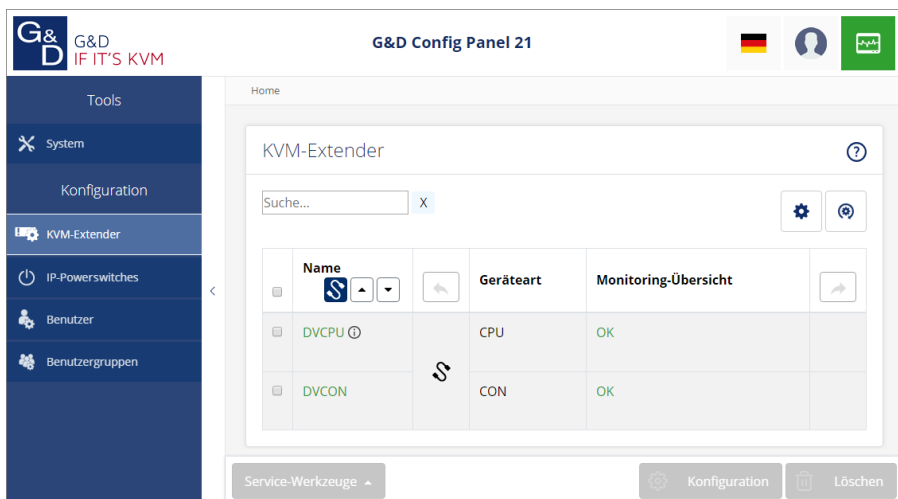


# G&D DP1.2-VisionXG



DE

Web-Applikation »Config Panel«  
Konfiguration des KVM-Extenders

---

## **Zu dieser Dokumentation**

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

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

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

## **Gewährleistungsausschluss**

G&D übernimmt keine Gewährleistung für Geräte, die

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

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

## **Warenzeichennachweis**

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

## **Impressum**

© Guntermann & Drunck GmbH 2019. Alle Rechte vorbehalten.

### **Version 2.00 – 10.05.2019**

Config Panel 21-Version: 1.1.001

Guntermann & Drunck GmbH  
Obere Leimbach 9  
57074 Siegen

Germany

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

<http://www.gdsys.de>  
[sales@gdsys.de](mailto:sales@gdsys.de)

# Inhaltsverzeichnis

## Kapitel 1: Grundfunktionen

<b>Systemvoraussetzungen</b> .....	<b>5</b>
Unterstützte Betriebssysteme .....	5
Empfohlene Grafikauflösungen .....	5
<b>Erstkonfiguration der Netzwerkeinstellungen</b> .....	<b>6</b>
<b>Erste Schritte</b> .....	<b>7</b>
Start der Webapplikation .....	7
Bedienung der Webapplikation .....	8
Die Benutzeroberfläche.....	8
Häufig verwendete Schaltflächen .....	10
Tabellenspalten konfigurieren .....	10
Sprache der Webapplikation auswählen .....	12
Webapplikation beenden .....	12
Versionsnummer der Webapplikation anzeigen .....	12
<b>Grundkonfiguration der Webapplikation</b> .....	<b>13</b>
Netzwerkeinstellungen .....	13
Konfiguration der Netzwerkschnittstellen.....	13
Konfiguration der globalen Netzwerkeinstellungen.....	14
Ausfallsicherheit der Netzwerkverbindung durch Link-Aggregation erhöhen. ....	15
Status der Netzwerkschnittstellen auslesen .....	18
Netzfilterregeln einrichten und administrieren .....	19
Neue Netzfilterregel erstellen .....	19
Bestehende Netzfilterregel bearbeiten .....	20
Bestehende Netzfilterregeln löschen .....	22
Reihenfolge bzw. Priorität der Netzfilterregeln ändern.....	22
Erstellung eines SSL-Zertifikats .....	23
Besonderheiten für komplexe KVM-Systeme .....	23
Erzeugen eines Certificate Authority-Zertifikats.....	23
Erzeugen eines beliebigen Zertifikats.....	25
X509-Zertifikat erstellen und signieren .....	26
PEM-Datei erstellen .....	26
Auswahl eines SSL-Zertifikats .....	26
Durchführung von Firmware-Updates .....	28
Firmware-Update eines bestimmten KVM-Extenders .....	28
Firmware-Update mehrerer Geräte des KVM-Systems.....	28
Wiederherstellung der Werkseinstellungen .....	29
Neustart des Gerätes durchführen .....	30
<b>Netzwerkfunktionen der Geräte</b> .....	<b>31</b>
NTP-Server .....	31
Zeitsynchronisation mit einem NTP-Server .....	31
Manuelle Einstellung von Uhrzeit und Datum.....	32

Protokollierung von Syslog-Meldungen .....	33
Lokale Protokollierung der Syslog-Meldungen .....	33
Versand von Syslog-Meldungen an einen Server .....	34
Lokale Syslog-Meldung einsehen und speichern .....	35
Benutzerauthentifizierung mit Verzeichnisdiensten .....	35
<b>Monitoring-Funktionen .....</b>	<b>38</b>
Alle Monitoring-Werte einsehen .....	38
Monitoring-Werte deaktivieren .....	39
Erweiterte Funktionen zur Verwaltung der kritischen Geräte .....	40
Auflistung der kritischen Monitoring-Werte einsehen .....	40
Alarm eines kritischen Gerätes bestätigen .....	40
<b>Geräteüberwachung via SNMP .....</b>	<b>41</b>
Praktischer Einsatz des SNMP-Protokolls .....	41
Konfiguration des SNMP-Agents .....	41
Konfiguration von SNMP-Traps .....	44
<b>Benutzer und Gruppen .....</b>	<b>46</b>
Anlegen eines neuen Benutzerkontos .....	46
Änderung des Namens eines Benutzerkontos .....	47
Änderung des Passworts eines Benutzerkontos .....	47
Aktivierung oder Deaktivierung eines Benutzerkontos .....	47
Löschen eines Benutzerkontos .....	48
System-Rechte .....	48
Berechtigung zum uneingeschränkten Zugriff (Superuser) .....	48
Berechtigung zum Login in die Webapplikation .....	49
Berechtigung zur Änderung des eigenen Passworts .....	49
<b>Erweiterte Funktionen des KVM-Systems .....</b>	<b>50</b>
Identifizierung eines Gerätes durch Aktivierung der Identification-LED .....	50
Sicherung und Wiederherstellung der Daten des KVM-Systems .....	50

## Kapitel 2: KVM-Extender

<b>Grundkonfiguration der KVM-Extender .....</b>	<b>52</b>
Änderung des Namens eines KVM-Extender .....	52
Änderung des Kommentares eines KVM-Extenders .....	52
Einen KVM-Extender aus dem KVM-System löschen .....	53
<b>Konfigurationseinstellungen der KVM-Extender .....</b>	<b>53</b>
Gerätekonfiguration .....	53
Betriebsarten des KVM-Extenders .....	53
Änderung der Hotkey-Modifiziertaste .....	54
Änderung der OSD-Taste .....	55
On-Screen-Display mit doppeltem Tastendruck starten .....	56
USB-HID-Modus auswählen .....	56
Änderung des Scancode-Sets einer PS/2-Tastatur .....	58
Tastaturlayout für Eingaben innerhalb des OSDs auswählen .....	59
Reinitialisierung von USB-Eingabegeräten .....	60

Gerätekonfiguration ( <i>Fortsetzung</i> )	
Wartezeit des Bildschirmschoners einstellen .....	61
Fallback-Kompression ein oder ausschalten .....	61
Berechtigung für exklusiven Zugriff des Arbeitsplatzes .....	62
Änderung der Videobetriebsart der Arbeitsplätze .....	63
Änderung der Zeitspanne der Eingabesperre .....	63
Änderung der Exklusivmodus-Aktionstaste .....	64
Videokanal-Konfiguration .....	65
EDID-Profil eines Monitores einlesen .....	65
EDID-Profil eines Kanals festlegen .....	66
Reduzierung der Farbtiefe der zu übertragenden Bilddaten .....	67
DDC/CI-Unterstützung (de)aktivieren .....	67
Verwendung des Freeze-Modus .....	68
Freeze-Modus-Puffer an bzw. ausschalten .....	69
Persönliche Einstellungen .....	70
Anzeige der Informationseinblendung .....	70
Transparenz des On-Screen-Displays einstellen .....	70
Farbe der Informationseinblendung ändern .....	71
Automatisches Schließen des OSD nach Inaktivität .....	72
<b>Rechte</b> .....	<b>73</b>
Berechtigung zum Ändern des persönlichen Profils .....	73
Berechtigung zum Einsehen und Editieren der Gerätekonfiguration .....	73
Zugriff auf USB-Geräte .....	74
Zugriffsrecht auf ein Rechnermodul .....	75
Berechtigung zur Schaltung der Steckdosen eines Rechnermoduls .....	75
<b>Erweiterte Funktionen für KVM-Extender</b> .....	<b>76</b>
Konfigurationseinstellungen übertragen (Gerät ersetzen) .....	76
Monitoring-Werte konfigurieren .....	76
Auswahl der zu überwachenden Monitoring-Werte .....	76
Statusinformationen eines KVM-Extenders einsehen .....	77
<b>IP-Powerswitch</b> .....	<b>79</b>
Konfiguration .....	79
Einen IP-Powerswitch zum KVM-System hinzufügen .....	79
Änderung von Namen oder Kommentar eines IP-Powerswitches .....	79
Einen IP-Powerswitch konfigurieren .....	80
Powerswitch-Steckdose dem KVM-Extender zuordnen .....	80
Einen IP-Powerswitch aus dem KVM-System löschen .....	81
Statusinformationen eines IP-Powerswitches einsehen .....	81

# 1 Grundfunktionen

Die Webapplikation *ConfigPanel* bietet eine grafische Benutzeroberfläche zur Konfiguration des KVM-Systems. Sie kann über einen unterstützten Webbrowser (s. Seite 5) bedient werden.

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

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

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

# Systemvoraussetzungen

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

Anschließend sind – sofern nicht bereits erledigt – die auf Seite 6 beschriebenen Netzwerkeinstellungen anzupassen.

