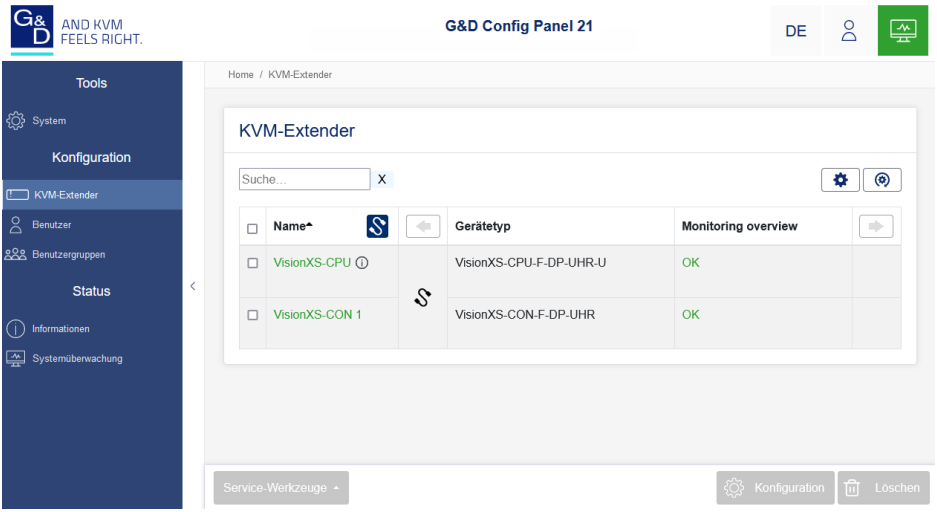
G&D VisionXS-Serie

DE Webapplikation »Config Panel«
Konfiguration des Extenders



A9100398-1.40

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 1.40 – 04.11.2024
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-Extender

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. Weiterführende Informationen finden Sie im Installationshandbuch.

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 129
- Microsoft Edge 127
- Mozilla Firefox 130

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*: **192.168.0.1**
- globale Netzwerkeinstellungen: Bezug der Einstellungen via **DHCP**

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

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

1. Verbinden Sie die Netzwerkschnittstelle eines beliebigen Rechners mit der Schnittstelle *Network* 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* auf Seite 15 f. beschrieben.
6. Entfernen Sie die Twisted-Pair-Kabelverbindung zwischen dem Rechner und dem Gerät.
7. Integrieren Sie das Gerät in das lokale Netzwerk.

Erste Schritte

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

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

Start der Webapplikation

HINWEIS: Informationen zu den Systemvoraussetzungen der Webapplikation finden Sie auf Seite 3.

So starten Sie die Webapplikation:

1. Geben in der Adresszeile folgende URL ein:

   https://[IP-Adresse des Gerätes]

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

Nutzungsbedingungen zustimmen:	Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren.
	HINWEIS: Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde (siehe *Anzeigen von Nutzungsbedingungen* ab Seite 11).
Benutzername:	Geben Sie Ihren Benutzernamen ein.
Passwort:	Geben Sie das Passwort Ihres Benutzerkontos ein.
2-Factor Auth Code (TOTP):	Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
	HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 43 ff.) und aktiviert wurde (s. Seite 57 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 61).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

3. Klicken Sie auf **Login**.

Bedienung der Webapplikation

Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus mehreren Bereichen:

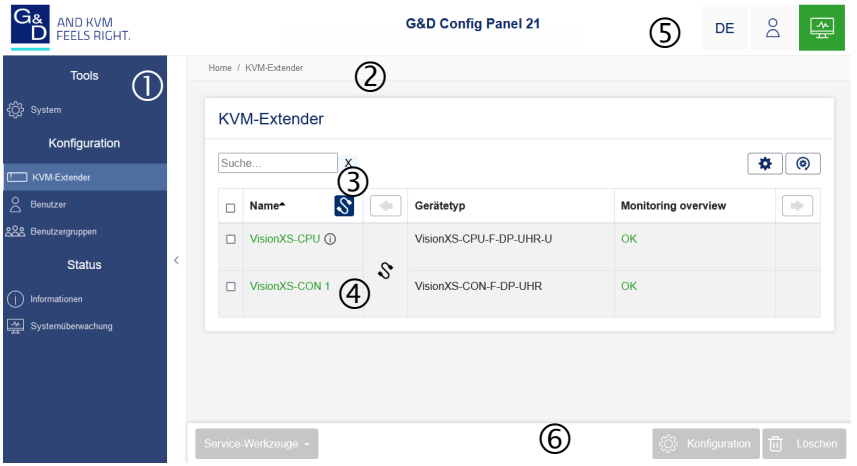


Abbildung 1: Benutzeroberfläche der Webapplikation

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

Menü ①	Im Menü sind die unterschiedlichen Funktionen der Webapplikation in Themenbereichen zusammengefasst.
Brotkrumen-Navigation ②	Die Brotkrumennavigation zeigt Ihnen den Pfad zum derzeit geöffneten Dialog an. 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-Extender** und **Benutzer** können Sie an Ihre Bedürfnisse anpassen.

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

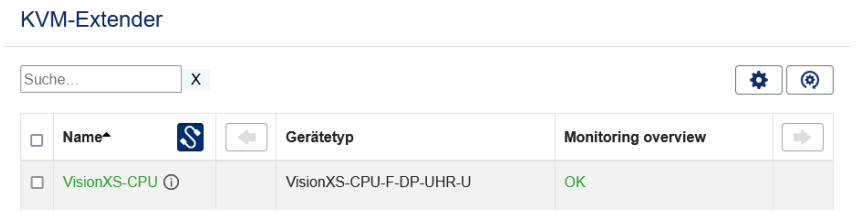


Abbildung 2: Tabellenspalten (Auswahl) eines KVM-Extenders

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. Bei Bedarf können Sie jedem Benutzerkonto eine (abweichende) Sprache fest zuordnen.

HINWEIS: Alle Spracheinstellungen gelten sowohl für die Webapplikation als auch für das On-Screen-Display (OSD) des Gerätes.

Falls das OSD die ausgewählte Sprache *nicht* unterstützt, wird das OSD in Englisch angezeigt.

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**.

Sprache für ein bestimmtes Benutzerkonto auswählen

So stellen Sie die Sprache eines *bestimmten* Benutzerkontos ein:

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 **KVM-Extender-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Sprache** zwischen folgenden Optionen:

System:	Verwendung der Systemsprache (s. oben).
[Auswahl]	Verwendung der ausgewählten Sprache

5. 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 61) und Anlage eines neuen Benutzerkontos (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 56) 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.

Grundkonfiguration der Webapplikation

Netzwerkeinstellungen

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

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

Konfiguration der Netzwerkschnittstelle

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

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

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

So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:

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

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

5. Erfassen Sie im Abschnitt **Schnittstelle A** folgende Daten:

Betriebsmodus:	Wählen Sie den Betriebsmodus der **Schnittstelle A** aus: ▪ **Aus:** Netzwerkschnittstelle ausschalten. ▪ **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. 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-Extender**.
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**.

