



G&D DP1.2-MUX3-ATC

DE Webapplikation »Config Panel«
Konfiguration des Matrixswitches



The screenshot shows the G&D Config Panel 21 web application interface. The top header includes the G&D logo with the tagline "AND KVM FEELS RIGHT.", the title "G&D Config Panel 21", and the device identifier "DP1.2-MUX3-ATC | MUX 0000082B". On the right, there are buttons for "DE", a user profile icon, and a monitor icon.

The main content area is titled "KVM-Switches" and features a search bar with the text "Suche...". Below the search bar is a table with the following columns: "Name", "Gerätetyp", "Kommentar", and "Monitoring overview". The table contains one entry:

<input checked="" type="checkbox"/> Name *	Gerätetyp	Kommentar	Monitoring overview
<input checked="" type="checkbox"/> MUX 0000082B ⓘ	DP1.2-MUX3-ATC		OK

At the bottom of the interface, there are buttons for "Schalten -", "Service-Werkzeuge -", "Konfiguration", and "Löschen".

Zu dieser Dokumentation

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

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

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

Gewährleistungsausschluss

G&D übernimmt keine Gewährleistung für Geräte, die

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

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

Warenzeichennachweis

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

Impressum

© Guntermann & Drunck GmbH 2025. Alle Rechte vorbehalten.

Version 1.10 – 17.03.2025

Config Panel 21-Version: 1.6.001

Guntermann & Drunck GmbH

Obere Leimbach 9

57074 Siegen

Germany

Telefon +49 (0) 271 23872-0

Telefax +49 (0) 271 23872-120

www.gdsys.com

sales@gdsys.com

Inhaltsverzeichnis

Einleitung	6
Systemvoraussetzungen	7
Unterstützte Betriebssysteme	7
Empfohlene Grafikauflösungen	7
Erstkonfiguration der Netzwerkeinstellungen	8
Erste Schritte	9
Start der Webapplikation	9
Bedienung der Webapplikation	11
Die Benutzeroberfläche.....	11
Häufig verwendete Schaltflächen	13
Tabellenspalten konfigurieren	13
Spracheinstellungen	15
Sprache der Webapplikation auswählen	15
Systemsprache auswählen	15
Sprache für ein bestimmtes Benutzerkonto auswählen	16
Automatisches Logout	17
Anzeigen von Nutzungsbedingungen	18
Passwort-Komplexität	19
Anmeldeoptionen	20
Versionsnummer der Webapplikation anzeigen	21
Webapplikation beenden	21
Kanalumschaltung via EasyControl	22
Start des Umschalt-Tools »EasyControl«	22
Umschalten des aktiven KVM-Kanals	23
Geräte an USB 3.0-Schnittstellen permanent umschalten	24
Farbschema des Umschalt-Tools ändern	24
Umbenennung der Kanal-Kanäle	25
Beenden des Umschalt-Tools »EasyControl«	25
Grundkonfiguration der Webapplikation	26
Netzwerkeinstellungen	26
Konfiguration der Netzwerkschnittstellen.....	26
Konfiguration der globalen Netzwerkeinstellungen.....	28
Ausfallsicherheit der Netzwerkverbindung durch Link-Aggregation erhöhen	29
Status der Netzwerkschnittstellen auslesen	31
Netzfilterregeln einrichten und administrieren	32
Neue Netzfilterregel erstellen	32
Bestehende Netzfilterregel bearbeiten	34
Bestehende Netzfilterregeln löschen	35
Reihenfolge bzw. Priorität der Netzfilterregeln ändern	36