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

- Apple Safari 12
- Google Chrome 74
- Internet Explorer 11
- Microsoft Edge 44
- Mozilla Firefox 66

## Unterstützte Betriebssysteme

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

## Empfohlene Grafikauflösungen

- Eine Mindestauflösung von 1366×768 Bildpunkten wird empfohlen.
- Die Webapplikation ist für die Darstellung der Inhalte im Querformat (Landscape-Modus) optimiert.
- Das Hochformat (Portrait-Modus) wird unterstützt. Möglicherweise sind in diesem Modus *nicht* alle Inhalte sichtbar.

# Erstkonfiguration der Netzwerkeinstellungen

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

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

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

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

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

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

3. Schalten Sie das Gerät ein.
4. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile die URL **192.168.0.1** ein.
5. Konfigurieren Sie die Netzwerkschnittstelle(n) und die globalen Netzwerkeinstellungen wie im Abschnitt *Netzwerkeinstellungen* auf Seite 13 f. beschrieben.

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

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



# Erste Schritte

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

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

## Start der Webapplikation

**HINWEIS:** Informationen zu den Systemvoraussetzungen der Webapplikation finden Sie auf Seite 5.

### 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:

**Benutzername:** Geben Sie Ihren Benutzernamen ein.

**Passwort:** Geben Sie das Passwort Ihres Benutzerkontos ein.

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

Melden Sie sich hierfür mit dem Administratorkonto in die Webapplikation ein und ändern Sie anschließend das Passwort (s. Seite 47).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

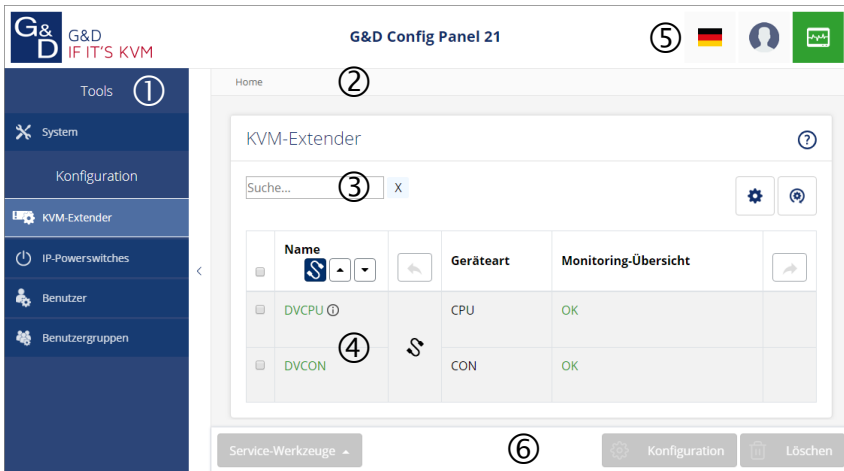
- **Benutzername:** Admin
- **Passwort:** 4658

3. Klicken Sie auf **Login**.

# Bedienung der Webapplikation

## Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus mehreren Bereichen:



**Abbildung 1: Benutzeroberfläche der Webapplikation**

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

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

**Schnellzugriffe** ☺

**Sprachauswahl:** Die Länderflagge zeigt die derzeit aktive Sprache in der Webapplikation an.

Zur Umschaltung der Sprache (*deutsch/englisch*) klicken Sie auf die Länderflagge. Daraufhin öffnet sich ein Untermenü, das alle unterstützten Sprachen in Form von Flaggen anzeigt. Schalten Sie mit einem Klick auf die gewünschte Flagge 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** ☺:

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

## Häufig verwendete Schaltflächen

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

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

## Tabellenspalten konfigurieren

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

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

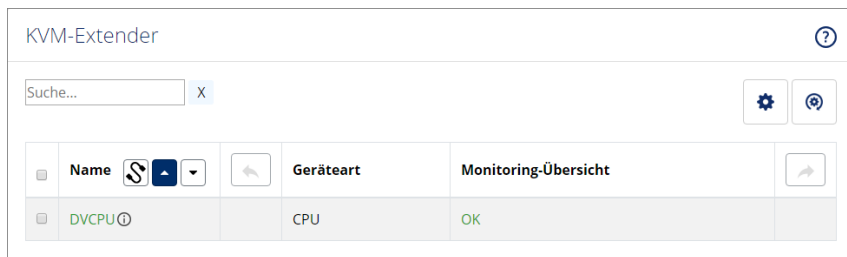
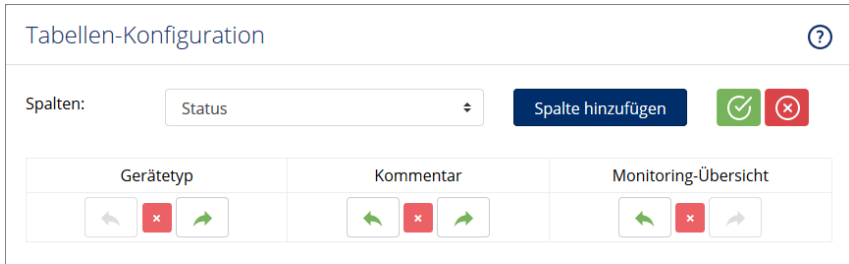


Abbildung 2: Tabellenspalten (Standardeinstellung) eines KVM-Extenders

### 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 Schaltfläche (✖️) 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**.

## Sprache der Webapplikation auswählen

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

### So ändern Sie die Standardsprache der Webapplikation:

1. Klicken Sie auf die **Länderflagge** rechts oben.



Es öffnet sich ein Untermenü, das alle unterstützten Sprachen in Form von Flaggen anzeigt.

2. Schalten Sie mit einem Klick auf die gewünschte **Flagge** die Sprache um.

## 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.



## 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.

# Grundkonfiguration der Webapplikation

## Netzwerkeinstellungen

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

**WICHTIG:** Beachten Sie die separaten Anweisungen zur *Erstkonfiguration der Netzwerkeinstellungen* auf Seite 6.

## Konfiguration der Netzwerkschnittstellen

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

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

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

## So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:

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

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

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

<b>Betriebsmodus:</b>	Wählen Sie den Betriebsmodus der <b>Schnittstelle A</b> bzw. <b>Schnittstelle B</b> aus: <ul style="list-style-type: none"><li>▪ <b>Aus:</b> Netzwerkschnittstelle ausschalten.</li><li>▪ <b>Statisch:</b> Es wird eine statische IP-Adresse zugeteilt.</li><li>▪ <b>DHCP:</b> ■Bezug der IP-Adresse von einem DHCP-Server.:</li></ul>
<div style="border: 1px solid black; padding: 5px; margin: 5px 0;">In der Drop-Down-Liste wird der Text <b>Link-Aggregation aktiv</b> angezeigt, falls die Schnittstelle zu einer Netzwerkschnittstellen-Gruppe hinzugefügt wurde. Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall im Bereich »Link-Aggregation«.</div>	
<b>IP-Adresse:</b>	Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die IP-Adresse der Schnittstelle an.
<b>Netzmaske:</b>	Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die Netzmaske des Netzwerkes an.

6. Klicken Sie auf **Speichern**.

## Konfiguration der globalen Netzwerkeinstellungen

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

**So konfigurieren Sie die globalen Netzwerkeinstellungen:**

1. Klicken Sie im Menü auf **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 Einstellungen**.



## 5. Erfassen Sie folgende Daten:

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

6. Klicken Sie auf **Speichern**.

### Ausfallsicherheit der Netzwerkverbindung durch Link-Aggregation erhöhen

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

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

Zur Überwachung der Schnittstellen stehen zwei verschiedene Modi zur Verfügung:

- **MII-Modus:** Der Carrier-Status der Netzwerkschnittstelle wird über das *Media Independent Interface* überwacht. In diesem Modus wird lediglich die Funktionalität der Netzwerkschnittstelle geprüft.
- **ARP-Modus:** Über das *Address-Resolution-Protokoll* werden Anfragen an ein ARP-Target im Netzwerk gesendet. Die Antwort des ARP-Targets bestätigt sowohl die Funktionalität der Netzwerkschnittstelle, als auch eine einwandfreie Netzwerkverbindung zum ARP-Target.

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

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

**So konfigurieren Sie die Einstellungen einer Netzwerkschnittstellen-Gruppe:**

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

1. Klicken Sie im Menü auf **KVM-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 **Link-Aggregation**.
5. Erfassen Sie im Abschnitt **Netzwerk** folgende Daten:

<b>Name:</b>	Geben Sie den gewünschten Namen der Netzwerkschnittstellen-Gruppe ein.
<b>Betriebsmodus:</b>	Wählen Sie den Betriebsmodus der Netzwerkschnittstellen-Gruppe aus: <ul style="list-style-type: none"><li>▪ <b>Aus:</b> Link-Aggregation ausschalten. <i>Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall im Bereich »Schnittstellen«.</i></li><li>▪ <b>Statisch:</b> Es wird eine statische IP-Adresse zugeteilt.</li><li>▪ <b>DHCP:</b> Bezug der IP-Adresse von einem DHCP-Server.</li></ul>
<b>IP-Adresse:</b>	Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die IP-Adresse der Schnittstelle an.
<b>Netzmaske:</b>	Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die Netzmaske des Netzwerkes an.