Status der Netzwerkschnittstelle auslesen

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

So ermitteln Sie den Status der Netzwerkschnittstelle:

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

Link detected:	Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**).
	HINWEIS: Die folgenden Informationen werden nur bei CAT-Varianten angezeigt.
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-Extender**.
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:

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-Extender**.
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.

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-Extender**.
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-Extender**.
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 23 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 24) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 28) 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 24) 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-Extender**.
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 23 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-Extender**.
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.

Firmware-Update mehrerer Geräte des KVM-Systems

So aktualisieren Sie die Firmware mehrerer Geräte des KVM-Systems:

1. Klicken Sie im Menü auf **System**.
2. Klicken Sie auf **System-Update**.
3. Markieren Sie die Geräte, deren Firmware Sie aktualisieren möchten und klicken Sie auf **Firmware-Update**.

   HINWEIS: Bei Geräten, für die ein Firmware-Update aktuell nicht möglich ist, wird der Grund hierfür im Feld **Status** angezeigt.

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**.

HINWEIS: Um bei größeren Datenmengen die Übertragung der Updates zu den Endgeräten zu gewährleisten, werden die Endgeräte bei Bedarf nacheinander in Gruppen aktualisiert.

WICHTIG: Schließen Sie **nicht** die Browser-Session, während die Geräte aktualisiert werden! Schalten Sie die Produkte während dem Update **nicht** aus, und trennen Sie sie **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-Extender**.
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 jedes dieser Geräte innerhalb des KVM-Systems 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
- Überwachung und Steuerung von Computern und Netzwerkgeräten über das *Simple Network Management Protocol* (s. Seite 48 ff.)

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-Extender**.
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-Extender**.
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-Extender**.
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-Extender**.
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-Extender**.
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 43) 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-Extender**.
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 56).

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 43) 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 57).

So aktivieren Sie die 2FA am Gerät:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Gerät (**CPU** bzw. **CON**).
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 56).

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 34). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 36).

Informationen zur Aktivierung der Zwei-Faktor-Authentifizierung finden Sie auf Seite 57 ff.

Monitoring-Funktionen

In den Themenbereichen **KVM-Extender** 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:

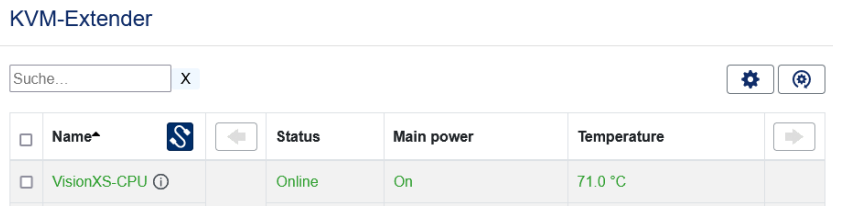


Abbildung 4: Detailansicht einer exemplarischen Monitoring-Tabelle

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

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

Alle Monitoring-Werte einsehen

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

So öffnen Sie die Liste aller Monitoring-Werte:

1. Klicken Sie im Menü auf **KVM-Extender**.
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 und es werden *keine* SNMP-Traps hierzu versendet!

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

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

Erweiterte Funktionen zur Verwaltung der kritischen Geräte

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

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

Auflistung der kritischen Monitoring-Werte einsehen

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

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

Alarm eines kritischen Gerätes bestätigen

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

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

So bestätigen Sie die Monitoring-Meldungen eines Gerätes:

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

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-Extender**.
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-Extender**.
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-Extender**.
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**.

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
Persönliches Profil ändern	Nein	Ja	**Ja**	**Ja**
Gerätekonfiguration	Nein	**Ja**	Nein	**Ja**
Zugriff auf USB-Geräte	**Ja**	Nein	Nein	**Ja**

Das Effektivrecht der Rechte *Persönliches Profil ändern* und *Gerätekonfiguration* resultieren aus den Rechten der Benutzergruppen. Das Recht *Zugriff auf USB-Geräte* wurde hingegen direkt im Benutzerkonto vergeben. 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 (Tastenkombinationen, Sprachauswahl, …) 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 zur *Gerätekonfiguration* erhalten, bieten sich folgende Möglichkeiten an, dies mit Benutzergruppen zu realisieren:

- Sie erstellen eine Benutzergruppe (z. B. *Office_Gerätekonfiguration*), mit den identischen Einstellungen der Gruppe *Office*. Das Recht *Gerätekonfiguration* wird abschließend *aktiviert*. Ordnen Sie dieser Gruppe die entsprechenden Benutzerkonten zu.
- Sie erstellen eine Benutzergruppe (z. B. *Gerätekonfiguration*) und setzen ausschließlich das Recht *Gerätekonfiguration* 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 die *Gerätekonfiguration*.

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 12).

So erstellen Sie ein neues Benutzerkonto:

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

Name:	Geben Sie den gewünschten Benutzernamen ein. **HINWEIS:** Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Benutzerauthentifizierung mit Verzeichnisdiensten* ab Seite 40).
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 43), sind im Folgenden die Einstellungen für das Benutzerkonto vorzunehmen (s. Seite 57).

Aktivierung der Zwei-Faktor-Authentifizierung

HINWEIS: Für die Verwendung der Zwei-Faktor-Authentifizierung (2FA) muss zunächst die Einrichtung am Gerät erfolgen (s. Seite 43).

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 43), 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 68), oder der Anwender muss mit dem entsprechenden Benutzerprofil angemeldet sein (s. Seite 68) und über das Recht *Eigenes Passwort ändern* (s. Seite 69) verfügen.

WICHTIG: Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 34). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 36).

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 62).

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 64).

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 40).

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 68)
oder das Recht *Eigenes Passwort ändern*
(siehe *Berechtigung zur Änderung des eigenen Passworts* ab Seite 69).

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

So ändern Sie das Passwort eines Benutzerkontos:

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

Aktuelles Passwort:	Geben Sie das bisherige Passwort ein. **HINWEIS:** Bei Benutzern mit aktiviertem Superuser-Recht (s. Seite 68 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 43 ff.) und aktiviert wurde (s. Seite 57 ff.).

4. Klicken Sie auf **Speichern**.

Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

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

System-Rechte

Bezeichnung	Berechtigung	Seite
Superuser-Recht	Zugriff auf die Konfiguration des Systems uneingeschränkt möglich	Seite 68
Config Panel Login	Login mit der Webapplikation *ConfigPanel*	Seite 68
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 69
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 69

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 listet 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 68
Config Panel Login	Login mit der Webapplikation *ConfigPanel*	Seite 68
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 69
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 69

Mitgliederverwaltung einer Benutzergruppe

So verwalten Sie die Mitglieder einer Benutzergruppe:

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

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

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

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

6. Klicken Sie auf **Speichern**.

Aktivierung oder Deaktivierung einer Benutzergruppe

So aktivieren oder deaktivieren Sie eine Benutzergruppe:

1. Klicken Sie im Menü auf **Benutzergruppen**.
2. Klicken Sie auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Aktivieren Sie die Benutzergruppe mit dem Schieberegler **Aktiviert**.

