im KVM-System integrierter – KVM-Switch durch das System nicht gefunden, geht das System davon aus, dass das Gerät ausgeschaltet ist.

Falls ein KVM-Switch dauerhaft aus dem System entfernt wurde, können Sie diesen manuell aus der Auflistung der KVM-Switches löschen.

HINWEIS: Es können ausschließlich *ausgeschaltete* KVM-Switches gelöscht werden.

So löschen Sie einen ausgeschalteten oder vom System getrennten KVM-Switch:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu löschenden KVM-Switch und anschließend auf **Löschen**.
3. Bestätigen Sie die erscheinende Sicherheitsabfrage durch Klick auf **Ja** oder brechen Sie den Vorgang durch Klick auf **Nein** ab.

Konfigurationseinstellungen der KVM-Switches

Gerätekonfiguration

Änderung der Hotkey-Taste

Die Hotkey-Taste wird zur Umschaltung auf einen Rechner verwendet. Betätigen Sie die Hotkey-Taste gleichzeitig mit einem Select-Key zur Umschaltung auf den entsprechenden Rechner.

HINWEIS: In der Standardeinstellung ist die Hotkey-Taste **Strg** voreingestellt.

Werden auf einem Rechner viele Anwendungsprogramme mit Tastenkombinationen bedient oder verschiedene KVM-Geräte in einer Kaskade verwendet, ist die Zahl der „freien" Tastenkombinationen möglicherweise eingeschränkt.

Falls ein Anwendungsprogramm oder ein anderes Gerät innerhalb der Kaskade den gleichen Hotkey verwendet, kann dieser geändert werden.

HINWEIS: Als Hotkey können Sie eine Taste oder eine Kombination aus den Tasten *Strg*, *Alt*, *Alt Gr*, *Win* oder *Shift* wählen.

So ändern Sie die Hotkey-Taste:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Wählen Sie im Feld **Hotkey-Modifizierer** des Abschnitts **Konfiguration** *mindestens* eine der aufgeführten Modifizierertasten durch Markierung des entsprechenden Kontrollkästchens:

   - **Strg**
   - **Alt**
   - **Alt Gr**
   - **Win**
   - **Shift**

   HINWEIS: Werden mehrere Modizierertasten ausgewählt, so sind diese gemeinsam zu betätigen, um den Hotkey auszulösen!

5. Klicken Sie auf **Speichern**.

Änderung des Select-Key-Sets

In der Standardeinstellung sind die Select-Keys **1** bis **4** (Set »**1…4**«) zur Umschaltung zwischen den am KVM-Switch angeschlossenen Rechnern aktiv.

BEISPIEL: Die Umschaltung zu Rechner 2 erfolgt in der Standardeinstellung mit der Tastenkombination **Hotkey+2** (Standard: **Strg+2**).

Falls eine der aus dem Select-Key-Set resultierenden Tastenkombinationen mit einer Tastenkombination eines eingesetzten Anwendungsprogramms kollidiert, kann sowohl die Hotkey-Taste (s. Seite 83) als auch das in diesem Abschnitt beschriebene Select-Key-Set geändert werden.

So ändern Sie das Select-Key-Set:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Wählen Sie im Feld **Select-Key-Set** des Abschnitts **Konfiguration** eine der folgenden Optionen:

1…4:	Aktivierung der Select-Keys **1**, **2**, **3**, **4**
Num1…4:	Aktivierung der Select-Keys **Num1**, **Num2**, **Num3**, **Num4**
A…D:	Aktivierung der Select-Keys **A**, **B**, **C**, **D**
F1…F4:	Aktivierung der Select-Keys **F1**, **F2**, **F3**, **F4**

HINWEIS: Alternativ zur gezielten Umschaltung auf einen Kanal mittels eines Select-Keys können Sie die Kanäle in auf- oder absteigender Folge mit den Step-Keys (s. separates Handbuch »Installation und Bedienung«) umschalten.

Die jeweils aktiven Step-Keys sind von der Auswahl der Select-Keys abhängig. Zu Ihrer Information werden Step-Keys hinter der Bezeichnung des Select-Key-Sets angezeigt.

5. Klicken Sie auf **Speichern**.

Switching (de)aktivieren

Die Umschaltung auf einen bestimmten Kanal kann wahlweise über die *Taster* am Gerät, über die konfigurierten *Select-Keys*, über die *IP-Control-API*, per SNMP oder über die Webapplikation *ConfigPanel* gesteuert werden.