Erstellung eines SSL-Zertifikats	36
Besonderheiten für komplexe KVM-Systeme	37
Erzeugen eines Certificate Authority-Zertifikats	37
Erzeugen eines beliebigen Zertifikats	39
X509-Zertifikat erstellen und signieren	40
PEM-Datei erstellen	41
Auswahl eines SSL-Zertifikats	42
Durchführung von Firmware-Updates	44
Firmware-Update eines bestimmten Geräts	44
Firmware-Update mehrerer Geräte des KVM-Systems	45
Wiederherstellung der Werkseinstellungen	46
Neustart des Gerätes durchführen	46
Netzwerkfunktionen der Geräte	47
NTP-Server	47
Zeitsynchronisation mit einem NTP-Server	47
Manuelle Einstellung von Uhrzeit und Datum	49
Protokollierung von Syslog-Meldungen	50
Lokale Protokollierung der Syslog-Meldungen	51
Versand von Syslog-Meldungen an einen Server	52
Lokale Syslog-Meldung einsehen und speichern	53
Benutzerauthentifizierung mit Verzeichnisdiensten	53
Einrichtung der Zwei-Faktor-Authentifizierung am Gerät (Option)	56
Monitoring-Funktionen	58
Alle Monitoring-Werte einsehen	58
Monitoring-Werte deaktivieren	59
Erweiterte Funktionen zur Verwaltung der kritischen Geräte	60
Auflistung der kritischen Monitoring-Werte einsehen	60
Alarm eines kritischen Gerätes bestätigen	60
Geräteüberwachung via SNMP	61
Praktischer Einsatz des SNMP-Protokolls	61
Konfiguration des SNMP-Agents	61
Hinzufügen und Konfiguration von SNMP-Traps	64
XML-Steuerung des KVM-Switches (Remote-Control)	66
Benutzer und Gruppen	67
Effizienter Einsatz der Rechteverwaltung	67
Das Effektivrecht	67
Effizienter Einsatz der Benutzergruppen	68

Verwaltung von Benutzerkonten	69
Anlegen eines neuen Benutzerkontos	70
Aktivierung der Zwei-Faktor-Authentifizierung (Option)	71
Änderung des Namens eines Benutzerkontos	74
Änderung des Passworts eines Benutzerkontos	75
Änderung der Rechte eines Benutzerkontos	76
Änderung der Gruppenzugehörigkeit eines Benutzerkontos	77
Aktivierung oder Deaktivierung eines Benutzerkontos	78
Löschen eines Benutzerkontos	78
Verwaltung von Benutzergruppen	79
Anlegen einer neuen Benutzergruppe	79
Änderung des Namens einer Benutzergruppe	79
Änderung der Rechte einer Benutzergruppe	80
Mitgliederverwaltung einer Benutzergruppe	81
Aktivierung oder Deaktivierung einer Benutzergruppe	81
Löschen einer Benutzergruppe	81
System-Rechte	82
Berechtigung zum uneingeschränkten Zugriff (Superuser)	82
Berechtigung zum Login in die Webapplikation	82
Berechtigung zum Zugriff auf das EasyControl-Tool	83
Berechtigung zur Änderung des eigenen Passworts	83
Berechtigung zur Bestätigung eines Monitoring-Alarms	83
Erweiterte Funktionen des KVM-Systems	84
Identifizierung eines Gerätes durch Aktivierung der Identification-LED	84
Sicherung der Konfigurationseinstellungen	84
Sicherung der Konfigurationseinstellungen mit der Auto-Backup-Funktion	85
Wiederherstellung der Konfigurationseinstellungen	87
Freischaltung kostenpflichtiger Zusatzfunktionen	88
Grundkonfiguration der KVM-Switches	89
Änderung des Namens eines KVM-Switches	89
Änderung des Kommentares eines KVM-Switches	89
Einen KVM-Switch aus dem KVM-System löschen	90
Konfigurationseinstellungen der KVM-Switches	91
Gerätekonfiguration	91
Betriebsart wählen (OpenAccess bzw. Standard)	91
Änderung des Hotkeys zum Aufruf des On-Screen-Displays (OSD)	92
OSD mit doppeltem Tastendruck starten	93
Änderung der Select-Keys	94
Switching (de)aktivieren	95
Reinitialisierung von USB-Eingabegeräten	96
Änderung des Scancode-Sets einer PS/2-Tastatur	97
DDC/CI-Unterstützung (de)aktivieren	98
Allgemeine OSD-Konfiguration	99
Verwendung des OSD an-/ausschalten	99
OSD-Auflösung einstellen	100
Tastaturlayout für Eingaben innerhalb des OSD auswählen	101