   Möchten Sie den Mitgliedern der Benutzergruppe den Zugang zum KVM-System sperren, so deaktivieren Sie das Kontrollkästchen.

4. Klicken Sie auf **Speichern**.

Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe:

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

System-Rechte

Berechtigung zum uneingeschränkten Zugriff (Superuser)

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

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

So ändern Sie die Berechtigung zum uneingeschränkten Zugriff:

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

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

5. Klicken Sie auf **Speichern**.

Berechtigung zum Login in die Webapplikation

So ändern Sie die Berechtigung zum Login mit der Webapplikation:

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

Aktiviert:	Zugriff auf die Webapplikation erlaubt
Deaktiviert:	Zugriff auf die Webapplikation untersagt

5. Klicken Sie auf **Speichern**.

Berechtigung zur Änderung des eigenen Passworts

So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:

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

Aktiviert:	Passwortänderung des eigenen Benutzerkontos erlaubt
Deaktiviert:	Passwortänderung des eigenen Benutzerkontos untersagt

5. Klicken Sie auf **Speichern**.

Berechtigung zur Bestätigung eines Monitoring-Alarms

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

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

Aktiviert:	Bestätigung von Monitoring-Alarmen erlaubt
Deaktiviert:	Bestätigung von Monitoring-Alarmen untersagt

5. Klicken Sie auf **Speichern**.

Erweiterte Funktionen des KVM-Systems

Identifizierung eines Gerätes durch Aktivierung der Identification-LED

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

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

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

1. Klicken Sie im Menü auf **KVM-Extender**.
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 KVM-Systems:

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 37).

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 KVM-Systems wieder her:

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

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

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

7. Klicken Sie auf **Restore**.

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

Freischaltung kostenpflichtiger Zusatzfunktionen

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

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

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

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

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

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

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features** sowie die Verwendung eines zusätzlichen **SFP-Transceivers** (bei den Fiber-Varianten) sind Voraussetzung für die Verbindung und Verwendung eines zweiten Arbeitsplatzmoduls (**CON-Trans 2**).

Grundkonfiguration der KVM-Extender

Änderung des Namens eines KVM-Extender

So ändern Sie den Namen eines KVM-Extender:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Modul (**CPU**, **CON-Trans 1** bzw. **CON-Trans 2**).
3. Geben Sie im Feld **Name** des Abschnitts **Gerät** den gewünschten Namen des KVM-Extenders ein.
4. Klicken Sie auf **Speichern**.

Änderung des Kommentares eines KVM-Extenders

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

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

So ändern Sie den Kommentar eines KVM-Extenders:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Modul (**CPU**, **CON-Trans 1** bzw. **CON-Trans 2**).
3. Geben Sie im Feld **Kommentar** des Abschnitts **Gerät** einen beliebigen Kommentar ein.
4. Klicken Sie auf **Speichern**.

Einen KVM-Extender aus dem KVM-System löschen

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

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

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

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

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu löschenden KVM-Extender 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-Extender

Gerätekonfiguration

Betriebsarten des KVM-Extenders

Je nach Einsatzzweck des KVM-Extenders kann die Betriebsart aus den folgenden Optionen gewählt werden:

- **Open Access-Betriebsart:** Der Zugang zum KVM-Extender ist in dieser Betriebsart *nicht* durch eine Authentifizierung geschützt.

HINWEIS: Diese Betriebsart ist im **Extenderbetrieb** *standardmäßig* eingestellt.

TIPP: Die Benutzerkonten der Open-Access-Arbeitsplätze werden mit einem *OAC*-Symbol gekennzeichnet.

Die Farbe des Symbols signalisiert, ob der korrespondierende Arbeitsplatz derzeit im *Open-Access*-Modus (**grün**) oder nicht im *Open-Access*-Modus (**grau**) betrieben wird (das Arbeitsplatzmodul wurde in die *Standard*-Betriebsart versetzt).

Für den KVM-Extender können Sie die gleichen Zugriffsrechte konfigurieren, wie sie auch für ein Benutzerkonto eingerichtet werden können.

WICHTIG: Die konfigurierten Zugriffsrechte gelten für alle Benutzer an diesem KVM-Extender.

- **Standard-Betriebsart:** Die Standard-Betriebsart erlaubt den Zugang zum KVM-Extender erst nach der Authentifizierung des Benutzers mit seinem Benutzernamen, seinem Passwort und, falls die Zwei-Faktor-Authentifizierung verwendet wird (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät* auf Seite 43), mit einem zusätzlichen Einmal-Passwort.

HINWEIS: Diese Betriebsart ist bei Verwendung des Extenders als **Matrixswitch-Modul** *standardmäßig* eingestellt.

Die Rechte des Benutzers können über die Einstellungen der Benutzerkonten indiviuell eingestellt werden.

So wählen Sie die Betriebsart des KVM-Extenders:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
3. Wählen Sie im Feld **Betriebsmodus** zwischen folgenden Optionen:

Open Access Console:	Open Access-Betriebsart (*Standard* im Extenderbetrieb)
Standard:	Standard-Betriebsart

4. Klicken Sie auf **OK**, um die erfassten Daten zu speichern.

Änderung der Hotkey-Modifizierertaste

Der Hotkey zum OSD-Aufruf besteht aus mindestens einer Hotkey-Modifizierertaste und einer zusätzlichen OSD-Taste, die vom Anwender innerhalb eines vorgegebenen Rahmens frei gewählt werden kann.

> **HINWEIS:** In der Standardeinstellung ist die Hotkey-Modifizierertaste **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-Modifizierertaste können Sie eine Taste oder eine Kombination aus den Tasten *Strg*, *Alt*, *Alt Gr*, *Win* oder *Shift* wählen.

So ändern Sie die Hotkey-Modifizierertaste:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. 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 Modifizierertasten ausgewählt, so sind diese gemeinsam zu betätigen, um den Hotkey auszulösen!

4. Klicken Sie auf **Speichern**.

Änderung der OSD-Taste

Der Hotkey zum OSD-Aufruf besteht aus mindestens einer Hotkey-Modifiziererertaste und einer zusätzlichen OSD-Taste, die vom Anwender innerhalb eines vorgegebenen Rahmens frei gewählt werden kann.

Sowohl die Hotkey-Modifiziererertaste **Strg** als auch die OSD-Taste **Num** können von Ihnen verändert werden.

So ändern Sie die OSD-Taste:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **Hotkey** die OSD-Taste aus, welche gemeinsam mit der bzw. den Hotkey-Modifiziererertaste(n) den Aufruf des On-Screen-Displays bewirkt.

   Zur Auswahl stehen die Tasten *Num, Pause*, *Einfg*, *Entf*, *Pos 1*, *Ende, Bild auf*, *Bild ab*, und *Leertaste*.
4. Klicken Sie auf **Speichern**.

OSD mit doppeltem Tastendruck starten

Alternativ zum Öffnen des OSD mit der Tastenkombination **Hotkey+Num** bzw. **Doppel-Hotkey+Num** können Sie das OSD durch die zweifache, aufeinanderfolgende Betätigung einer konfigurierten Taste öffnen.