Falls gewünscht, können Sie die Möglichkeiten der Umschaltung einschränken.

So (de)aktivieren Sie die verschiedenen Arten der Umschaltung:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Wählen Sie im Abschnitt **Switching deaktivieren** des Abschnitts **Konfiguration** die zu blockierenden Umschaltoptionen durch Markierung des/der entsprechenden Kontrollkästchen(s):.

Taster:	Umschaltung über die Taster an der Frontseite des Geräts deaktiviert.
IP-API & EasyControl:	Umschaltung über die IP-API und *EasyControl* deaktiviert.
Seriell:	Umschaltung über ein serielles Gerät deaktiviert.
Hotkeys:	Umschaltung via Select-Keys und Step-Keys deaktiviert.
Selectkey:	Umschaltung via Select-Keys deaktiviert.
Step/ Scan Up:	Umschaltung via Step-Key **Up** deaktiviert.
Step/ Scan Down:	Umschaltung via Step-Key **Down** deaktiviert.

4. Klicken Sie auf **Speichern**.

Umschaltung verzögern

Der KVM-Switch schaltet in der Standardeinstellung den aufzuschaltenden Kanal *sofort* nach Aufforderung (beispielsweise durch Betätigung eines Tasters oder durch Auslösung eines Select-Keys) um.

Die Signale des Rechners am aufzuschaltenden Kanal werden *sofort* an den Arbeitsplatz gesendet. Das Videosignal wird bereits nach kurzer Zeit am Monitor dargestellt.

Falls der angeschlossene Monitor das schnelle Umschalten nicht unterstützt und nach der Umschaltung kein Bild anzeigt, können Sie die Umschalt-Verzögerung aktivieren.

Bei aktivierter Umschalt-Verzögerung trennt der KVM-Switch zunächst die Signale des Arbeitsplatzes und schaltet nach der eingestellten Zeitspanne (max. 9.999 ms) den Zielkanal auf.

HINWEIS: Bei aktivierter Umschaltverzögerung verlängert sich die Zeit ohne Bild merklich.

So (de)aktivieren Sie die Umschaltverzögerung:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Geben Sie im Feld **Umschaltverzögerung** des Abschnitts **Konfiguration** die gewünschte Verzögerung in Millisekunden ein.

   HINWEIS: Die maximale Umschaltverzögerung beträgt 9.999 Millisekunden. Durch Eingabe des Wertes 0 wird die Verzögerung deaktiviert.

4. Klicken Sie auf **Speichern**.

Änderung des Scancode-Sets einer PS/2-Tastatur

Wird eine Taste der PS/2-Tastatur gedrückt, sendet der Tastaturprozessor ein Datenpaket, das als Scancode bezeichnet wird. Es gibt zwei gebräuchliche Scancode-Sets (Sets 2 und 3), die verschiedene Scancodes beinhalten.

Der KVM-Switch interpretiert in der Standardeinstellung alle Eingaben einer PS/2-Tastatur mit dem Scancode-Set 2.

TIPP: Falls das Verkettungszeichen (engl. *Pipe*, „|") nicht eingegeben werden kann oder die Pfeiltasten der Tastatur nicht wie erwartet funktionieren, ist die Umstellung auf das Scancode-Set 3 empfehlenswert.

So ändern Sie die Einstellung des Scancode-Sets:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Wählen Sie im Feld **Scancode-Set** des Abschnitts **Konfiguration** zwischen folgenden Optionen:

Set 2:	Aktivierung des Scancode-Sets 2 für PS/2-Tastatureingaben
Set 3:	Aktivierung des Scancode-Sets 3 für PS/2-Tastatureingaben

4. Klicken Sie auf **Speichern**.
5. Schalten Sie den KVM-Switch aus und wieder ein.

HINWEIS: Die Tastatur wird nach dem erneuten Einschalten initialisiert und das ausgewählte Scancode-Set angewendet.

Reinitialisierung von USB-Eingabegeräten

Sobald Sie eine USB-Tastatur bzw. -Maus an den KVM-Switch anschließen, wird das Eingabegerät initialisiert und kann ohne Einschränkungen verwendet werden.

Einige USB-Eingabegeräte erfordern eine Reinitialisierung der USB-Verbindung nach einer bestimmten Zeit. Aktivieren Sie die automatische Reinitialisierung der USB-Eingabegeräte, falls eine USB-Tastatur oder -Maus im laufenden Betrieb nicht mehr auf Ihre Eingaben reagiert.