Persönliche Einstellungen (Persönliches Profil)	102
Anzeige der Informationseinblendung	102
Transparenz des OSD einstellen	103
Farbe der Informationseinblendung ändern.....	104
Automatisches Schließen des OSDs (de)aktivieren	105
Standard-Menü-Modus ändern	105
Umschaltswelle für Änderung des Menü-Modus per Maus	106
Verweildauer der Autoscan- bzw. Autoskip-Funktion konfigurieren	107
Step-Keys auswählen	108
Automatisches Umschalten des zuletzt aufgeschalteten Kanals.....	109
Standardaktion nach der Benutzeranmeldung konfigurieren	110
Kanal-Konfiguration	112
Änderung des Namens eines Kanals	112
Änderung des Kommentares eines Kanals	112
Aktivierung/Deaktivierung eines Kanals	113
Aktivierung/Deaktivierung des Tastatur-Signals	114
Unterstützung für Multimedia- und Sondertasten.....	115
Failover-Switching einrichten	116
Videokanal-Konfiguration	117
Änderung des Namens eines Videokanals	117
Änderung des Kommentares eines Videokanals	117
EDID-Profil eines Monitores einlesen.....	118
EDID-Profil eines Kanals festlegen.....	119
EDID-Profil eines Monitores exportieren.....	120
Verwendung des Freeze-Modus.....	121
Aktivierung/Deaktivierung von DisplayPort-Power	122
Erweiterte Funktionen für KVM-Switches	123
Konfigurationseinstellungen übertragen (Gerät ersetzen)	123
Umschaltung des Kanals	123
Monitoring-Werte konfigurieren	124
Auswahl der zu überwachenden Monitoring-Werte.....	124
Rechteverwaltung	125
Berechtigung zum Ändern des persönlichen Profils	125
Zugriffsrecht auf einen KVM-Kanal.....	125
Berechtigung zur Konfiguration des KVM-Switches	126
Zugriff auf USB-Geräte	126
Statusinformationen eines KVM-Switches einsehen	128
Scripting-Funktion	130
Scripts konfigurieren	130
Schritt 1: Option »Scripts« wählen	130
Schritt 2: Scripts anlegen, bearbeiten, zusammenfügen oder löschen	131
Schritt 4: Besitzer festlegen	132
Schritt 5: Script-Verfügbarkeit.....	132
Schritt 6: Ziel-Gerät	133

Script-Gruppen konfigurieren	134
Schritt 1: Option »Script-Gruppen« wählen.....	134
Schritte 2: Script-Gruppen anlegen, bearbeiten oder löschen.....	134
Schritte 3: Script-Gruppe bearbeiten	135
Schritt 4: Scripts zur Gruppe hinzufügen oder aus der Gruppe entfernen	135
Schritt 5: Reihenfolge der Script-Ausführung festlegen	135
Schritt 6: Verfügbarkeit der Script-Gruppe	135
Berechtigung für das Ausführen von Scripts und Script-Gruppen einstellen	136
Ausführungsrecht für ein Script festlegen.....	136
Ausführungsrecht für eine Script-Gruppe festlegen.....	137
Script-Keys konfigurieren und zuordnen	138
Funktion der Script-Keys am Arbeitsplatzmodul	138
Verwaltung der Script-Keys	138
Schritt 1: Gerät auswählen	139
Schritt 2: Scripte zuordnen und Script-Key-Sets editieren	139

1 Grundfunktionen

Einleitung

Die Webapplikation *ConfigPanel* bietet eine grafische Benutzeroberfläche zur Konfiguration des KVM-Systems. Sie kann über einen unterstützten Webbrowser (s. Seite 7) bedient werden.

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

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

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

Systemvoraussetzungen

WICHTIG: Bevor die Webapplikation über den Webbrowser eines Computers gestartet werden kann, ist das Gerät, von welchem die Webapplikation geladen wird, zunächst mit dem lokalen Netzwerk zu verbinden. Weiterführende Informationen finden Sie im Installationshandbuch.

Anschließend sind – sofern nicht bereits erledigt – die auf Seite 8 beschriebenen Netzwerkeinstellungen anzupassen.

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

- Apple Safari 18
- Google Chrome 134
- Microsoft Edge 133
- Mozilla Firefox 136

Unterstützte Betriebssysteme

- Microsoft Windows
- macOS
- Linux
- Android
- iOS

Empfohlene Grafikauflösungen

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

Erstkonfiguration der Netzwerkeinstellungen

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

- IP-Adresse der *Netzwerkschnittstelle 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.