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

<b>Primärer Slave:</b>	<p>Wählen Sie, ob der Datenverkehr bevorzugt über die Schnittstelle <i>Network A</i> (<b>Schnittstelle A</b>) bzw. <i>Network B</i> (<b>Schnittstelle B</b>) erfolgen soll. Sobald die ausgewählte Schnittstelle verfügbar ist, wird diese Schnittstelle für den Datenverkehr verwendet.</p> <p>Wählen Sie die Option <b>Keiner</b>, wird der Datenverkehr über eine beliebige Schnittstelle gesendet. Eine Umschaltung erfolgt nur, wenn die aktive Schnittstelle ausfällt.</p>
<b>Link-Monitoring:</b>	Wählen Sie, ob der <b>MII-</b> oder der <b>ARP-Modus</b> (s. Erläuterung oben) zum Monitoring der Schnittstelle verwendet werden soll.
<b>MII-Down-Delay:</b>	<p>Wartezeit in Millisekunden, bevor eine ausgefallene Netzwerkschnittstelle deaktiviert wird.</p> <p>Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.</p>
<b>MII-Up-Delay:</b>	<p>Wartezeit in Millisekunden, bevor eine wiederhergestellte Netzwerkschnittstelle aktiviert wird.</p> <p>Der eingegebene Wert muss ein Vielfaches von 100 ms (der MII-Link-Monitoring-Frequenz) sein.</p>
<b>ARP-Intervall:</b>	Geben Sie das Intervall (100 bis 10.000 Millisekunden) ein, nach welchem eine Prüfung auf eingegangene ARP-Pakete der Netzwerkschnittstellen erfolgt.
<b>ARP-Validierung:</b>	<p>Die Validierung stellt sicher, dass das ARP-Paket für eine bestimmte Netzwerkschnittstelle von einem der angegebenen ARP-Targets generiert wurde.</p> <p>Wählen Sie, ob bzw. welche der eingehenden ARP-Pakete validiert werden sollen:</p> <ul style="list-style-type: none"> <li>▪ <b>Keine:</b> Die ARP-Pakete werden nicht validiert (Standard).</li> <li>▪ <b>Aktiv:</b> Ausschließlich die ARP-Pakete der aktiven Netzwerkschnittstelle werden validiert.</li> <li>▪ <b>Backup:</b> Ausschließlich die ARP-Pakete der inaktiven Netzwerkschnittstelle werden validiert.</li> <li>▪ <b>Alle:</b> Die ARP-Pakete aller Netzwerkschnittstellen der Gruppe werden validiert.</li> </ul>
<b>ARP-Target:</b>	<p>Die Tabelle enthält eine Liste aller konfigurierten ARP-Targets.</p> <p>Verwenden Sie die Schaltflächen <b>Hinzufügen</b>, <b>Ändern</b> und <b>Löschen</b>, um die ARP-Targets zu verwalten.</p>

7. Klicken Sie auf **Speichern**.

## Status der Netzwerkschnittstellen auslesen

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

### So ermitteln Sie den Status der Netzwerkschnittstellen:

1. Klicken Sie im Menü auf **KVM-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. In den Abschnitten **Schnittstelle A** und **Schnittstelle B** werden Ihnen folgende Daten angezeigt:

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

6. Klicken Sie auf **Speichern**.

## Netzfilterregeln einrichten und administrieren

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

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

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

### Neue Netzfilterregel erstellen

**So erstellen Sie eine neue Netzfilterregel:**

1. Klicken Sie im Menü auf **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:

<b>Schnittstelle:</b>	Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen: <ul style="list-style-type: none"> <li>▪ <b>Alle</b></li> <li>▪ <b>Schnittstelle A</b></li> <li>▪ <b>Schnittstelle B</b></li> <li>▪ <b>[Name einer Netzwerkschnittstellen-Gruppe]</b></li> </ul>
<b>Option:</b>	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: <ul style="list-style-type: none"> <li>▪ <b>Normal:</b> Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li> <li>▪ <b>Invertiert:</b> Die Regel gilt für Datenpakete, deren Absenderinformation <i>nicht</i> der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li> </ul>

**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.

<b>Schnittstelle:</b>	Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen: <ul style="list-style-type: none"> <li>▪ <b>Alle</b></li> <li>▪ <b>Netzwerk A</b></li> <li>▪ <b>Netzwerk B</b></li> </ul>
<b>Option:</b>	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: <ul style="list-style-type: none"> <li>▪ <b>Normal:</b> Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li> <li>▪ <b>Invertiert:</b> Die Regel gilt für Datenpakete, deren Absenderinformation <i>nicht</i> der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.</li> </ul>
<b>IP-Adresse/ Netzmaske:</b>	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes <b>Netzmaske</b> – den Adressraum der IP-Adressen ein. <p><b>Beispiele:</b></p> <ul style="list-style-type: none"> <li>▪ <b>192.168.150.187:</b> nur die IP-Adresse 192.168.150.187</li> <li>▪ <b>192.168.150.0/24:</b> IP-Adressen des Raums 192.168.150.x</li> <li>▪ <b>192.168.0.0/16:</b> IP-Adressen des Raums 192.168.x.x</li> <li>▪ <b>192.0.0.0/8:</b> IP-Adressen des Raums 192.x.x.x</li> <li>▪ <b>0.0.0.0/0:</b> alle IP-Adressen</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p> </div>
<b>MAC-Adresse:</b>	Geben Sie die MAC-Adresse ein, welche in dieser Filterregel zu berücksichtigen ist. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p> </div>
<b>Filterregel:</b>	<ul style="list-style-type: none"> <li>▪ <b>Drop:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden <i>nicht</i> verarbeitet.</li> <li>▪ <b>Accept:</b> Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.</li> </ul>
<b>Service:</b>	Wählen Sie einen bestimmten Service, für den diese Regel exklusiv angewendet wird oder wählen Sie ( <b>Alle</b> ).

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/Priorität Sie ändern möchten.
6. Klicken Sie auf die Schaltfläche **Pfeil hoch**, um die Priorität zu erhöhen oder auf die Schaltfläche **Pfeil runter**, um die Priorität zu verringern.
7. Klicken Sie auf **Speichern**.



## Erstellung eines SSL-Zertifikats

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

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 23) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 26) 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 Zertifikat wird durch OpenSSL erstellt und unter dem Dateinamen *ca.crt* gespeichert.

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

## Erzeugen eines beliebigen Zertifikats

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

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

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

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

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

So erstellen Sie die Zertifikatsanforderung:

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

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

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

Nachfolgend sind die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country Name (2 letter code)	DE
State or Province Name	NRW
Locality Name (eg, city)	Siegen
Organization Name (eg, company)	Guntermann & Drunck GmbH
Organizational Unit Name (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 x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
```

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

## PEM-Datei erstellen

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

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

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

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

a. Linux

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

b. Windows

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

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

## Auswahl eines SSL-Zertifikats

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

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

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

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

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

**WICHTIG:** Nur wenn alle Geräte innerhalb eines KVM-Systems Zertifikate der identischen *Certificate Authority* (s. Seite 23) verwenden, können die Geräte miteinander kommunizieren.

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

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

1. Klicken Sie im Menü auf **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.

**TIPP:** Ältere Geräte unterstützten *nicht* das **Zertifikat #1**. Verwenden Sie in diesem Fall **Zertifikat #2** oder **Eigenes Zertifikat** innerhalb des KVM-Systems.

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

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

Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat:

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

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

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

3. Klicken Sie auf **OK**, um den Dialog zu verlassen.

## Durchführung von Firmware-Updates

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

### Firmware-Update eines bestimmten KVM-Extenders

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

**So aktualisieren Sie die Firmware eines bestimmten KVM-Extenders:**

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**.

### 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**.

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**.

## Wiederherstellung der Werkseinstellungen

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

### So stellen Sie die Werkseinstellungen wieder her:

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

<b>Alle Einstellungen zurücksetzen:</b>	Alle Einstellungen des Gerätes zurücksetzen.
<b>Nur Einstellungen für lokales Netzwerk zurücksetzen:</b>	Ausschließlich die lokalen Netzwerkeinstellungen zurücksetzen.
<b>Nur Einstellungen für KVM-Anwendungen zurücksetzen:</b>	Alle Einstellungen außer den lokalen Netzwerkeinstellungen zurücksetzen.

4. Klicken Sie auf **Werkseinstellungen**.

## Neustart des Gerätes durchführen

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

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

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



# Netzwerkfunktionen der Geräte

Die Geräte innerhalb des KVM-Systems (z. B. *KVM-Extender* und *KVM-Matrixswitches*) 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 41 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:

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

5. Klicken Sie auf **Speichern**.

## Manuelle Einstellung von Uhrzeit und Datum

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

1. Klicken Sie im Menü auf **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-Zeit-synchronisation**, da andernfalls die manuelle Einstellung von Uhrzeit und Datum nicht möglich ist.

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

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

7. Klicken Sie auf **Speichern**.

## Protokollierung von Syslog-Meldungen

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

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

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

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

### Lokale Protokollierung der Syslog-Meldungen

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

1. Klicken Sie im Menü auf **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:

<b>Syslog lokal:</b>	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie die lokale Protokollierung von Syslog-Meldungen aus oder ein: <ul style="list-style-type: none"> <li>▪ <b>Deaktiviert</b></li> <li>▪ <b>Aktiviert</b></li> </ul>
<b>Log-Level:</b>	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.

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**:

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

5. Klicken Sie auf **Speichern**.

## Lokale Syslog-Meldung einsehen und speichern

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

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

1. Klicken Sie im Menü auf **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 (s. Seite 35) 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.

**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:

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

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

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

**TIPP:** Erfassen Sie nach der Auswahl eines Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers im Bereich *Servereinstellungen* der Dialogmaske.

**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.

6. Klicken Sie auf **Speichern**.

# 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:

The screenshot shows the 'KVM-Extender' interface. At the top, there is a search bar with the text 'Suche...' and a close button 'X'. To the right of the search bar are two icons: a gear for settings and a refresh icon. Below the search bar is a table with the following columns: 'Name' (with a dropdown arrow), 'Status', 'Main power', and 'Temperature'. The table contains one row for the device 'DVCPUI' (with an information icon). The 'Status' column shows 'Online', 'Main power' shows 'On', and 'Temperature' shows '34.0'. There are also left and right navigation arrows above the table.

Name	Status	Main power	Temperature
DVCPUI	Online	On	34.0

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

Die, für die Tabellenansicht (siehe *Tabellenspalten konfigurieren* auf Seite 10) 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 konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Monitoring**.

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

4. Klicken Sie auf **Speichern**.



## Monitoring-Werte deaktivieren

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

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

**WICHTIG:** Zu deaktivierten Monitoring-Werte erscheinen *keine* Warnungen in der Web-Applikation 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 den zu konfigurierenden KVM-Switch 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 den zu konfigurierenden KVM-Switch 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 8) 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.

**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:

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

<b>Access:</b>	Aktivieren Sie den lesenden Zugriff ( <b>View</b> ), schreibenden Zugriff ( <b>Full</b> ) oder verweigern Sie den Zugriff ( <b>No</b> ) über das <i>SNMPv2c</i> -Protokoll.
<b>Source:</b>	Geben Sie die IP-Adresse oder den Adressraum der Adressen eingehender SNMP-Pakete ein. <b>Beispiele:</b> <ul style="list-style-type: none"><li>▪ <b>192.168.150.187:</b> nur die IP-Adresse 192.168.150.187</li><li>▪ <b>192.168.150.0/24:</b> IP-Adressen des Raums 192.168.150.x</li><li>▪ <b>192.168.0.0/16:</b> IP-Adressen des Raums 192.168.x.x</li><li>▪ <b>192.0.0.0/8:</b> IP-Adressen des Raums 192.x.x.x</li></ul>