So (de)aktivieren Sie die Aktivierung des OSD mit doppeltem Tastendruck:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **OSD via doppeltem Tastendruck** die gewünschte Taste aus.

Aus:	OSD-Aufruf mit doppeltem Tastendruck deaktiviert (*Standard*)
Strg:	OSD-Aufruf mit doppeltem Druck auf die *Strg*-Taste
Alt:	OSD-Aufruf mit doppeltem Druck auf die *Alt*-Taste
Alt Gr:	OSD-Aufruf mit doppeltem Druck auf die *Alt Gr*-Taste
Win:	OSD-Aufruf mit doppeltem Druck auf die *Windows*-Taste
Shift:	OSD-Aufruf mit doppeltem Druck auf die *Umschalt*-Taste
Druck:	OSD-Aufruf mit doppeltem Druck auf die *Druck*-Taste
Pfeil links:	OSD-Aufruf mit doppeltem Druck auf die *Pfeil links*-Taste
Pfeil rechts:	OSD-Aufruf mit doppeltem Druck auf die *Pfeil rechts*-Taste
Pfeil unten:	OSD-Aufruf mit doppeltem Druck auf die *Pfeil unten*-Taste
Pfeil oben:	OSD-Aufruf mit doppeltem Druck auf die *Pfeil oben*-Taste

4. Klicken Sie auf **Speichern**.

USB-Tastaturmodus oder »Generic USB« (de)aktivieren

Der KVM-Extender unterstützt verschiedene USB-Eingabegeräte. Die besonderen Eigenschaften eines bestimmten USB-Eingabegerätes können Sie nach Auswahl des spezifischen USB-Tastaturmodus nutzen.

Alternativ zu dem spezifischen USB-Tastaturmodus können Sie den **Generic-USB**-Modus nutzen. In diesem Modus werden die Daten des USB-Gerätes unverändert an das Rechnermodul übertragen.

WICHTIG: Der **Generic-USB**-Modus unterstützt USB-Massenspeichergeräte sowie viele der am Markt erhältlichen USB-Geräte (beispielsweise auch FIDO-Sicherheitsschlüssel und diverse SmartCard-Reader). Der Betrieb eines bestimmten USB-Gerätes im Generic-USB-Modus kann nicht gewährleistet werden.

WICHTIG: Bei Anschluss eines USB-Hubs oder USB-Verbundgerätes mit mehreren USB-Geräten kann nur das erste der angeschlossenen HID-Geräte im **Generic-USB**-Modus verwendet werden.

▪ **USB-Tastaturen:** Im voreingestellten USB-Tastaturmodus **Multimedia** werden die Tasten des Standard-Tastaturlayouts unterstützt.

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

Die folgende Tabelle listet die unterstützten USB-Tastaturen auf:

EINGABEGERÄT	EINSTELLUNG
PC-Tastatur mit Standard-Tastaturlayout	‣ PC Standard
PC-Tastatur mit zusätzlichen Multimedia-Tasten	‣ Multimedia
Apple Keyboard mit Ziffernblock (A1243)	‣ Apple A1243

▪ **Displays und Tablets:** Sie können den am KVM-Extender angeschlossenen Rechner mit einem der unterstützten *Displays* oder *Tablets* bedienen:

EINGABEGERÄT	EINSTELLUNG
Wacom Intuos5 S	‣ Wacom Intuos 5 S
Wacom Intuos5 M	‣ Wacom Intuos 5 M
Wacom Intuos5 L	‣ Wacom Intuos 5 L
Wacom Intuos Pro L	‣ Wacom Intuos Pro L
Wacom Cintiq Pro 24 Pen	‣ Wacom Cintiq Pro 24 Pen
Wacom Cintiq Pro 27	‣ Wacom Cintiq Pro 27
Wacom Cintiq Pro 32 Pen	‣ Wacom Cintiq Pro 32 Pen
Wacom Cintiq Pro 32 Touch	‣ Wacom Cintiq Pro 32 Touch
iiyama TF2415	‣ iiyama TF2415

▪ **Generic-USB-Modus:** In diesem Modus werden die Daten des USB-Gerätes unverändert an das Rechnermodul übertragen.

EINGABEGERÄT	EINSTELLUNG
beliebiger USB-Massenspeicher oder beliebiges USB-Eingabegerät	‣ Generic USB

WICHTIG: Der **Generic-USB**-Modus unterstützt viele der am Markt erhältlichen USB-Massenspeichergeräte und -Eingabegeräte. Der Betrieb eines bestimmten Gerätes im Generic-USB-Modus kann *nicht* gewährleistet werden.

▪ **LK463-kompatible Tastatur:** An das Arbeitsplatzmodul können Sie eine LK463-kompatible Tastatur anschließen. Die Anordnung der 108 Tasten solcher Tastaturen entspricht dem OpenVMS-Tastaturlayout.

Ein spezieller USB-Tastaturmodus gewährleistet die Übermittlung der Betätigung einer Sondertaste dieser Tastatur an den Zielrechner:

EINGABEGERÄT	EINSTELLUNG
LK463-kompatible Tastatur	‣ LK463

So wählen Sie einen USB-HID-Modus:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **USB-HID-Mode** die gewünschte Option (s. oben).
4. Klicken Sie auf **Speichern**.

TIPP: Sie haben die Möglichkeit, ein USB-Gerät zu bestimmen, das nach einem Neustart priorisiert werden soll und auf jeden Fall wieder im Zugriff sein soll. Die Priorisierung können Sie nur über das On-Screen-Display konfigurieren.

Weiterführende Informationen zu dieser Möglichkeiten finden Sie im Installationshandbuch des Geräts.

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-Extender 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-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
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-Extender aus und wieder ein.

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

Tastaturlayout für Eingaben innerhalb des OSD auswählen

Werden bei der Eingabe von Zeichen auf der Tastatur des Arbeitsplatzes andere Zeichen im OSD angezeigt, ist das eingestellte Tastaturlayout der Tastatur nicht zutreffend.

Stellen Sie in diesem Fall fest, welchem Tastaturlayout die angeschlossene Tastatur entspricht und konfigurieren Sie dieses anschließend in den Einstellungen des Arbeitsplatzmoduls.

So wählen Sie das Tastaturlayout der Tastatur des Arbeitsplatzmoduls aus:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
3. Wählen Sie im Feld **Tastaturlayout** zwischen folgenden Optionen:

Deutsch (*Standard*)
Englisch (USA)
Englisch (Großbritannien)
Französisch
Spanisch
Lat. Amerikanisch
Portugiesisch
Schwedisch
Schweiz-Französisch
Dänisch

4. Klicken Sie auf **Speichern**.

Reinitialisierung von USB-Eingabegeräten

Sobald Sie eine USB-Tastatur bzw. -Maus an den KVM-Extender 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-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
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**.