TIPP: Die Erstkonfiguration der Netzwerkschnittstellen des KVM-Switches kann alternativ zu den unten beschriebenen Arbeitsschritten auch über das On-Screen-Display (OSD) des Arbeitsplatzes erledigt werden.

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 26 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 7.

So starten Sie die Webapplikation:

1. Geben in der Adresszeile folgende URL ein:

https://[IP-Adresse des Gerätes]

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

Nutzungsbedingungen zustimmen:	Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren.
<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p>HINWEIS: Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde (siehe <i>Anzeigen von Nutzungsbedingungen</i> ab Seite 18).</p> </div>	
Benutzername:	Geben Sie Ihren Benutzernamen ein.
Passwort:	Geben Sie das Passwort Ihres Benutzerkontos ein.
2-Factor Auth Code (TOTP):	Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
<div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <p>HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 56 ff.) und aktiviert wurde (s. Seite 71 ff.).</p> </div>	

WICHTIG: Ändern Sie das voreingestellte Passwort des Administratorkontos.

Melden Sie sich hierfür mit dem Administratorkonto in der Webapplikation an und ändern Sie anschließend das Passwort (s. Seite 75).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

HINWEIS: Das voreingestellte *Admin*-Passwort von Geräten mit Produktionsdatum vor Oktober 2020 lautet **4658**.

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

HINWEIS: Alternativ zum **Config Panel 21** können Sie nach dem Login das Tool **EasyControl** (s. Seite 22) öffnen.

Bedienung der Webapplikation

Die Benutzeroberfläche

Die Benutzeroberfläche der Webapplikation besteht aus mehreren Bereichen:

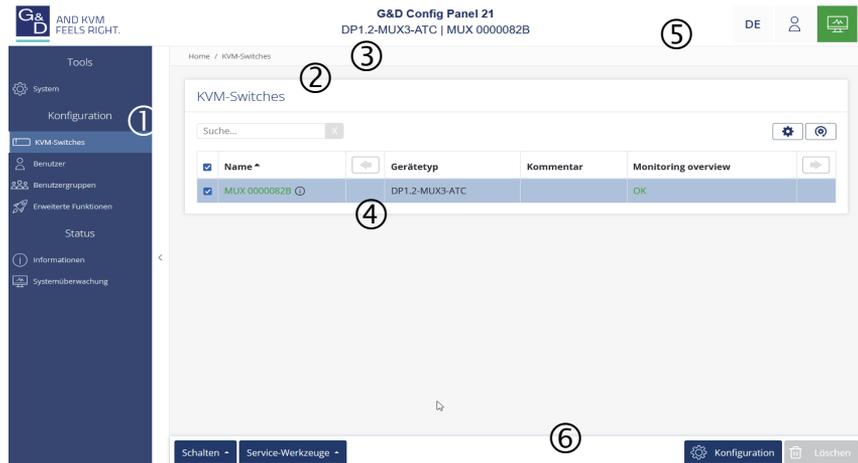


Abbildung 1: Benutzeroberfläche der Webapplikation

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

Menü ①:	Im Menü sind die unterschiedlichen Funktionen der Webapplikation in Themenbereichen zusammengefasst.
Brotkrumen-Navigation ②:	Die Brotkrumennavigation zeigt Ihnen den Pfad zum derzeit geöffneten Dialog an. Um schnell zu einem übergeordneten Dialog zurückzukehren können Sie diesen in der Brotkrumen-Navigation anklicken.
Filterfunktion ③:	Die Filterfunktion kann genutzt werden, um die in der Hauptansicht angezeigten Elemente 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] .
Hauptansicht ④:	Nach der Auswahl eines Themenbereichs im Menü werden hier die Inhalte des Themenbereichs dargestellt.