<b>Read-only community:</b>	Geben Sie die Bezeichnung einer bestimmten <i>Community</i> ein, welche auch im <i>Network Management System</i> 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:

<b>Access:</b>	Aktivieren Sie den lesenden Zugriff ( <b>View</b> ), schreibenden Zugriff ( <b>Full</b> ) oder verweigern Sie den Zugriff ( <b>No</b> ) über das <i>SNMPv3</i> -Protokoll.
<b>Benutzername:</b>	Geben Sie den Benutzernamen für die Kommunikation mit dem <i>Network Management System</i> an.
<b>Authentifizierungsprotokoll</b>	Wählen Sie das im <i>Network Management System</i> aktivierte Authentifizierungs-Protokoll ( <b>MD5</b> oder <b>SHA</b> ) aus.
<b>Authentifizierungspasswort</b>	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem <i>Network Management System</i> an.
<b>Security-Level</b>	Wählen Sie zwischen einer der folgenden Optionen: <ul style="list-style-type: none"> <li>▪ <b>noAuthNoPriv:</b> Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll deaktiviert</li> <li>▪ <b>authNoPriv:</b> Benutzer-Authentifizierung aktiviert, <i>Privacy</i>-Protokoll deaktiviert</li> <li>▪ <b>authPriv:</b> Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll aktiviert</li> </ul>
<b>Privacy-Protokoll:</b>	Wählen Sie das im <i>Network Management System</i> aktivierte Privacy-Protokoll ( <b>DES</b> oder <b>AES</b> ) aus.
<b>Privacy-Passwort:</b>	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem <i>Network Management System</i> an.
<b>Engine-ID-Methode:</b>	Wählen Sie, nach welcher Methode die <b>SnmpEngineID</b> gegeben werden soll: <ul style="list-style-type: none"> <li>▪ <b>Random:</b> Die <i>SnmpEngineID</i> wird bei jedem Neustart des Gerätes neu vergeben.</li> <li>▪ <b>Fix:</b> Die <i>SnmpEngineID</i> entspricht der MAC-Adresse der ersten Netzwerkschnittstelle des Gerätes.</li> <li>▪ <b>User:</b> Der im Feld <i>Engine-ID</i> eingetragene String wird als <i>SnmpEngineID</i> verwendet.</li> </ul>
<b>Engine-ID</b>	Bei Verwendung der <i>Engine-ID-Methode User</i> geben Sie hier den String ein, der als <i>Engine-ID</i> verwendet wird.

8. Klicken Sie auf **Speichern**.

## 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:

<b>Server:</b>	Geben Sie die IP-Adresse des <i>Network Management Servers</i> ein.
<b>Protokoll:</b>	Wählen Sie das Protokoll ( <b>TCP</b> oder <b>UDP</b> ) – üblicherweise UDP – aus, über welches die SNMP-Pakete übertragen werden sollen.
<b>Port:</b>	Geben Sie den Port – üblicherweise 162 – an, auf welchem <i>ausgehende</i> SNMP-Pakete übertragen werden.
<b>Versuche:</b>	Geben Sie die Anzahl der Versand-Wiederholungen eines <i>SNMP Inform</i> an.
<p><b>HINWEIS:</b> Eine Eingabe ist nur möglich, wenn im Feld <i>Notification type</i> die Option <i>Inform</i> gewählt wurde.</p>	
<b>Timeout:</b>	Geben Sie das Timeout (in Sekunden) ein, nach welchem die erneute Aussendung eines <i>SNMP Inform</i> erfolgt, wenn keine Bestätigung erfolgt.
<p><b>HINWEIS:</b> Eine Eingabe ist nur möglich, wenn im Feld <i>Notification type</i> die Option <i>Inform</i> gewählt wurde.</p>	
<b>Log-Level:</b>	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.
<p><b>HINWEIS:</b> Wählen Sie den Schweregrad 2 - <i>Kritisch</i>, so werden bei Ereignissen dieses, wie auch der Schweregrade 1 - <i>Alarm</i> und 0 - <i>Notfall</i>, SNMP-Traps ausgesendet.</p>	
<b>Version:</b>	Wählen Sie, ob die Traps gemäß der Protokollversion <i>SNMPv2c</i> ( <b>v2c</b> ) oder <i>SNMPv3</i> ( <b>v3</b> ) erstellt und versendet werden.
<b>Benachrichtigungsart:</b>	Wählen Sie, ob die Ereignisse als <i>Trap</i> - oder <i>Inform</i> -Paket versendet werden.
<p><b>HINWEIS:</b> <i>Inform</i>-Pakete erfordern eine Bestätigung des <i>Network Management Systems</i>. Liegt diese nicht vor, wird die Übertragung wiederholt.</p>	

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:

<b>Benutzername:</b>	Geben Sie den Benutzernamen für die Kommunikation mit dem <i>Network Management System</i> an.
<b>Authentifizierungsprotokoll</b>	Wählen Sie das im <i>Network Management System</i> aktivierte Authentifizierungs-Protokoll ( <b>MD5</b> oder <b>SHA</b> ) aus.
<b>Authentifizierungspasswort</b>	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem <i>Network Management System</i> an.
<b>Security-Level</b>	Wählen Sie zwischen einer der folgenden Optionen: <ul style="list-style-type: none"> <li>▪ <b>noAuthNoPriv:</b> Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll deaktiviert</li> <li>▪ <b>authNoPriv:</b> Benutzer-Authentifizierung aktiviert, <i>Privacy</i>-Protokoll deaktiviert</li> <li>▪ <b>authPriv:</b> Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll aktiviert</li> </ul>
<b>Privacy-Protokoll:</b>	Wählen Sie das im <i>Network Management System</i> aktivierte Privacy-Protokoll ( <b>DES</b> oder <b>AES</b> ) aus.
<b>Privacy-Passwort:</b>	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem <i>Network Management System</i> an.
<b>Engine-ID:</b>	Geben Sie die <i>Engine-ID</i> 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

Durch die Verwendung von Benutzerkonten besteht die Möglichkeit, die Rechte des Benutzers individuell festzulegen.

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

## Anlegen eines neuen Benutzerkontos

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

### So erstellen Sie ein neues Benutzerkonto:

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

<b>Name:</b>	Geben Sie den gewünschten Benutzernamen ein.
<b>Passwort:</b>	Geben Sie das Passwort des Benutzerkontos ein.
<b>Passwort bestätigen:</b>	Wiederholen Sie das oben eingegebene Passwort.
<b>Klartext:</b>	Aktivieren Sie ggf. dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können.
<b>Vollständiger Name:</b>	Geben Sie hier – falls gewünscht – den vollständigen Namen des Benutzers ein.
<b>Kommentar:</b>	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto.
<b>Aktiviert:</b>	Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.

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.



## 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**.

## Änderung des Passworts eines Benutzerkontos

So ändern Sie das Passwort eines Benutzerkontos:

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

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

4. Klicken Sie auf **Speichern**.

## 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.

## 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**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **System-Rechte**.
4. Wählen Sie im Feld **Superuser-Recht** zwischen folgenden Optionen:

<b>Ja:</b>	Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte erlaubt
<b>Nein:</b>	Uneingeschränkten Zugriff auf das KVM-System und die angeschlossenen Geräte untersagt

5. Klicken Sie auf **Speichern**.

## Berechtigung zum Login in die Webapplikation

So ändern Sie die Berechtigung zum Login mit der Webapplikation:

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

<b>Ja:</b>	Zugriff auf die Webapplikation erlaubt
<b>Nein:</b>	Zugriff auf die Webapplikation untersagt

5. Klicken Sie auf **Speichern**.

## Berechtigung zur Änderung des eigenen Passworts

So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:

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

<b>Ja:</b>	Passwortänderung des eigenen Benutzerkontos erlaubt
<b>Nein:</b>	Passwortänderung des eigenen Benutzerkontos 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 an der Frontblende 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 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 und Wiederherstellung der Daten des KVM-Systems

Alle 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 **Netzwerk-Einstellungen** und/oder die **Anwendungs-Einstellungen** sichern.
6. Klicken Sie auf **Backup**.

**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 gewünschten Backup-Datei handelt.
6. Wählen Sie den Umfang der zu wiederherzustellenden Daten: Sie können wahlweise die **Netzwerk-Einstellungen** und/oder die **Anwendungs-Einstellungen** wiederherstellen.

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

7. Klicken Sie auf **Restore**.

# 2 KVM-Extender

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

## 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein** und darunter auf den Reiter **CPU** bzw. **CON**.
4. Geben Sie im Feld **Name** des Abschnitts **Gerät** den gewünschten Namen des KVM-Extenders ein.
5. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein** und darunter auf den Reiter **CPU** bzw. **CON**.