Wartezeit des Bildschirmschoners einstellen

Der Bildschirmschoner schaltet nach einer von Ihnen einstellbaren Zeit der Inaktivität des Benutzers die Bildschirmanzeige am Arbeitsplatz ab.

HINWEIS: Diese Einstellung ist unabhängig von den Bildschirmschoner-Einstellungen des am Rechnermodul angeschlossenen Rechners.

So stellen Sie die Wartezeit des Bildschirmschoners ein:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
3. Geben Sie in der Zeile **Bildschirmschoner (Minuten)** die Wartezeit (1 bis 999 Minuten) des Bildschirmschoners ein.

   HINWEIS: Der Wert **0** deaktiviert den Bildschirmschoner.

4. Klicken Sie auf **Speichern**.

Betriebsmodus der RS232-Schnittstelle einstellen

In der Standardeinstellung des Extenders können Sie jedes **RS232**-kompatible Gerät an die *optionale* RS232-Schnittstelle des Arbeitsplatzmoduls anschließen. Der RS232-Datenstrom wird unverändert zum Rechnermodul übertragen.

Für die *alternative* Übertragung von **RS422**-Signalen können Sie zwei **G&D RS232-422-Adapter** verwenden. Je ein Adapter wandelt die RS232-Schnittstelle des Arbeitsplatz- sowie des Rechnermoduls in RS422-Schnittstellen um.

WICHTIG: Für die Übertragung der **RS422**-Signale ist neben der Verwendung der Adapter die Umstellung des Betriebsmodus der *RS232*-Schnittstellen des Arbeitsplatz- *und* des Rechnermoduls erforderlich.

So stellen Sie den Betriebsmodus der RS232-Schnittstelle ein:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Modul (**CPU**, **CON-Trans 1, CON-Trans 2**).
3. Wählen Sie im Feld **Serielle Kommunikation** des Abschnitts **Konfiguration** eine der folgenden Optionen:

RS232:	Der Datenstrom eines RS232-Gerätes wird vom Rechnermodul zum Arbeitsplatzmodul übertragen (*Standard*).
RS422:	Der Datenstrom eines RS422-Gerätes wird über die separat erhältlichen **G&D RS232-422-Adapter** vom Rechnermodul zum Arbeitsplatzmodul übertragen.

4. Klicken Sie auf **Speichern**.

Berechtigung für exklusiven Zugriff des Arbeitsplatzes

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

Erfolgt innerhalb der eingestellten Zeitspanne der automatischen Eingabesperre (*Standard*: 1 Sekunde) keine Eingabe am aktiven Arbeitsplatz, erlaubt der KVM-Extender in der Standardeinstellung auch dem anderen Arbeitsplatz die Bedienung des Extenders.

Wird die Berechtigung für exklusiven Zugriff des Arbeitsplatzes in der Webapplikation eingeschaltet, können Anwender an einem solchen Arbeitsplatz mit der Tastenkombination **Hotkey+Druck** (*Standard*: **Strg+Druck**) die exklusive Bedienung des KVM-Extenders erreichen.

Nach Betätigung dieser Tastenkombination werden die Eingabegeräte des konkurrierenden Arbeitsplatzes deaktiviert.

WICHTIG: Eingaben an Geräten, die an der **Generic-Schnittstelle** des konkurrierenden Arbeitsplatzes angeschlossen sind, sind weiterhin möglich.

Durch erneutes Ausführen der Tastenkombination am aktiven Arbeitsplatz, wird die Bedienung des KVM-Extenders wieder für beide Arbeitsplätze freigeschaltet.

HINWEIS: Nach Aktivierung der exklusiven Bedienung des KVM-Extenders an einem Arbeitsplatz blinken an der Tastatur des gesperrten Arbeitsplatzes abwechselnd die *Caps Lock*- und die *Num*- sowie *Scroll Lock*-LEDs.

Die exklusive Bedienung des KVM-Extenders wird am aktiven Arbeitsplatz durch das Blinken der *Scroll Lock*-LED angezeigt.

So wählen Sie die Berechtigung für exklusiven Zugriff eines Arbeitsplatzes:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
3. Wählen Sie im Feld **Permanent-Access-Modus** zwischen folgenden Optionen:

Aktiviert:	Berechtigung für exklusiven Zugriff erteilt (*Standard*)
Deaktiviert:	Berechtigung für exklusiven Zugriff verweigert

4. Klicken Sie auf **Speichern**.

Änderung der Videobetriebsart der Arbeitsplätze

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

In der Standardkonfiguration des KVM-Extenders wird das Bild des Rechners sowohl am Monitor des aktiven als auch am Monitor des konkurrierenden Arbeitsplatzes ausgegeben.

Alternativ können Sie festlegen, dass das Bild des anderen Arbeitsplatzes *temporär* oder *permanent* ausgeschaltet wird, sobald eine Eingabe an einem Arbeitsplatz erfolgt.

WICHTIG: Eine Eingabe an Geräten, die an der **Generic-Schnittstelle** angeschlossen sind, löst **keine** Ausschaltung des Bildes am konkurrierenden Arbeitsplatz aus.

So wählen Sie die Videobetriebsart eines Arbeitsplatzes:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Arbeitsplatzmodul (**CON-Trans 1** bzw. **CON-Trans 2**).
3. Wählen Sie im Feld **Bildanzeige** zwischen folgenden Optionen:

Immer an:	Das Bild des Rechners wird sowohl am Monitor des aktiven als auch am Monitor des konkurrierenden Arbeitsplatzes ausgegeben (*Standard*).
Permanent aus:	Das Bild *dieses Arbeitsplatzes* wird *permanent* ausgeschaltet, sobald eine Eingabe am konkurrierenden Arbeitsplatz erfolgt. Nach Ablauf der *Zeitspanne der Eingabesperre* ist eine Eingabe an diesem Arbeitsplatz erforderlich, um das Bild wieder einzuschalten.
Temporär aus:	Das Bild *dieses Arbeitsplatzes* wird *temporär* ausgeschaltet, sobald eine Eingabe am konkurrierenden Arbeitsplatz erfolgt. Nach Ablauf der *Zeitspanne der Eingabesperre* wird das Bild *automatisch* wieder eingeschaltet.

4. Klicken Sie auf **Speichern**.

Änderung der Zeitspanne der Eingabesperre

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

Wird an einem Arbeitsplatz eine Eingabe per Tastatur oder Maus durchgeführt, sperrt der KVM-Extender automatisch die Eingabegeräte des konkurrierenden Arbeitsplatzes.

WICHTIG: Eine Eingabe an Geräten, die an der **Generic-Schnittstelle** angeschlossen sind, löst **keine** Sperrung der Eingabegeräte des konkurrierenden Arbeitsplatzes aus.

WICHTIG: Eingaben an Geräten, die an der **Generic-Schnittstelle** des konkurrierenden Arbeitsplatzes angeschlossen sind, sind weiterhin möglich.

Die Sperre wird aufgehoben, wenn innerhalb der eingestellten Zeitspanne der Eingabesperre (*Standard*: 1 Sekunde) keine weitere Eingabe am aktiven Arbeitsplatz erfolgt.