So (de)aktivieren Sie die Reinitialisierung der USB-Eingabegeräte:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Wählen Sie im Feld **USB-Auto-Refresh** des Abschnitts **Konfiguration** eine der folgenden Optionen:

Nur fehlerhafte Geräte:	Der Status der USB-Geräte wird überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, wird dieses Gerät reinitialisiert (*Standard).*
Alle Geräte:	Der Status der USB-Geräte wird überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, werden alle angeschlossenen USB-Geräte reinitialisiert.
Aus:	Der Status der USB-Geräte wird **nicht** überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, findet **keine** Reinitialisierung statt.

4. Klicken Sie auf **Speichern**.

AuxSnoopEnable (de)aktivieren

HINWEIS: Diese Funktion wird ausschließlich von den **DP1.4**-Varianten der G&D MUX-NT-Serie unterstützt.

Ist das Bildsignal der Quelle zu schwach, z. B. bei Verwendung einer Docking-Station, kann **AuxSnoopEnable** aktiviert und über den Equalizer-Wert (siehe *Anpassung des Equalizer-Werts* auf Seite 96) angepasst werden.

HINWEIS: In der Regel sind hier die Standardeinstellungen beizubehalten.

Lediglich bei speziellen Quellen sind in Ausnahmefällen Justierungen vorzunehmen.

Sprechen Sie mit unserem Support, falls Sie Unterstützung wünschen.

So (de)aktivieren Sie AuxSnoopEnable:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Wählen Sie im Feld **AuxSnoopEnable** des Abschnitts **Konfiguration** eine der folgenden Optionen:

Deaktiviert:	Die Funktion ist deaktiviert (*Standard).*
Aktiviert:	Die Funktion ist aktiviert.

4. Klicken Sie auf **Speichern**.

Kanal-Konfiguration

Änderung des Namens eines Kanals

So ändern Sie einen Kanalnamen:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Geben Sie im Feld **Name** des Abschnitts **Kanal** den gewünschten Kanalnamen ein.
6. Klicken Sie auf **Speichern**.

Änderung des Kommentares eines Kanals

So ändern Sie den Kommentar eines Kanals:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Geben Sie im Feld **Kommentar** des Abschnitts **Kanal** einen beliebigen Kommentar ein.
6. Klicken Sie auf **Speichern**.

Aktivierung/Deaktivierung eines Kanals

An den KVM-Switch können Sie bis zu drei Rechner anschließen. Der am Gerät eingerichtete Arbeitsplatz kann sich auf diese Kanäle aufschalten.

Werden an den KVM-Switch weniger als drei Rechner angeschlossen, können die nicht genutzten Kanäle deaktiviert werden. Die Aufschaltung sowie die Auswertung der Monitoring-Daten wird somit verhindert.

So (de)aktivieren Sie einen Kanal:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Aktivieren Sie das Kontrollkästchens **Kanal aktiviert** im Abschnitt **Kanal**, um die Aufschaltung dieses Kanals zu erlauben oder deaktivieren Sie dieses Kontrollkästchens, um die Aufschaltung dieses Kanals zu verbieten.
6. Klicken Sie auf **Speichern**.

Aktivierung/Deaktivierung des Tastatur-Signals

In der Standardeinstellung werden die Signale der am Arbeitsplatz angeschlossenen Tastatur und Maus an den Rechner des aufgeschalteten Kanals übertragen.

In den Einstellungen des KVM-Switches können Sie die Übertragung des Tastatur-Signals für jeden einzelnen Kanal ein- bzw. ausschalten.

So (de)aktivieren Sie die Übertragung des Tastatur-Signals eines Kanals:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **Tastatur aktiviert** des gewünschten Kanals zwischen folgenden Optionen:

Aktiviert:	Die Tastatur-Signale werden an den Rechner dieses Kanals übertragen (*Standard*)
Deaktiviert:	Die Tastatur-Signale werden *nicht* an den Rechner dieses Kanals übertragen.

6. Klicken Sie auf **Speichern**.

Unterstützung für Multimedia- und Sondertasten

Im voreingestellten USB-Tastaturmodus **PC Multimedia** werden neben den Tasten des Standard-Tastaturlayouts einige Multimedia-Sondertasten wie *Lauter* und *Leiser* unterstützt.