4. Geben Sie im Feld **Kommentar** des Abschnitts **Gerät** einen beliebigen Kommentar ein.
5. 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 standardmäßig eingestellt.

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 und seinem Passwort.

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

**So wählen Sie die Betriebsart des KVM-Extenders:**

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 **Allgemein** und darunter auf den Reiter **CON**.
4. Wählen Sie im Feld **Betriebsmodus** zwischen folgenden Optionen:

<b>Open Access Console:</b>	Open Access-Betriebsart ( <i>Standard</i> )
<b>Standard:</b>	Standard-Betriebsart

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

**Änderung der Hotkey-Modifiziertaste**

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

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

**So ändern Sie die Hotkey-Modifiziertaste:**

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 **Allgemein** und darunter auf den Reiter **CPU**.



4. Wählen Sie im Feld **Hotkey-Modifizierer** des Abschnitts **Konfiguration** *mindestens* eine der aufgeführten Modifizierertasten durch Markierung des entsprechenden Kontrollkästchens:

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

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

5. Klicken Sie auf **Speichern**.

## Änderung der OSD-Taste

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.

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

### So ändern Sie die aktuellen OSD-Taste:

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 **Allgemein** und darunter auf den Reiter **CPU**.
4. Wählen Sie im Feld **Hotkey** die OSD-Taste aus, welche gemeinsam mit der bzw. den Hotkey-Modifizierertaste(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*.

5. Klicken Sie auf **Speichern**.

## On-Screen-Display mit doppeltem Tastendruck starten

Alternativ zum Öffnen des On-Screen-Displays (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 On-Screen-Displays mit doppeltem Tastendruck:

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 **Allgemein** und darunter auf den Reiter **CPU**.
4. Wählen Sie im Feld **OSD via doppeltem Tastendruck** die gewünschte Taste aus.

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

5. Klicken Sie auf **Speichern**.

## USB-HID-Modus auswählen

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 den spezifischen USB-Tastaturmodi können Sie den **Generic-HID**-Modus nutzen. In diesem Modus werden die Daten des USB-Gerätes an der obersten **Keyb./Mouse**-Buchse des Arbeitsplatzmoduls unverändert an das Rechnermodul übertragen.

**WICHTIG:** Der **Generic-HID**-Modus unterstützt viele der am Markt erhältlichen HID-Geräte. Der Betrieb eines bestimmten HID-Gerätes im Generic-HID-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-HID-Modus** verwendet werden.

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

Bei Einsatz eines *Apple Keyboards* bzw. *Sun Keyboards* erlauben spezielle Tastaturmodi die Verwendung der Sondertasten dieser Tastaturen.

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
HP 2310tk	▸ HP 2310t
iiyama T1931	▸ iiyama T1931
NOTTROT N170 KGE	▸ NOTTROT N170 KGE
Wacom Cintiq 21UX	▸ Wacom Cintiq 21US
Wacom Intuos3	▸ Wacom Intuos 3
Wacom Intuos4 S	▸ Wacom Intuos 4 S
Wacom Intuos4 M	▸ Wacom Intuos 4 M
Wacom Intuos4 L	▸ Wacom Intuos 4 L
Wacom Intuos4 XL	▸ Wacom Intuos 4 XL
Wacom Intuos5 S	▸ Wacom Intuos 5 S
Wacom Intuos5 M	▸ Wacom Intuos 5 M
Wacom Intuos5 L	▸ Wacom Intuos 5 L

- **Generic-HID-Modus:** In diesem Modus werden die Daten des USB-Gerätes an der obersten **Keyb./Mouse**-Buchse des Arbeitsplatzmoduls unverändert an das Rechnermodul übertragen.

EINGABEGERÄT	EINSTELLUNG
beliebiges USB-Gerät	▸ Generic HID

**WICHTIG:** Der **Generic-HID**-Modus unterstützt viele der am Markt erhältlichen HID-Geräte. Der Betrieb eines bestimmten HID-Gerätes im Generic-HID-Modus kann nicht gewährleistet werden.

▪ **Controller:** Der Multimedia-Controller **ShuttlePRO v2** wird zur Bedienung verschiedener Audio- und Videoprogramme genutzt. Ein spezieller USB-Tastaturmodus erlaubt die Verwendung des Controllers zur Bedienung des am Target-Moduls angeschlossenen Rechners:

EINGABEGERÄT	EINSTELLUNG
Contour ShuttlePRO v2	▸ Contour Shuttle Pro 2

▪ **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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein** und darunter auf den Reiter **CPU**.
4. Wählen Sie im Feld **USB-HID-Mode** die gewünschte Option (s. oben).
5. Klicken Sie auf **Speichern**.

### Änderung des Scancode-Sets einer PS/2-Tastatur

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

Der KVM-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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**, falls Sie die Einstellung des lokalen Arbeitsplatzes (am **CPU**-Modul) einstellen möchten.

Klicken Sie auf den Reiter **CON**, falls Sie die Einstellung des entfernten Arbeitsplatzes (am **CON**-Modul) einstellen möchten.

5. 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

6. Klicken Sie auf **Speichern**.
7. 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 OSDs auswählen

Werden bei der Eingabe von Zeichen auf der Tastatur des Arbeitsplatzes andere Zeichen im On-Screen-Display 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein** und darunter auf den Reiter **CON**.

4. Wählen Sie im Feld **Tastaturlayout** zwischen folgenden Optionen:

<b>Deutsch</b> ( <i>Standard</i> )
<b>Englisch (USA)</b>
<b>Englisch (Großbritannien)</b>
<b>Französisch</b>
<b>Spanisch</b>
<b>lat. Amerikanisch</b>
<b>Portugiesisch</b>

5. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**, falls Sie die Einstellung des lokalen Arbeitsplatzes (am **CPU**-Modul) einstellen möchten.

Klicken Sie auf den Reiter **CON**, falls Sie die Einstellung des entfernten Arbeitsplatzes (am **CON**-Modul) einstellen möchten.

5. Wählen Sie im Feld **USB Auto Refresh** des Abschnitts **Konfiguration** eine der folgenden Optionen:

<b>Aus:</b>	Die angeschlossenen USB-Eingabegeräte erfordern <i>keine</i> Reinitialisierung.
<b>Alle Geräte:</b>	Alle USB-Geräte werden regelmäßig reinitialisiert.
<b>Nur fehlerhafte Geräte:</b>	Der Status der USB-Geräte wird überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, wird dieses Gerät reinitialisiert ( <i>Standardeinstellung</i> ).

6. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**, falls Sie den Bildschirmschoner des lokalen Arbeitsplatzes (am **CPU**-Modul) einstellen möchten.

Klicken Sie auf den Reiter **CON**, falls Sie den Bildschirmschoner des entfernten Arbeitsplatzes (am **CON**-Modul) einstellen möchten.

5. Geben Sie in der Zeile **Bildschirmschoner (Minuten)** die Wartezeit (1 bis 999 Minuten) des Bildschirmschoners ein.

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

6. Klicken Sie auf **Speichern**.

## Fallback-Kompression ein oder ausschalten

Aktivieren Sie die Fallback-Kompression, falls Sie im Falle eines Faserausfalls die Bilddaten komprimiert über die noch aktiven Fasern übertragen möchten.

### So schalten Sie die Fallback-Kompression ein oder 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 **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**.
5. Wählen Sie im Feld **Fallback-Kompression** zwischen folgenden Optionen:

**Aktiviert:** Im Falle eines Faserausfalls werden die Bilddaten *komprimiert* über die noch aktiven Fasern übertragen (*Standard*).

**Deaktiviert:** Die Übertragung der Bilddaten erfolgt immer *unkomprimiert*.

6. Klicken Sie auf **Speichern**.

## Berechtigung für exklusiven Zugriff des Arbeitsplatzes

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** (Vorgabe: **Strg+Druck**) die exklusive Bedienung des KVM-Extenders erreichen.

Nach Betätigung dieser Tastenkombination werden die Eingabegeräte des konkurrierenden Arbeitsplatzes deaktiviert. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**, falls Sie die Berechtigung für den lokalen Arbeitsplatz (am **CPU**-Modul) einstellen möchten.

Klicken Sie auf den Reiter **CON**, falls Sie die Berechtigung für den entfernten Arbeitsplatz (am **CON**-Modul) einstellen möchten.

5. Wählen Sie im Feld **Permanent-Access-Modus** zwischen folgenden Optionen:

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

**Deaktiviert:** Berechtigung für exklusiven Zugriff verweigert

6. Klicken Sie auf **Speichern**.