Schnellzugriffe ⑤

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

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

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

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

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

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

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

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

Schaltflächen ⑥:

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

Häufig verwendete Schaltflächen

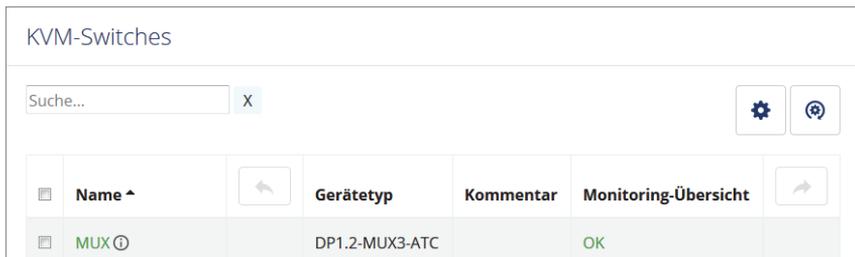
Die Benutzeroberfläche verwendet verschiedene Schaltflächen zur Durchführung von Operationen. Über die Bezeichnungen und Funktionen der in vielen Dialogmasken verwendeten Schaltflächen informiert Sie die folgende Tabelle:

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

Tabellenspalten konfigurieren

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

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



The screenshot shows the 'KVM-Switches' interface. At the top, there is a search bar with the text 'Suche...' and a clear 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 an upward arrow), 'Gerätetyp', 'Kommentar', and 'Monitoring-Übersicht' (with a rightward arrow). The first row of data shows 'MUX' in green text with a downward arrow, 'DP1.2-MUX3-ATC', and 'OK' in green text.

Name ^	Gerätetyp	Kommentar	Monitoring-Übersicht
MUX ↓	DP1.2-MUX3-ATC		OK

Abbildung 2: Tabellenspalten (Auswahl) eines KVM-Switches

So ändern Sie die anzuzeigenden Spalten:

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

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

Tabellen-Konfiguration

Spalten:

Sichtbare Spalten:

Gerätetyp	Kommentar	Monitoring overview
<input type="button" value="←"/> <input type="button" value="✖"/> <input type="button" value="→"/>	<input type="button" value="←"/> <input type="button" value="✖"/> <input type="button" value="→"/>	<input type="button" value="←"/> <input type="button" value="✖"/> <input type="button" value="→"/>

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**.

Spracheinstellungen

Sprache der Webapplikation auswählen

So ändern Sie die Sprache der Webapplikation:

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

A rectangular button with a light gray background and a thin border. Inside the button, the letters 'DE' are displayed in a dark blue, sans-serif font, representing the German language code.

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

Systemsprache auswählen

Die festgelegte *Systemsprache* wird standardmäßig allen Benutzerkonten zugewiesen. Bei Bedarf können Sie jedem Benutzerkonto eine (abweichende) Sprache fest zuordnen.

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

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

So stellen Sie die Systemsprache ein:

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

Sprache für ein bestimmtes Benutzerkonto auswählen

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

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Sprache** zwischen folgenden Optionen:

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

5. Klicken Sie auf **Speichern**.

Automatisches Logout

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

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

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

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

So aktivieren oder deaktivieren Sie die automatische Logout-Funktion:

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

HINWEIS: Wird eine Aktivität des Benutzers festgestellt, wird der Timer zurückgesetzt.

Mit dem Start eines Updatevorgangs über die Webapplikation wird der Timer ebenfalls zurückgesetzt und läuft erst wieder nach Abschluss des Updatevorgangs.

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

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

5. Klicken Sie auf **Speichern**.

Anzeigen von Nutzungsbedingungen

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

So konfigurieren Sie die Anzeige von Nutzungsbedingungen:

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

Aus:	Bei einer Anmeldung werden <i>keine</i> Nutzungsbedingungen angezeigt (<i>Standard</i>).
Benutzerdefiniert:	Bei einer Anmeldung werden <i>individuelle</i> Nutzungsbedingungen angezeigt.

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

Passwort-Komplexität

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

WICHTIG: Änderungen im Bereich der Passwort-Komplexität haben **keinen** Einfluss auf bereits bestehende Passwörter, sondern werden nur bei einer Passwort-Änderung (siehe *Änderung des Passworts eines Benutzerkontos* ab Seite 75) und Anlage eines neuen Benutzerkontos (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 70) berücksichtigt. Daher sollten Sie, falls gewünscht, die Passwort-Komplexität möglichst frühzeitig konfigurieren.

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

So konfigurieren Sie die Passwort-Komplexität:

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

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

9. Klicken Sie auf **Speichern**.

Anmeldeoptionen

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

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

So konfigurieren Sie die Anmeldeoptionen:

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

<p>HINWEIS: Die maximale Anzahl gleichzeitiger Superuser-Sitzungen gilt je Schnittstelle (Gerät/OSD und ConfigPanel).</p>
--

6. Klicken Sie auf **Speichern**.

Versionsnummer der Webapplikation anzeigen

So zeigen Sie die Versionsnummer der Webapplikation an:

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

Webapplikation beenden

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

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

Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die Webapplikation:

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



Kanalumschaltung via EasyControl

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

Alle Benutzer mit der Berechtigung **Config Panel Login** (s. Seite 82) können das Umschalt-Tool verwenden.