Bei Einsatz eines *Apple Keyboards* erlaubt ein spezieller Tastaturmodus die Verwendung der Sondertasten dieser Tastaturen.

So schalten Sie die Unterstützung für Multimedia- oder Sondertasten ein oder aus:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **USB-Tastaturmodus** des gewünschten Kanals zwischen folgenden Optionen:

PC Standard:	Standard-Tastaturmodus
PC Multimedia:	Unterstützung für Multimedia-Sondertasten (*Standard*)
Apple A1243:	Tastaturmodus für Apple-Rechner
LK463:	LK463-kompatible Tastatur

6. Klicken Sie auf **Speichern**.

Videokanal-Konfiguration

HINWEIS: Falls Sie eine Multichannel-Variante des KVM-Switches erworben haben, sind die in diesem Bereich beschriebenen Konfigurationseinstellungen für jeden Multichannel-Kanal separat verfügbar.

Änderung des Namens eines Videokanals

So ändern Sie den Namen eines Videokanals:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Geben Sie im Feld **Videokanal** des Abschnitts **Videokanal** den gewünschten Kanalnamen ein.
6. Klicken Sie auf **Speichern**.

Änderung des Kommentares eines Videokanals

So ändern Sie den Kommentar eines Videokanals:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Geben Sie im Feld **Kommentar** des Abschnitts **Videokanal** einen beliebigen Kommentar ein.
6. Klicken Sie auf **Speichern**.

Aktivierung/Deaktivierung von DisplayPort-Power

HINWEIS: Diese Funktion wird ausschließlich von den **DP1.4**-Varianten der G&D MUX-NT-Serie unterstützt.

DisplayPort-Power liefert eine Spannung von 3,3V bei 500mA. Über diese Funktionalität können beispielsweise aktive Adapter betrieben werden.

So (de)aktivieren Sie DisplayPort-Power für einen Videokanal:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **DisplayPort-Power** des gewünschten Kanals zwischen folgenden Optionen:

Aktiviert:	DisplayPort-Power ist aktiviert (*Standard*).
Deaktiviert:	DisplayPort-Power ist deaktiviert.

6. Klicken Sie auf **Speichern**.

Anpassung des Equalizer-Werts

HINWEIS: Diese Funktion wird ausschließlich von den **DP1.4**-Varianten der G&D MUX-NT-Serie unterstützt.

Der Equalizer-Wert ermöglicht eine manuelle Anpassung zur besseren Übertragung der Bilddaten, falls das Bildsignal der Quelle zu schwach ist.

HINWEIS: In der Regel sind hier die Standardeinstellungen beizubehalten.

Lediglich bei speziellen Quellen sind in Ausnahmefällen Justierungen vorzunehmen.

Sprechen Sie mit unserem Support, falls Sie Unterstützung wünschen.

So passen Sie den Equalizer-Wert für einen Videokanal an:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **Equalizer-Wert** des gewünschten Kanals den gewünschten Wert (*Standard*: 4).
6. Klicken Sie auf **Speichern**.

EDID-Profil eines Monitores einlesen

HINWEIS: Diese Funktion wird ausschließlich von den **DL-DVI**-Varianten der G&D MUX-NT-Serie unterstützt.

Die EDID-Informationen (*Extended Display Identification Data*) eines Monitors informieren die Grafikkarte des angeschlossenen Rechners u. a. über verschiedene technische Eigenschaften des Gerätes. Die Informationen werden vom KVM-Switch üblicherweise unverändert über Enhanced-DDC (*Enhanced Display Data Channel*) an den Rechner weitergeleitet.

Alternativ kann das EDID-Profil eines Monitores eingelesen und durch den KVM-Switch an einen (oder mehrere) der angeschlossenen Rechner übermittelt werden.

HINWEIS: Ein EDID-Profil kann wahlweise direkt aus einem am KVM-Switch angeschlossenen Monitor oder aus einer bin-Datei eingelesen werden.

So lesen Sie das EDID-Profil eines angeschlossenen Monitores ein:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Klicken Sie auf **Neues EDID-Profil anlegen** im Abschnitt **Videokanal**.
6. Klicken Sie in das Listenfeld **Erlernen** und markieren Sie den Monitor, dessen EDID-Informationen Sie einlesen möchten.

   HINWEIS: Die Felder **Name** und **Kommentar** des Profils werden automatisch vorbefüllt und der Inhalt der EDID-Informationen angezeigt.