## Änderung der Videobetriebsart der Arbeitsplätze

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 ausgeschaltet wird, sobald eine Eingabe an einem Arbeitsplatz erfolgt.

Das Bild wird auf dem anderen Arbeitsplatz angezeigt, sobald die Eingaben des Anwenders am Arbeitsplatz abgeschlossen sind.

### So wählen Sie die Videobetriebsart eines Arbeitsplatzes:

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 **Allgemein**.
4. Klicken Sie auf den Reiter **CPU**, falls Sie die Videobetriebsart des lokalen Arbeitsplatz (am CPU-Modul) einstellen möchten.

Klicken Sie auf den Reiter **CON**, falls Sie die Videobetriebsart des entfernten Arbeitsplatz (am CON-Modul) einstellen möchten.

5. Wählen Sie im Feld **Bildanzeige** zwischen folgenden Optionen:

<p><b>immer an</b> (<i>Standard</i>)</p> <p><b>bei Aktionen am entfernten/lokalen Arbeitsplatz aus</b></p>
--

6. Klicken Sie auf **Speichern**.

## Änderung der Zeitspanne der Eingabesperre

Wird an einem Arbeitsplatz eine Eingabe per Tastatur oder Maus durchgeführt, sperrt der KVM-Extender automatisch die Eingabegeräte des konkurrierenden Arbeitsplatzes. 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 0 bis 90 Sekunden eingestellt werden.

<p><b>HINWEIS:</b> Zum Deaktivieren der Funktion geben Sie die Ziffer <b>0</b> ein.</p>
---

### So ändern Sie die Zeitspanne der Eingabesperre:

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 **Allgemein** und darunter auf den Reiter **CPU**.
4. Geben Sie im Feld **Multiuser-Eingabesperre** die gewünschte Zeitspanne der Eingabesperre (0 bis 90 Sekunden) ein.

**HINWEIS:** Der Wert **0** deaktiviert die Eingabesperre.

5. Klicken Sie auf **Speichern**.

### Änderung der Exklusivmodus-Aktionstaste

Nach Betätigung der Tastenkombination für die exklusive Bedienung des Extenders sind die Eingabegeräte des konkurrierenden Arbeitsplatzes deaktiviert. 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-Modifiziertaste (siehe *Änderung der OSD-Taste* auf Seite 55) und einer zusätzlichen *Exklusiv*-Taste, die vom Anwender innerhalb eines vorgegebenen Rahmens frei gewählt werden kann. Sowohl die Hotkey-Modifiziertaste **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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
1. Klicken Sie auf den Reiter **Allgemein** und darunter auf den Reiter **CPU**.
2. Wählen Sie im Feld **Exklusivmodus-Aktionstaste** die gewünschte Taste aus.

Zur Auswahl stehen die Tasten *Backspace*, *Druck*, *Rollen*, *Num*, *Pause*, *Einf.*, *Entf.*, *Pos 1*, *Ende*, *Bild↑*, *Bild↓* und *Space*.

3. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Klicken Sie auf **Neues EDID-Profil anlegen**.
6. Klicken Sie in das Listenfeld **Erlernen** und markieren Sie den Monitor, dessen EDID-Informationen Sie einlesen möchten.

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

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

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

1. Klicken Sie im Menü auf **KVM-Extender**.
2. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Klicken Sie auf **Neues EDID-Profil anlegen**.
6. Klicken Sie auf **Datei auswählen**.
7. Wählen Sie über den Datei-Dialog die zu importierende bin-Datei und klicken Sie auf **Öffnen**.

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

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

**EDID-Profil eines Kanals festlegen**

**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**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **EDID-Profil** des Abschnitts **Videokanal** zwischen folgenden Optionen:

<b>[Auto]:</b>	automatische Behandlung der EDID-Daten (Standard)
<b>Profilname:</b>	Auswahl eines zuvor vom Anwender eingelesenen EDID-Profiles

6. 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**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **Farbtiefe** zwischen folgenden Optionen:

- |                |   |
|----------------|---|
| <b>24 Bit:</b> | Übertragung der Bilddaten mit einer maximalen Farbtiefe von 24 Bit ( <i>Standard</i> ). |
| <b>18 Bit:</b> | Reduzierung der Farbtiefe der Bilddaten auf 18 bit.                                     |

6. 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**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.

5. Wählen Sie im Feld **DDC/CI Monitor** zwischen folgenden Optionen:

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

6. 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. Klicken Sie auf den zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Videokanäle**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **Freeze-Modus** zwischen folgenden Optionen:

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

6. Klicken Sie auf **Speichern**.

## Freeze-Modus-Puffer an bzw. ausschalten

**HINWEIS:** In der Standardeinstellung ist der *Freeze-Modus-Puffer* eingeschaltet.

Im Freeze-Modus (siehe vorangegangenen Abschnitt) gewährleistet der Puffer die Darstellung eines *vollständigen* Bildes bei Verbindungsabbruch. In diesem Modus werden die Videoausgaben verschiedener Extender bzw. Videokanäle *nicht* synchronisiert.

Bei **Deaktivierung** des Puffers kann es im Fall eines Verbindungsabbruchs zur Darstellung eines *unvollständigen* Bildes kommen. In diesem Modus werden die Videoausgaben verschiedener Extender bzw. Videokanäle *synchronisiert*. Auf dicht aneinander stehenden Bildschirmen und auf Split-Screen-Bildschirmen ist so kein zeitlicher Versatz sichtbar.

### So schalten Sie den Freeze-Modus-Puffer an oder 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**.
4. Klicken Sie bei Einsatz eines *Multichannel*-Gerätes auf den gewünschten Videokanal und anschließend auf **Konfiguration**.
5. Wählen Sie im Feld **Freeze-Modus Puffer** zwischen folgenden Optionen:

<b>Mit Puffer:</b>	Der Puffer gewährleistet die Darstellung eines <i>vollständigen</i> Bildes bei Verbindungsabbruch. In diesem Modus werden die Videoausgaben verschiedener Extender bzw. Videokanäle <i>nicht</i> synchronisiert (s. u.).
<b>Ohne Puffer:</b>	Bei Verzicht auf den Puffer kann es im Fall eines Verbindungsabbruchs zur Darstellung eines <i>unvollständigen</i> Bildes kommen!  In diesem Modus werden die Videoausgaben verschiedener Extender bzw. Videokanäle synchronisiert. Auf dicht aneinander stehenden Bildschirmen und auf Split-Screen-Bildschirmen ist so kein zeitlicher Versatz sichtbar.

6. Klicken Sie auf **Speichern**.

## Persönliche Einstellungen

### Anzeige der Informationseinblendung

Informationseinblendungen erfolgen temporär (5 Sekunden) in der linken, oberen Ecke.

**TIPP:** Ist die temporäre Informationseinblendung aktiv, können Sie mit der Tastenkombination **Strg+Feststelltaste** jederzeit eine Wiederholung der Einblendung erreichen.

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:

<b>Aus:</b>	Informationseinblendung ausschalten
<b>Temporär:</b>	temporäre Informationseinblendung für 5 Sekunden ( <i>Standard</i> )
<b>Permanent:</b>	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:

<b>Hoch:</b>	hohes Durchscheinen des Bildschirminhalts
<b>Mittel:</b>	mittleres Durchscheinen des Bildschirminhalts ( <i>Standard</i> )
<b>Niedrig:</b>	leichtes Durchscheinen des Bildschirminhalts
<b>Aus:</b>	überdeckende Darstellung des On-Screen-Displays

5. Klicken Sie auf **Speichern**.

## Farbe der Informationseinblendung ändern

Informationseinblendungen werden standardmäßig in hellgrün angezeigt. Alternativ können Sie eine andere Farbe einstellen.

### 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** zwischen folgenden Optionen:

<b>hellgrün:</b>	Informationseinblendungen in hellgrün darstellen (Standard)
<b>schwarz, dunkelrot, grün, dunkelgelb, dunkelblau, violett, dunkeltürkis, silber, gelb, blau, magenta, helltürkis oder weiß</b>	Informationseinblendungen in der ausgewählten Farbe darstellen

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** 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** zwischen folgenden Optionen:

<b>Ja:</b>	Einsehen und Editieren des eigenen Benutzerprofils erlaubt
<b>Nein:</b>	Einsehen und Editieren des eigenen Benutzerprofils untersagt

5. Klicken Sie auf **Speichern**.

## Berechtigung zum Einsehen und Editieren 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** zwischen folgenden Optionen:

<b>Ja:</b>	Einsehen und Editieren der Gerätekonfiguration erlaubt