Start des Umschalt-Tools »EasyControl«

So starten Sie das Umschalt-Tool:

1. Geben in der Adresszeile folgende URL ein:

https://[IP-Adresse des Gerätes]

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

Nutzungsbedingungen zustimmen:	Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren.
HINWEIS: Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde (siehe <i>Anzeigen von Nutzungsbedingungen</i> ab Seite 18).	
Benutzername:	Geben Sie Ihren Benutzernamen ein.
Passwort:	Geben Sie das Passwort Ihres Benutzerkontos ein.
2-Factor Auth Code (TOTP):	Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 56 ff.) und aktiviert wurde (s. Seite 71 ff.).	

WICHTIG: Ändern Sie das voreingestellte Passwort des Administratorkontos. Melden Sie sich hierfür mit dem Administratorkonto in der Webapplikation an und ändern Sie anschließend das Passwort (s. Seite 75).

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

HINWEIS: Das voreingestellte *Admin*-Passwort von Geräten mit Produktionsdatum vor Oktober 2020 lautet **4658**.

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

Umschalten des aktiven KVM-Kanals

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

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



Abbildung 4: Benutzeroberfläche des Umschalt-Tools »EasyControl«

So schalten Sie auf einen anderen KVM-Kanal um:

- Klicken Sie auf die Schaltfläche des auszuschaltenden Kanals.

Geräte an USB 3.0-Schnittstellen permanent umschalten

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

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

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

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

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

Farbschema des Umschalt-Tools ändern

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

So ändern Sie das anzuwendende Farbschema des Umschalt-Tools:

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

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

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

Umbenennung der Kanal-Kanäle

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

So ändern Sie die Namen der KVM-Kanäle:

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

Beenden des Umschalt-Tools »EasyControl«

So beenden Sie das Umschalt-Tool:

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

Grundkonfiguration der Webapplikation

Netzwerkeinstellungen

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

WICHTIG: Beachten Sie die separaten Anweisungen zur *Erstkonfiguration der Netzwerkeinstellungen* auf Seite 8.

Konfiguration der Netzwerkschnittstellen

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

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

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

So konfigurieren Sie die Einstellungen einer Netzwerkschnittstelle:

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

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

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

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

Betriebsmodus:	Wählen Sie den Betriebsmodus der Schnittstelle A bzw. Schnittstelle B aus: <ul style="list-style-type: none">▪ Aus: Netzwerkschnittstelle ausschalten.▪ Statisch: Es wird eine statische IP-Adresse zugeteilt.▪ DHCP: Bezug der IP-Adresse von einem DHCP-Server.
<p>In der Drop-Down-Liste wird der Text Link-Aggregation aktiv angezeigt, falls die Schnittstelle zu einer Netzwerkschnittstellen-Gruppe hinzugefügt wurde. Konfigurieren Sie die Netzwerkschnittstellen in diesem Fall im Bereich »Link-Aggregation«.</p>	
IP-Adresse:	Geben Sie – nur bei Auswahl des Betriebsmodus <i>Statisch</i> – die IP-Adresse der Schnittstelle an
Netzmaske:	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-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Globale Netzwerkeinstellungen**.
5. Erfassen Sie folgende Daten:

Betriebsmodus:	Wählen Sie den gewünschten Betriebsmodus: <ul style="list-style-type: none">▪ Statisch: Verwendung von statischen Einstellungen.▪ DHCP: Bezug der Einstellungen von einem DHCP-Server.
Host-Name:	Geben Sie den Host-Namen des Gerätes ein. WICHTIG: Falls bei aktiviertem DHCP der DHCP-Server selbst keinen Host-Namen vergibt, wird der hier erfasste Host-Name verwendet. Ansonsten wird der vom DHCP-Server bezogene Host-Name verwendet. Im Betriebsmodus <i>DHCP</i> werden die folgenden Einstellungen automatisch bezogen. Eine Eingabe ist nicht möglich.
Domäne:	Geben Sie die Domäne an, welcher das Gerät angehören soll.
Gateway:	Geben Sie die IP-Adresse des Gateways an.
DNS-Server 1:	Geben Sie die IP-Adresse des DNS-Servers an.
DNS-Server 2:	Geben Sie <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-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Link-Aggregation**.