Nach Ablauf der Zeitspanne der Eingabesperre ist die Bedienung des Rechners wieder an beiden Arbeitsplätzen freigeschaltet.

Die Zeitspanne der Eingabesperre kann durch den Anwender innerhalb des Bereichs von 1 bis 90 Sekunden eingestellt werden.

So ändern Sie die Zeitspanne der Eingabesperre:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Geben Sie im Feld **Multiuser-Eingabesperre (Sekunden)** die gewünschte Zeitspanne der Eingabesperre (1 bis 90 Sekunden) ein.
4. Klicken Sie auf **Speichern**.

Arbeitsplatzaktivierung nach permanenter Ausschaltung der Bildanzeige

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

Bei Auswahl der **Bildanzeige**-Option **Permanent aus** wird das Bild nach Ablauf der *Zeitspanne der Eingabesperre* erst nach einer Benutzereingabe wieder eingeschaltet.

In der Standardeinstellung bewirken sowohl Tastatur- als auch Mauseingaben die Bildeinschaltung. Alternativ können Sie *nur Tastatur-* oder *nur Mauseingaben* als Auslöser für die Bildeinschaltung zulassen.

WICHTIG: Eine Eingabe an Geräten, die an der **Generic-Schnittstelle** angeschlossen sind, löst **keine** Bildeinschaltung aus.

So wählen Sie das/die zulässige(n) Eingabegerät(e) für das Auslösen der Bildeinschaltung:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **Arbeitsplatz-Aktivierung via** zwischen folgenden Optionen:

Tastatur/Maus (*Standard*)
Nur Tastatur
Nur Maus

4. Klicken Sie auf **Speichern**.

Aktiver Arbeitsplatz nach Start des Extender

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

Bei Auswahl der **Bildanzeige**-Option **Permanent aus** zeigen *beide* Arbeitsplatzmodule nach einem Neustart des Extenders kein Bild an. Erst nach einer Eingabe an einem Arbeitsplatz, wird dessen Bild auf dem Monitor angezeigt.

WICHTIG: Eine Eingabe an Geräten, die an der **Generic-Schnittstelle** angeschlossen sind, löst **keine** Bildeinschaltung aus.

Mit der Einstellung **Aktiver Arbeitsplatz nach Start** können Sie alternativ ein Modul festlegen, dessen Bildanzeige *sofort* nach dem Start des Extenders aktiviert wird.

So wählen Sie, ob und auf welchem Modul die Bildanzeige nach dem Extender-Neustart aktiviert wird:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **Aktiver Arbeitsplatz nach Start** zwischen folgenden Optionen:

Kein:	Beide Arbeitsplatzmodule zeigen nach dem Start zunächst kein Bild (*Standard*).
CON (Trans. 1):	Das Arbeitsplatzmodul an *Transmission 1* zeigt nach dem Start sofort ein Bild an.
CON (Trans. 2):	Das Arbeitsplatzmodul an *Transmission 2* zeigt nach dem Start sofort ein Bild an.

4. Klicken Sie auf **Speichern**.

Änderung der Exklusivmodus-Aktionstaste

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy-Features**, die Verwendung eines zusätzlichen **SFP-Transceivers** (bei Fiber-Varianten) sowie die Verbindung mit einem zweiten Arbeitsplatzmodul sind Voraussetzung für diese Bedienmöglichkeit.

Nach Betätigung der Tastenkombination für die exklusive Bedienung des Extenders sind die Eingabegeräte des konkurrierenden Arbeitsplatzes deaktiviert.

WICHTIG: Eingaben an Geräten, die an der **Generic-Schnittstelle** des konkurrierenden Arbeitsplatzes angeschlossen sind, sind weiterhin möglich.

Erst durch erneute Betätigung der Tastenkombination am aktiven Arbeitsplatz, wird die Bedienung des KVM-Extenders wieder für beide Arbeitsplätze freigeschaltet.

Die Tastenkombination für die exklusive Bedienung besteht aus mindestens einer Hotkey-Modifizierertaste (siehe *Änderung der OSD-Taste* auf Seite 80) und einer zusätzlichen *Exklusiv*-Taste, die vom Anwender innerhalb eines vorgegebenen Rahmens frei gewählt werden kann. Sowohl die Hotkey-Modifizierertaste **Strg** als auch die Exklusiv-Taste **Druck** können von Ihnen verändert werden.

So ändern Sie die Exklusiv-Taste:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Wählen Sie im Feld **Exklusivmodus-Aktionstaste** die gewünschte Taste aus.

   Zur Auswahl stehen die Tasten *Druck*, *Rollen*, *Num*, *Pause*, *Einf.*, *Entf.*, *Pos 1*, *Ende*, *Bild auf*, *Bild ab, Leertaste* und *Backspace.*
4. Klicken Sie auf **Speichern**.

Videokanal-Konfiguration

EDID-Profil eines Monitores einlesen

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-Extender 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-Extender an einen (oder mehrere) der angeschlossenen Rechner übermittelt werden.

HINWEIS: Ein EDID-Profil kann wahlweise direkt aus einem am KVM-Extender 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-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Klicken Sie auf **Neues EDID-Profil anlegen**.
5. 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.

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

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

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Klicken Sie auf **Neues EDID-Profil anlegen**.
5. Klicken Sie auf **Datei auswählen**.
6. 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.

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

EDID-Profil eines Monitores exportieren

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Wählen Sie das zu exportierende **EDID-Profil**.
5. Klicken Sie auf **EDID exportieren**.
6. Ändern Sie ggf. im Datei-Dialog den Namen der zu exportierenden bin-Datei.
7. Klicken Sie auf **Speichern**.

EDID-Profil eines Kanals festlegen

So wählen Sie das EDID-Profil aus:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. 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

5. Klicken Sie auf **Speichern**.

Reduzierung der Farbtiefe der zu übertragenden Bilddaten

In der Standardeinstellung des KVM-Extenders werden die Bildinformationen mit einer maximalen Farbtiefe von 24 bit an das Arbeitsplatzmodul übertragen.

Bei Verwendung einer hohen Bildauflösung und Darstellung von Bewegtbildern kann es in Ausnahmefällen vorkommen, dass einige Bilder am Arbeitsplatzmodul „übersprungen“ werden.

Reduzieren Sie in einem solchen Fall die zu übertragende Farbtiefe der Bilddaten auf 18 bit. Hierdurch kann die zu übertragende Datenmenge reduziert werden.

HINWEIS: Abhängig vom Bildinhalt können gegebenenfalls leichte Farbstufen bei Reduzierung der Farbtiefe erkennbar werden.

So ändern Sie die Farbtiefe der zu übertragenden Bilddaten:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Wählen Sie im Feld **Farbtiefe** zwischen folgenden Optionen:

24 Bit:	Übertragung der Bilddaten mit einer maximalen Farbtiefe von 24 Bit (*Standard*).
18 Bit:	Reduzierung der Farbtiefe der Bilddaten auf 18 bit.