<b>Nein:</b>	Einsehen und Editieren der Gerätekonfiguration untersagt

5. Klicken Sie auf **Speichern**.

## 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** des Abschnitts **Globale Extender-Rechte** zwischen folgenden Optionen:

<b>Ja:</b>	Zugriff auf die USB-Geräte erlaubt.
<b>Nein:</b>	Zugriff auf die USB-Geräte untersagt.

5. Klicken Sie auf **Speichern**.

### 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** zwischen folgenden Optionen für jedes aufgelistete Modul:

<b>Ja:</b>	Zugriff auf die USB-Geräte erlaubt.
<b>Nein:</b>	Zugriff auf die USB-Geräte untersagt.

5. Klicken Sie auf **Speichern**.

## 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:

<b>Vollzugriff (grüner Haken):</b>	Vollzugriff auf den am Rechnermodul angeschlossenen Computer erlaubt
<b>Nein (rotes Verbotsschild)</b>	Zugriff auf den am Rechnermodul angeschlossenen Computer untersagt
<b>Ansicht: (Auge-Symbol)</b>	Ansicht des Monitorbildes des am Rechnermodul angeschlossenen Computers erlaubt

5. Klicken Sie auf **Speichern**.

## Berechtigung zur Schaltung der Steckdosen eines Rechnermoduls

So ändern Sie die Berechtigung zur Schaltung der, dem Rechnermodul zugeordneten, Steckdose(n):

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 **Target-Power** des Abschnitts **Individuelle Rechte** zwischen folgenden Optionen für jedes aufgelistete Modul:

<b>Ja:</b>	Schaltung der, dem ausgewählten Rechnermodul zugeordneten, Steckdosen erlaubt
<b>Nein:</b>	Schaltung der, dem ausgewählten Rechnermodul zugeordneten, Steckdosen untersagt

5. Klicken Sie auf **Speichern**.

# 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.
4. Klicken Sie auf **Speichern**.

## Monitoring-Werte konfigurieren

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

### Auswahl der zu überwachenden Monitoring-Werte

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

4. (De)aktivieren Sie die einzelnen Monitoring-Werte in dem Sie den Regler nach *links* schieben (**aus**) oder nach *rechts* schieben (**an**).

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

5. Klicken Sie auf **Speichern**.

## Statusinformationen 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 zu konfigurierenden KVM-Extender und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Informationen**.
4. Im jetzt erscheinenden Dialog werden Ihnen folgende Informationen angezeigt:

KVM-Extender	
<b>Name:</b>	Name des KVM-Extenders
<b>Geräte-ID:</b>	physikalische ID des KVM-Extenders
<b>Status:</b>	aktueller Status ( <b>Online</b> oder <b>Offline</b> ) des KVM-Extenders
<b>Klasse:</b>	Geräteklasse des KVM-Extenders

Hardware-Informationen	
<b>IP-Adresse A:</b>	IP-Adresse der Schnittstelle <i>Network A</i>
<b>MAC A:</b>	MAC-Adresse der Schnittstelle <i>Network A</i>
<b>IP-Adresse B:</b>	IP-Adresse der Schnittstelle <i>Network B</i>
<b>MAC B:</b>	MAC-Adresse der Schnittstelle <i>Network B</i>
<b>Firmware-Name:</b>	Bezeichnung der Firmware
<b>Seriennummer:</b>	Seriennummer des KVM-Extenders
<b>Firmware-Revision:</b>	Firmware-Version
<b>Hardware-Revision:</b>	Hardware-Revision
<b>FPGA-Revision:</b>	FPGA-Revision

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

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

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



# IP-Powerswitch

Durch die Verwendung eines kompatiblen IP-Powerswitches (**ePowerSwitch 1G R2, 4M+ R2** und **8M+ R2**) haben Sie die Möglichkeit, die Stromversorgung von Geräten über den KVM-Extender ein- und auszuschalten.

Hierzu wird ein kompatibler Powerswitch über die **Network**-Schnittstelle angeschlossen. Bevor die Schaltung der Steckdose über das OSD erfolgen kann, ist der Powerswitch in der Webapplikation zum KVM-System hinzuzufügen und zu konfigurieren.

## Konfiguration

### Einen IP-Powerswitch zum KVM-System hinzufügen

**So fügen Sie einen IP-Powerswitch zum KVM-System hinzu:**

1. Klicken Sie im Menü auf **IP-Power-Switches**.
2. Klicken Sie auf **IP-Power-Switch** hinzufügen.
3. Geben Sie im Feld **Name** den gewünschten Namen des Powerswitches ein.
4. Erfassen Sie im Feld **Kommentar** ggf. einen beliebigen Kommentar zum Powerswitch.
5. Klicken Sie auf **Speichern**.

### Änderung von Namen oder Kommentar eines IP-Powerswitches

**So ändern Sie den Namen oder den Kommentar eines IP-Powerswitches:**

1. Klicken Sie im Menü auf **IP-Power-Switches**.
2. Klicken Sie auf den zu konfigurierenden IP-Powerswitch und anschließend auf **Konfiguration**.
3. Ändern Sie im Feld **Name** ggf. den vorgegebenen Namen des Powerswitches.
4. Ändern oder erfassen Sie im Feld **Kommentar** ggf. einen beliebigen Kommentar zum Powerswitch.
5. Klicken Sie auf **Speichern**.

## Einen IP-Powerswitch konfigurieren

Damit der KVM-Extender den Powerswitch steuern kann, ist die Angabe der IP-Adresse und der Zugangsdaten des *Hidden Page Accounts* (s. Installationsanleitung des Powerswitches) des Powerswitches erforderlich.

### So konfigurieren Sie einen IP-Powerswitch:

1. Klicken Sie im Menü auf **IP-Power-Switches**.
2. Klicken Sie auf den zu konfigurierenden IP-Powerswitch und anschließend auf **Konfiguration**.
3. Füllen Sie im Abschnitt **Konfiguration** alle Felder aus.
4. Klicken Sie auf **Speichern**.

## Powerswitch-Steckdose dem KVM-Extender zuordnen

Ist das System mit mindestens einem Powerswitch ausgestattet, können Sie dem KVM-Extender eine oder mehrere Steckdosen zuordnen.

Die zugeordneten Steckdosen können anschließend über das On-Screen-Display der Arbeitsplätze geschaltet werden.

### So ändern Sie die Zuordnung von Powerswitch-Steckdosen des KVM-Extenders:

1. Klicken Sie im Menü auf **IP-Power-Switches**.
2. Klicken Sie auf den zu konfigurierenden IP-Powerswitch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Steckdosen**.

Auf der Reiterkarte werden in der linken Tabelle (**Steckdosen-Index**) alle verfügbaren Powerswitch-Steckdosen angezeigt. In der rechten Tabelle werden alle Rechnermodule (**Target-Module**) aufgelistet.

**HINWEIS:** Die Markierung **Zugeordnet** in der linken Tabelle, kennzeichnet die Powerswitch-Steckdosen, denen ein Rechnermodul zugewiesen ist.

4. Markieren Sie in der *linken* Tabelle die Steckdose, die Sie einem Rechnermodul zuordnen möchten oder dessen Zuordnung Sie entfernen möchten.
5. (De)aktivieren Sie die Zuordnung einer Steckdose zu einem bestimmten Rechnermodul in der rechten Tabelle, in dem Sie den Regler **Zugeordnet** des Rechnermoduls nach *rechts* schieben (*zugeordnet*) oder nach *links* schieben (*nicht zugeordnet*).
6. Klicken Sie auf **Speichern**.

## Einen IP-Powerswitch aus dem KVM-System löschen

Wird ein bereits bekannter Powerswitch durch das KVM-System nicht gefunden, geht das System davon aus, dass das Gerät ausgeschaltet ist.

Löschen Sie einen Powerswitch, der dauerhaft aus dem System entfernt wird, daher manuell aus der Auflistung der Powerswitches.

**HINWEIS:** Es können ausschließlich ausgeschaltete Powerswitches gelöscht werden.

### So löschen Sie einen ausgeschalteten oder vom System getrennten IP-Powerswitch:

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

### Statusinformationen eines IP-Powerswitches einsehen

Über das Kontextmenü eines Powerswitches können Sie einen Dialog mit verschiedenen Statusinformationen aufrufen.

### So können Sie die Statusinformationen eines IP-Powerswitches einsehen:

1. Klicken Sie im Menü auf **IP-Power-Switches**.
2. Klicken Sie auf den zu konfigurierenden IP-Powerswitch und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Information**.

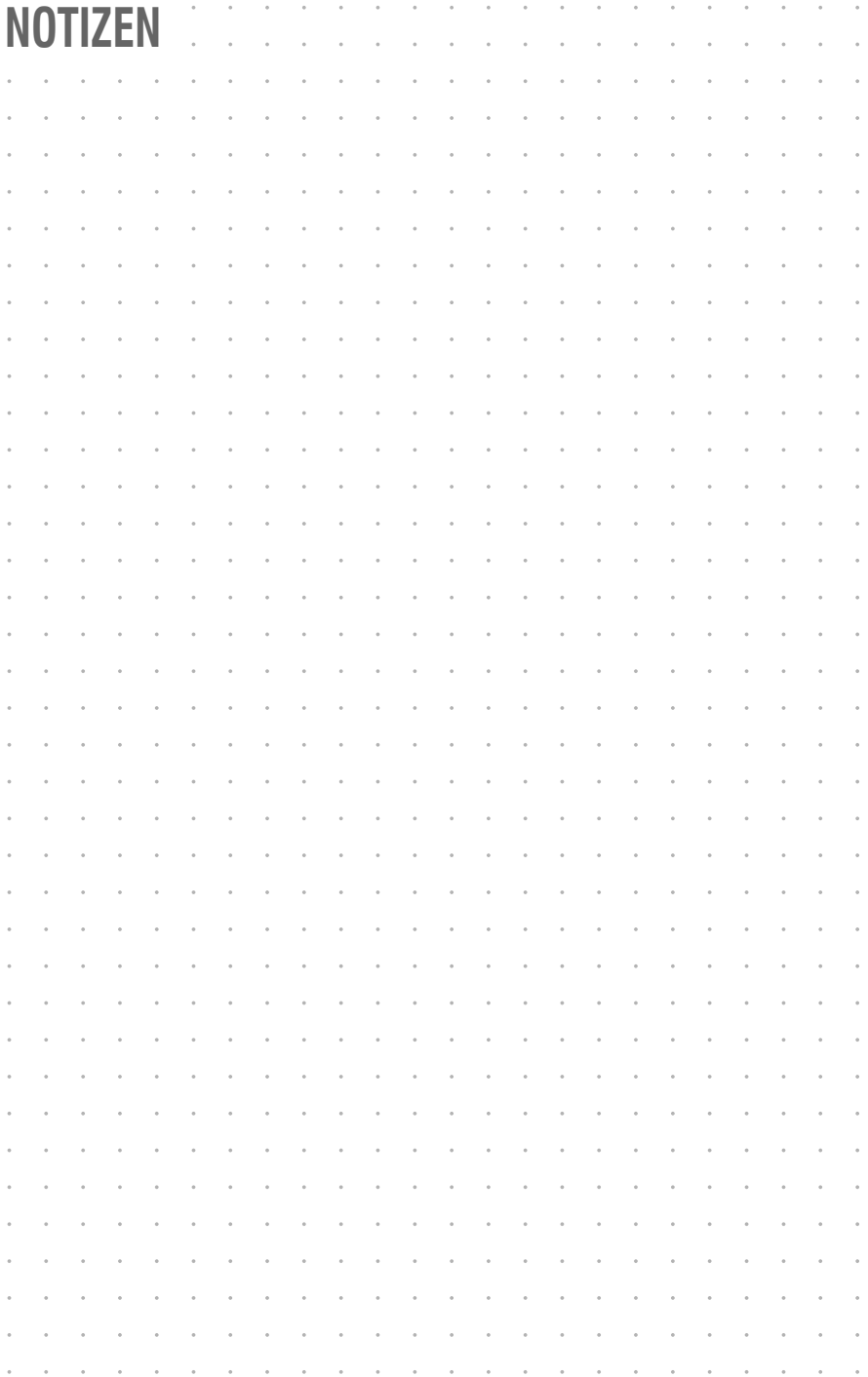
Auf der Reiterkarte werden Ihnen folgende Informationen angezeigt:

<b>Name:</b>	Name des Powerswitches
<b>Status:</b>	aktuellen Status ( <i>Online</i> oder <i>Offline</i> ) des Powerswitches

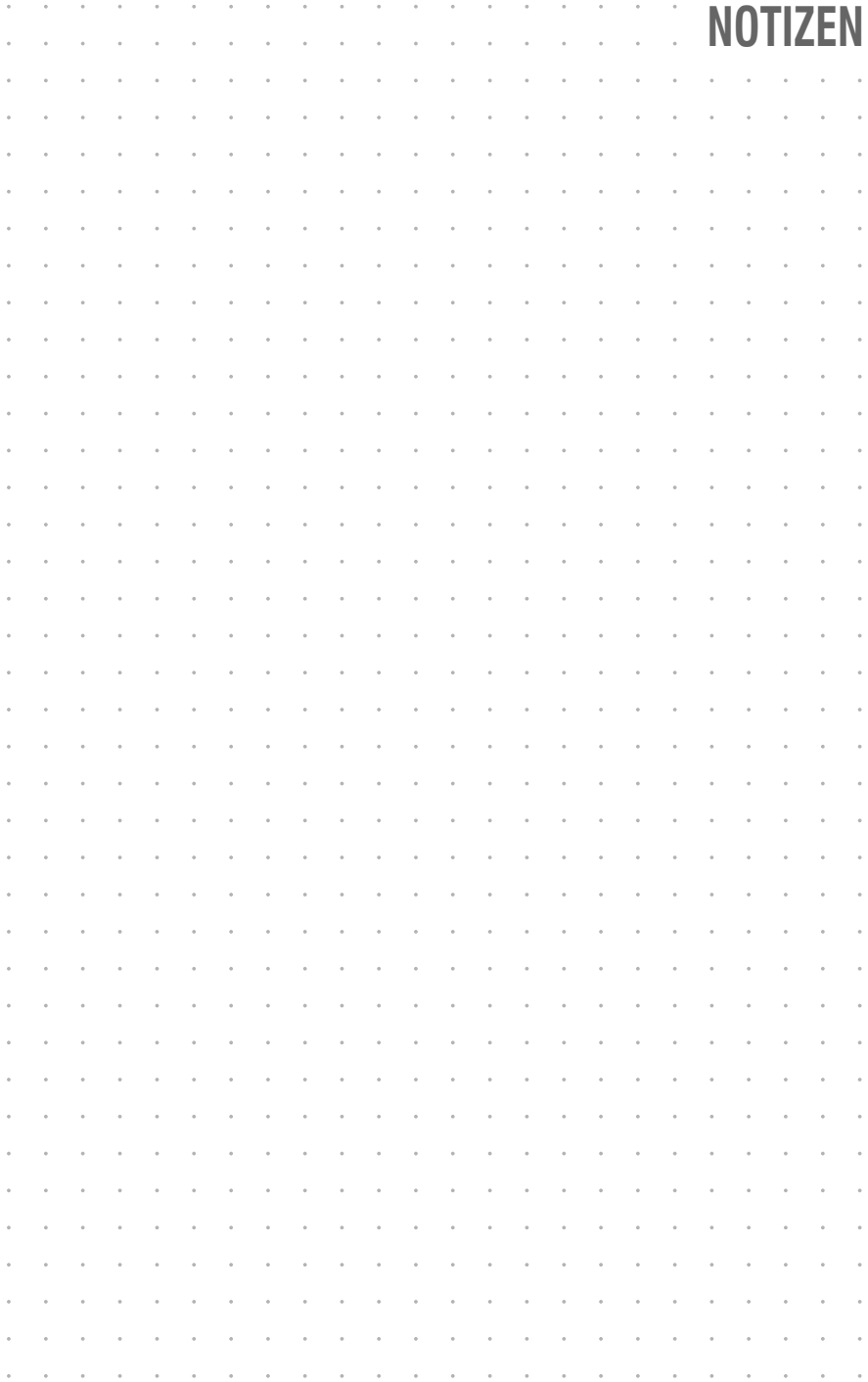
**HINWEIS:** Im Abschnitt *Steckdosen* finden Sie eine Auflistung aller Kanäle des Powerswitches. Der Tabelle kann zudem u. a. entnommen werden, welches Rechnermodul zugeordnet ist.

4. Klicken Sie auf **Speichern**.

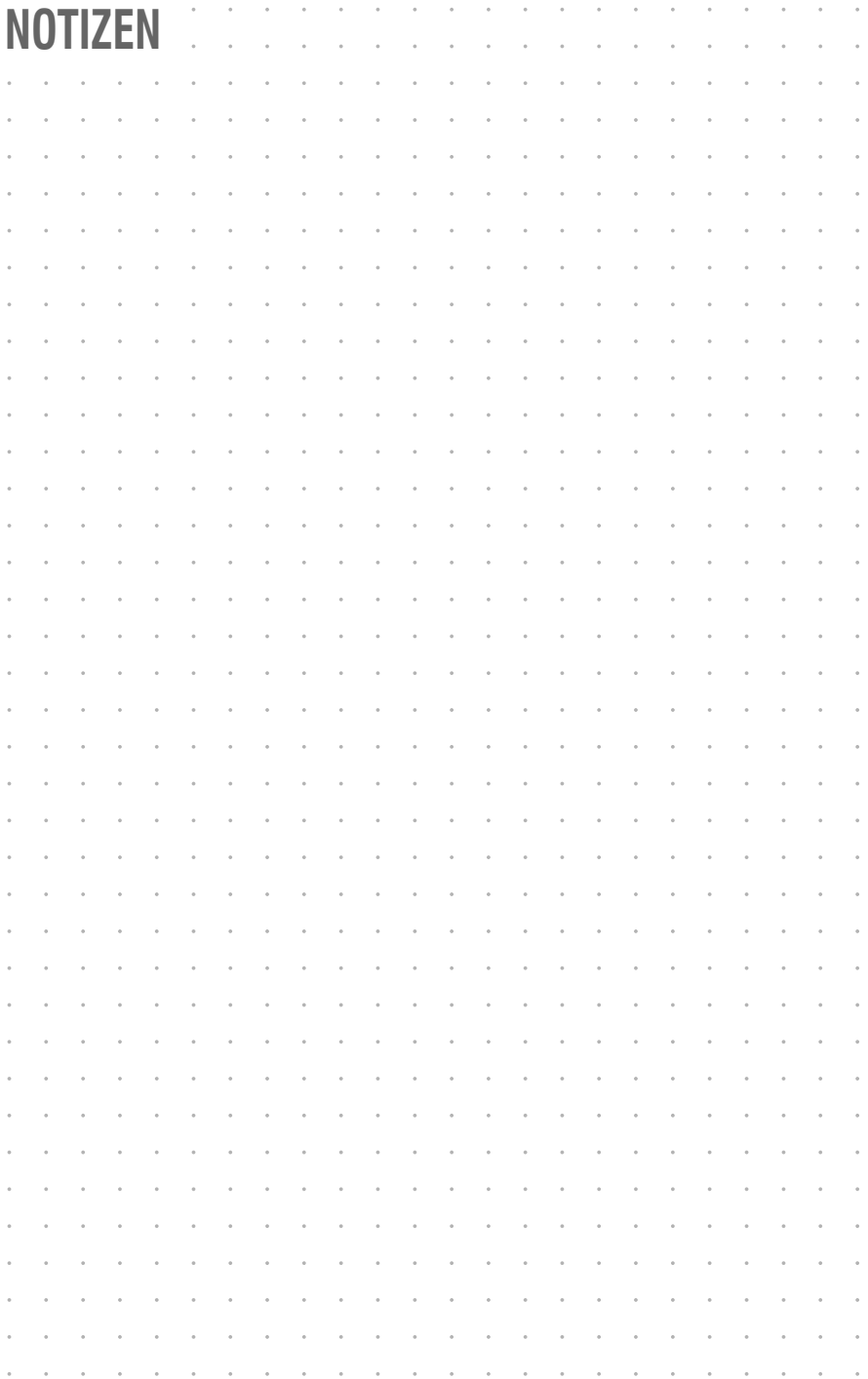
# NOTIZEN



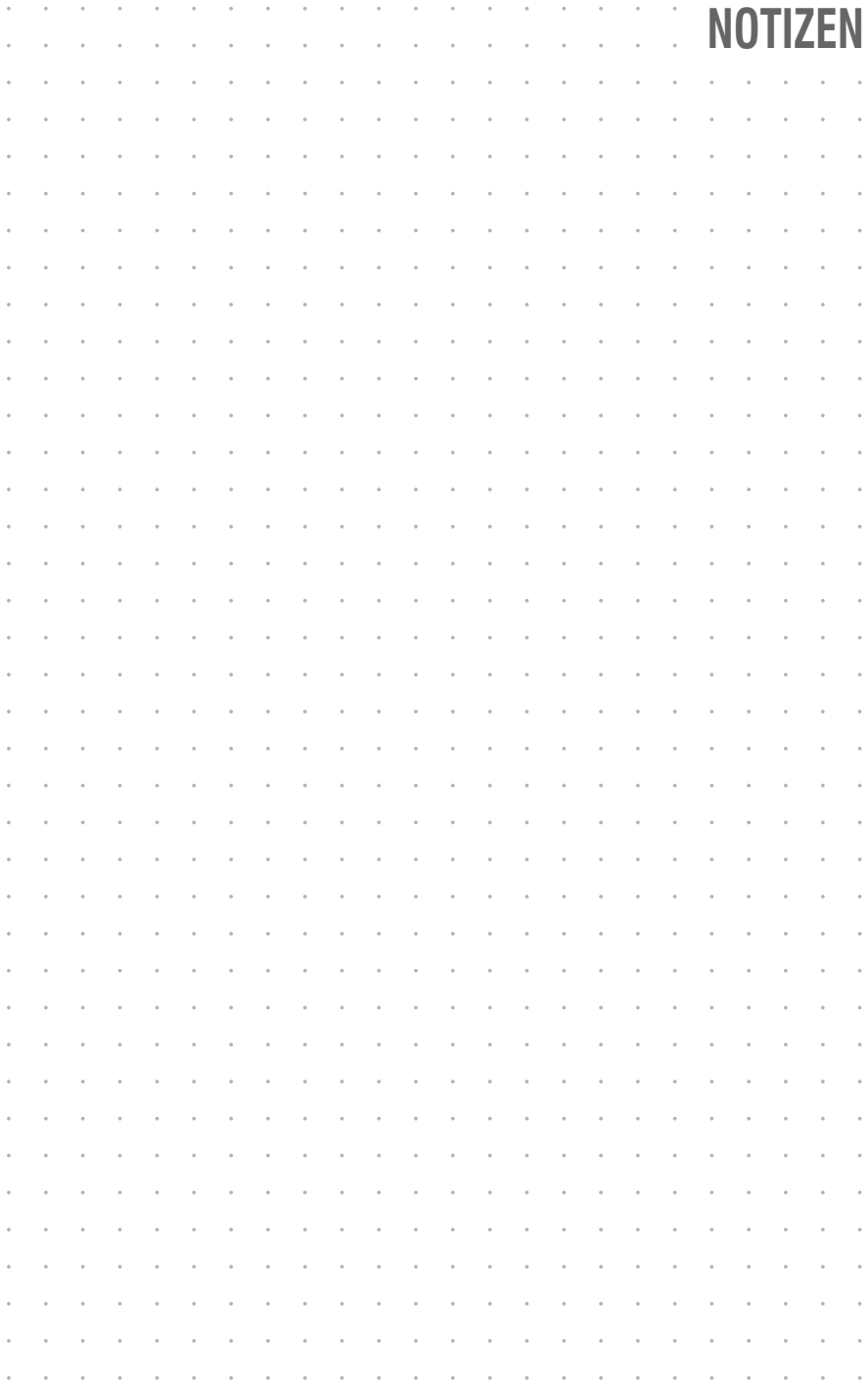
# NOTIZEN



# NOTIZEN



# NOTIZEN





Das Handbuch wird fortlaufend aktualisiert und im Internet veröffentlicht.

<https://gdsys.de/A9100272>

**Guntermann & Drunck GmbH**

Obere Leimbach 9  
57074 Siegen

Germany

<http://www.gdsys.de>  
[sales@gdsys.de](mailto:sales@gdsys.de)