7. Klicken Sie auf **OK**.
8. Ändern Sie – falls gewünscht – die Informationen in den Feldern **Name** und/oder **Kommentar**.
9. Klicken Sie auf **Speichern**.

So lesen Sie das EDID-Profil eines Monitores aus einer Datei ein:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Klicken Sie auf **Neues EDID-Profil anlegen** im Abschnitt **Videokanal**.
6. Klicken Sie auf **Durchsuchen**.
7. Wählen Sie über den Datei-Dialog die zu importierende bin-Datei und klicken Sie auf **Öffnen**.

   HINWEIS: Die Felder **Name** und **Kommentar** des Profils werden automatisch vorbefüllt und der Inhalt der EDID-Informationen angezeigt.

8. Ändern Sie – falls gewünscht – die Informationen in den Feldern **Name** und/oder **Kommentar**.
9. Klicken Sie auf **Speichern**.

EDID-Profil eines Kanals festlegen

HINWEIS: Diese Funktion wird ausschließlich von den **DL-DVI**-Varianten der G&D MUX-NT-Serie unterstützt.

So wählen Sie das EDID-Profil aus:

TIPP: Möchten ein EDID-Profil auf *dieselben* Videokanäle der anderen Kanäle anwenden, klicken Sie auf die Schaltfläche **Alle**.

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **EDID-Profil** des Abschnitts **Videokanal** zwischen folgenden Optionen:

[Auto]:	automatische Behandlung der EDID-Daten (Standard)
Profilname:	Auswahl eines zuvor vom Anwender eingelesenen EDID-Profils

6. Klicken Sie auf **Speichern**.

Erweiterte Funktionen für KVM-Switches

Umschaltung des Kanals

Die Umschaltung auf einen der am KVM-Switch angeschlossenen Rechner kann – alternativ zu den Tastern am Gerät und den konfigurierten Select-Keys – über die Webapplikation durchgeführt werden.

Die Tastatur- und Mauseingaben sowie der Datenstrom der am KVM-Switch angeschlossenen USB-Geräte und des eingehenden Audiosignals werden nach der Umschaltung sofort an den aktiven Rechner geleitet.

So schalten Sie die Signalübertragung auf einen Rechner:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Markieren Sie auf den zu schaltenden KVM-Switch.
3. Klicken Sie auf **Schalten**.
4. Klicken Sie auf den aufzuschaltenden Kanal (z. B. **CPU_2**).

HINWEIS: Die **OK**-Markierung hinter dem Kanalnamen signalisiert den aufgeschalteten Kanal. Falls die Umschaltung nicht ausgeführt werden kann, informiert Sie ein separates Fenster über die Details.

Monitoring-Werte konfigurieren

Im Bereich *Monitoring* können Sie 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 KVM-Switches.

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 **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Monitoring**.
4. (De)aktivieren Sie die einzelen 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 eines KVM-Switches einsehen

Über das Konfigurationsmenü eines KVM-Switches können Sie eine Ansicht mit verschiedenen Statusinformationen des KVM-Switches aufrufen.

So können Sie die Statusinformationen eines KVM-Switches einsehen:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Informationen**.
4. Im jetzt erscheinenden Dialog werden Ihnen folgende Informationen angezeigt:

KVM Switch	
Name:	Name des KVM-Switches
Geräte-ID:	physikalische ID des KVM-Switches
Status:	aktueller Status (**Online** oder **Offline**) des KVM-Switches
Klasse:	Geräteklasse des KVM-Switches
Kommentar:	vom Benutzer erfasster Kommentar zum KVM-Switch

Hardware-Informationen	
Firmware name:	Bezeichnung der Firmware
Firmware rev.:	Firmware-Version
Hardware rev.:	Hardware-Revision
IP address A:	IP-Adresse der Schnittstelle *Network A*
IP address B:	IP-Adresse der Schnittstelle *Network B*
MAC A:	MAC-Adresse der Schnittstelle *Network A*
MAC B:	MAC-Adresse der Schnittstelle *Network B*
Serial number:	Seriennummer des KVM-Switches

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 konfigurert (**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

G&D. FEELS RIGHT.

Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

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

US-Büro | US-Office

G&D North America Inc.

4540 Kendrick Plaza Drive, Suite 100 | Houston, TX 77032 | USA
Phone +1-346-620-4362
sales.us@gdsys.com | www.gdsys.com