5. Klicken Sie auf **Speichern**.

DDC/CI-Unterstützung (de)aktivieren

Die vom KVM-Extender unterstützten Rechner- und Arbeitsplatzmodule wurden vorbereitet, um Monitore mit **DDC/CI**-Funktion zu unterstützen.

Die **DDC/CI**-Informationen werden nach Aktivierung der Funktion *transparent* an den Monitor weitergeleitet, um eine größtmögliche Anzahl an Monitoren zu unterstützen. Die Unterstützung kann jedoch *nicht* für alle Monitor-Modelle garantiert werden.

So konfigurieren Sie die DDC/CI-Unterstützung eines Arbeitsplatzmoduls:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**. Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Wählen Sie im Feld **DDC/CI Monitor** zwischen folgenden Optionen:

Deaktiviert:	Die Übertragung von DDC/CI-Signalen ist deaktiviert (Standard).
Rechner > Monitor:	Die Übertragung von DDC/CI-Signalen erfolgt ausschließlich vom Rechner in Richtung des Monitors.
Bidirektional:	Die Übertragung von DDC/CI-Signalen erfolgt bidirektional.

5. Klicken Sie auf **Speichern**.

Verwendung des Freeze-Modus

Wird die Kabelverbindung zwischen dem Rechner- und dem Arbeitsplatzmodul im laufenden Betrieb unterbrochen, wird in der Standardeinstellung des KVM-Extenders kein Bild auf dem Monitor des entfernten Arbeitsplatzes dargestellt.

Aktivieren Sie den *Freeze*-Modus, wenn Sie im Falle eines Verbindungsabbruchs das zuletzt am Arbeitsplatzmodul empfangene Bild darstellen möchten bis die Verbindung wiederhergestellt ist.

Um den Verbindungsabbruch deutlich zu signalisieren, wird das zuletzt empfangene Bild wahlweise mit einem farbigen Rahmen und/oder der Einblendung **Frozen** und der vergangenen Zeit seit dem Verbindungsabbruch dargestellt.

So konfigurieren Sie den Freeze-Modus:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Doppelklicken Sie auf das zu konfigurierende Rechnermodul (**CPU**).
3. Klicken Sie auf den Reiter **Videokanäle**.
   Klicken Sie bei Einsatz einer *DH-Variante* zunächst auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
4. Wählen Sie im Feld **Freeze-Modus** zwischen folgenden Optionen:

Aus:	Kein Bild bei Verbindungsabbruch anzeigen (*Standard*).
An | OSD-Timer + Rahmen:	Anzeige eines farbigen Rahmens bei Verbindungsabbruch sowie Einblendung des Hinweises *Frozen* und der vergangenen Zeit seit dem Verbindungsabbruch.
An | Rahmen:	Anzeige eines farbigen Rahmens bei Verbindungsabbruch.
An | OSD-Timer:	Einblendung des Hinweises *Frozen* und der vergangenen Zeit seit dem Verbindungsabbruch.

5. Klicken Sie auf **Speichern**.

Downsampling des Video-Eingangsformats

HINWEIS: Diese Funktion wird ausschließlich von den **DP-UHR**-Varianten der G&D VisionXS-Serie unterstützt.

In der Standardeinstellung des KVM-Extenders werden eingehende Videosignale am Rechnermodul unverändert am Videoausgang des Arbeitsplatzmoduls ausgegeben.

Falls Sie einen Monitor an das Arbeitsplatzmodul anschließen möchten, der die Bildwiederholrate (Vertikalfrequenz) des Eingangsformates *nicht* unterstützt, kann der KVM-Extender die Bildwiederholrate am Videoausgang des Arbeitsplatzmoduls via Downsampling auf eine unterstützte Frequenz anpassen.

In der Webapplikation können Sie hierfür Downsampling-Regeln für *verschiedene* Bildformate konfigurieren. Die Bildwiederholraten eingehender Videosignale, auf die eine der Regeln zutrifft, werden daraufhin via Downsampling angepasst.

So erstellen Sie eine neue Downsampling-Regel:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie auf **Downsampling konfigurieren**.
5. Klicken Sie auf **Hinzufügen**.
6. Wählen Sie das gewünschte **Eingangsformat**, für das Sie eine Downsampling-Regel erstellen möchten.
7. Klicken Sie auf **Anlegen**.
8. Klicken Sie in die Spalte **Zielformat** der neuen Regel und wählen Sie eines der unterstützten Formate mit der gewünschten Bildwiederholfrequenz.
9. Klicken Sie auf **Speichern**.

So ändern Sie eine Downsampling-Regel:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie auf **Downsampling konfigurieren**.
5. Klicken Sie in die Spalte **Zielformat** der zu ändernden Regel und wählen Sie eines der unterstützten Formate mit der gewünschten Bildwiederholfrequenz.
6. Klicken Sie auf **Speichern**.

So löschen Sie eine Downsampling-Regel:

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie auf **Downsampling konfigurieren**.
5. Klicken Sie in die Spalte **Eingangsformat** der zu löschenden Regel.
6. Klicken Sie auf **Löschen**.
7. Klicken Sie auf **Speichern**.

Persönliche Einstellungen

Anzeige der Informationseinblendung

Informationseinblendungen erfolgen temporär (5 Sekunden) in der linken, oberen Ecke. Alternativ zur temporären Einblendung kann die Informationseinblendung permanent erfolgen oder ausgeschaltet werden.

So ändern Sie die Einstellung der Informationseinblendung:

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 **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **OSD-Info anzeigen** zwischen folgenden Optionen:

Aus:	Informationseinblendung ausschalten
5 Sekunden:	temporäre Informationseinblendung für 5 Sekunden (*Standard*)
Permanent:	permanente Informationseinblendung

5. Klicken Sie auf **Speichern**.

Transparenz des On-Screen-Displays einstellen

In der Standardeinstellung wird das On-Screen-Display (OSD) mit einer mittleren Transparenz über dem Bildschirminhalt angezeigt. Den durch das OSD überlagerten Teil des Bildschirminhalts können Sie „durch“ das OSD erkennen.

Die Transparenzstufe können Sie einstellen oder ausschalten.

So stellen Sie die Transparenzstufe des On-Screen-Displays ein:

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 **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **OSD-Transparenz** zwischen folgenden Optionen:

Hoch:	hohes Durchscheinen des Bildschirminhalts
Mittel:	mittleres Durchscheinen des Bildschirminhalts (*Standard*)
Niedrig:	leichtes Durchscheinen des Bildschirminhalts
Aus:	überdeckende Darstellung des On-Screen-Displays

5. Klicken Sie auf **Speichern**.

Farbe der Informationseinblendung ändern

Informationseinblendungen werden standardmäßig in hellgrün angezeigt. Im persönlichen Profil können Sie die Farbe dieser Einblendungen anpassen.

Folgende Farben werden unterstützt:

schwarz	**dunkelrot**
grün	**dunkelgelb**
dunkelblau	**violett**
dunkeltürkis	**silber**
hellgrün	**gelb**
blau	**magenta**
helltürkis	**weiß**

So ändern Sie die Einstellung der Informationseinblendung:

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 **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Farbe OSD-Info** die gewünschte Farbe.
5. Klicken Sie auf **Speichern**.

Automatisches Schließen des OSD nach Inaktivität

Falls gewünscht, können Sie einstellen, dass das OSD automatisch nach Ablauf einer Zeitspanne der Inaktivität geschlossen wird.

Den Zeitraum der Inaktivität können Sie im Bereich von **5** bis **99** Sekunden festlegen.

HINWEIS: Zum Deaktivieren der Funktion geben Sie die Ziffer **0** ein.

So ändern Sie die Zeitspanne der Inaktivität nach deren Ablauf das OSD geschlossen wird:

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 **KVM-Extender-Systeme**.
4. Geben Sie im Feld **Timeout OSD-Sitzung (Sekunden)** die gewünschte Zeitspanne im Bereich von **5** bis **99** Sekunden ein.
5. Klicken Sie auf **Speichern**.

Rechte

Berechtigung zum Ändern des persönlichen Profils

So ändern Sie die Berechtigung zum Ändern des persönlichen Profils:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Persönliches Profil ändern** in der Spalte **Individuell** zwischen folgenden Optionen:

Aktiviert:	Einsehen und Editieren des eigenen Benutzerprofils erlaubt (*Standard*)
Deaktiviert:	Einsehen und Editieren des eigenen Benutzerprofils untersagt

5. Klicken Sie auf **Speichern**.

WICHTIG: Beim jeweiligen Benutzer sehen Sie in der Spalte **Effektiv** welche Berechtigung aktuell tatsächlich gilt. Klicken Sie auf das i, um zu sehen, woher diese Berechtigung resultiert und an welcher Stelle Sie diese bei Bedarf ändern können.

WICHTIG: Das Effektivrecht (s. Seite 54) ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

Berechtigung zum Einsehen und Ändern der Gerätekonfiguration

So ändern Sie die Berechtigung zum Einsehen und Editieren der Gerätekonfiguration:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Gerätekonfiguration** in der Spalte **Individuell** zwischen folgenden Optionen:

Aktiviert:	Einsehen und Editieren der Gerätekonfiguration erlaubt (*Standard*)
Deaktiviert:	Einsehen und Editieren der Gerätekonfiguration untersagt

5. Klicken Sie auf **Speichern**.

WICHTIG: Beim jeweiligen Benutzer sehen Sie in der Spalte **Effektiv** welche Berechtigung aktuell tatsächlich gilt. Klicken Sie auf das i, um zu sehen, woher diese Berechtigung resultiert und an welcher Stelle Sie diese bei Bedarf ändern können.

WICHTIG: Das Effektivrecht (s. Seite 54) ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

Zugriff auf USB-Geräte

So ändern Sie die USB-Zugriffsberechtigung für *alle* Module:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Zugriff auf USB-Geräte** im Abschnitt **Globale Extender-Rechte** in der Spalte **Individuell** zwischen folgenden Optionen:

Aktiviert:	Zugriff auf die USB-Geräte erlaubt (*Standard*).
Deaktiviert:	Zugriff auf die USB-Geräte untersagt.

5. Klicken Sie auf **Speichern**.

WICHTIG: Beim jeweiligen Benutzer sehen Sie in der Spalte **Effektiv** welche Berechtigung aktuell tatsächlich gilt. Klicken Sie auf das **i**, um zu sehen, woher diese Berechtigung resultiert und an welcher Stelle Sie diese bei Bedarf ändern können.

WICHTIG: Das Effektivrecht (s. Seite 54) ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

So ändern Sie die USB-Zugriffsberechtigung für *ein bestimmtes* Modul:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Zugriff auf USB-Geräte** des Abschnitts **Individuelle Rechte** in der Spalte **Zugriff** zwischen folgenden Optionen für jedes aufgelistete Modul:

Aktiviert:	Zugriff auf die USB-Geräte erlaubt.
Deaktiviert:	Zugriff auf die USB-Geräte untersagt (*Standard*).

5. Klicken Sie auf **Speichern**.

WICHTIG: Beim jeweiligen Benutzer sehen Sie in der Spalte **Effektiv** welche Berechtigung aktuell tatsächlich gilt.

WICHTIG: Das Effektivrecht (s. Seite 54) ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

Zugriffsrecht auf ein Rechnermodul

So ändern Sie die Rechnermodul-Zugriffsrechte:

1. Klicken Sie im Menü auf **Benutzer** bzw. auf **Benutzergruppen**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto bzw. auf die zu konfigurierende Benutzergruppe und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Extender-Systeme**.
4. Wählen Sie im Feld **Zugriff** des Abschnitts **Individuelle Rechte** zwischen folgenden Optionen für jedes aufgelistete Modul:

Ja:	Vollzugriff auf den am Rechnermodul angeschlossenen Computer erlaubt
Nein:	Zugriff auf den am Rechnermodul angeschlossenen Computer untersagt
Ansicht:	Ansicht des Monitorbildes des am Rechnermodul angeschlossenen Computers erlaubt

5. Klicken Sie auf **Speichern**.

WICHTIG: Beim jeweiligen Benutzer sehen Sie in der Spalte **Effektiv** welche Berechtigung aktuell tatsächlich gilt.

WICHTIG: Das Effektivrecht (s. Seite 54) ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

Erweiterte Funktionen für KVM-Extender

Konfigurationseinstellungen übertragen (Gerät ersetzen)

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

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

So übertragen Sie die Konfigurationseinstellungen eines Moduls:

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

Monitoring-Werte konfigurieren

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

Auswahl der zu überwachenden Monitoring-Werte

Das KVM-System überwacht standardmäßig eine Vielzahl verschiedener Werte des KVM-Extenders. 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-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Monitoring**.
4. (De)aktivieren Sie die einzelnen Monitoring-Werte in dem Sie den Regler nach *links* schieben (**aus**) oder nach *rechts* schieben (**an**).

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

5. Klicken Sie auf **Speichern**.

Statusinformationen eines KVM-Extenders einsehen

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

So können Sie die Statusinformationen eines KVM-Extenders einsehen:

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

KVM-Extender	
Name:	Name des KVM-Extenders
Geräte-ID:	physikalische ID des KVM-Extenders
Status:	aktueller Status (**Online** oder **Offline**) des KVM-Extenders
Klasse:	Geräteklasse des KVM-Extenders

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

Aktive Features	
Name:	In diesem Bereich werden alle aktivierten Zusatzfunktionen aufgelistet.

Link-Status	
Link detected:	Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**).
	HINWEIS: Die folgenden Informationen werden nur bei CAT-Varianten angezeigt.
Auto-negotiation:	Die Übertragungsgeschwindigkeit und das Duplex-Verfahren wurden automatisch (**ja**) oder manuell vom Administrator konfiguriert (**nein**).

Link-Status	
Speed:	Übertragungsgeschwindigkeit
Duplex:	Duplexverfahren (**full** bzw. **half**)

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

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

NOTIZEN

NOTIZEN

NOTIZEN

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