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

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

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

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

ARP-Validierung:	Die Validierung stellt sicher, dass das ARP-Paket für eine bestimmte Netzwerkschnittstelle von einem der angegebenen ARP-Targets generiert wurde. Wählen Sie, ob bzw. welche der eingehenden ARP-Pakete validiert werden sollen: <ul style="list-style-type: none"> ▪ Keine: Die ARP-Pakete werden nicht validiert (Standard). ▪ Aktiv: Ausschließlich die ARP-Pakete der aktiven Netzwerkschnittstelle werden validiert. ▪ Backup: Ausschließlich die ARP-Pakete der inaktiven Netzwerkschnittstelle werden validiert. ▪ Alle: Die ARP-Pakete aller Netzwerkschnittstellen der Gruppe werden validiert.
ARP-Target:	Die Tabelle enthält eine Liste aller konfigurierten ARP-Targets. Verwenden Sie die Schaltflächen Hinzufügen , Ändern und Löschen , um die ARP-Targets zu verwalten.

7. Klicken Sie auf **Speichern**.

Status der Netzwerkschnittstellen auslesen

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

So ermitteln Sie den Status der Netzwerkschnittstellen:

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

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

6. Klicken Sie auf **Speichern**.

Netzfilterregeln einrichten und administrieren

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

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

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

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

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

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

Neue Netzfilterregel erstellen

So erstellen Sie eine neue Netzfilterregel:

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

Schnittstelle: Wählen Sie im Pull-Down-Menü aus, auf welchen Netzwerkschnittstellen die Datenpakete abgefangen und manipuliert werden sollen:

- **Alle**
- **Schnittstelle A**
- **Schnittstelle B**
- **Link-Aggregation group**

Option:	Wählen Sie im Pull-Down-Menü aus, wie die Absenderinformation der Regel zu interpretieren ist: <ul style="list-style-type: none"> ▪ Normal: Die Regel gilt für Datenpakete, deren Absenderinformation der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht. ▪ Invertiert: Die Regel gilt für Datenpakete, deren Absenderinformation <i>nicht</i> der in der Regel angegebenen IP-Adresse bzw. MAC-Adresse entspricht.
IP-Adresse/ Netzmaske:	Geben Sie die IP-Adresse der Datenpakete oder – durch Verwendung des Feldes Netzmaske – den Adressraum der IP-Adressen ein. <p>Beispiele:</p> <ul style="list-style-type: none"> ▪ 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 <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>HINWEIS: Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p> </div>
MAC-Adresse:	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>HINWEIS: Innerhalb einer Regel können wahlweise die <i>IP-Adresse</i> und/oder eine <i>MAC-Adresse</i> angegeben werden.</p> </div>
Filterregel:	<ul style="list-style-type: none"> ▪ Drop: Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden <i>nicht</i> verarbeitet. ▪ Accept: Datenpakete, deren Absenderinformation mit der IP-Adresse bzw. MAC-Adresse übereinstimmt, werden verarbeitet.
Service:	Wählen Sie einen bestimmten Service, für den diese Regel exklusiv angewendet wird oder wählen Sie (Alle).

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

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

7. Klicken Sie auf **Speichern**.

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

Bestehende Netzfilterregel bearbeiten

So bearbeiten Sie eine bestehende Netzfilterregel:

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

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

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

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

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

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

Bestehende Netzfilterregeln löschen

So löschen Sie bestehende Netzfilterregeln:

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

Reihenfolge bzw. Priorität der Netzfilterregeln ändern

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

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

So ändern Sie die Reihenfolge/Priorität der bestehenden Netzfilterregeln:

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

Erstellung eines SSL-Zertifikats

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

WICHTIG: Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkkertifikate für die Webapplikation (s. Seite 36 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

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

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

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

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

Besonderheiten für komplexe KVM-Systeme

Falls innerhalb eines KVM-Systems verschiedene G&D-Geräte miteinander kommunizieren sollen, ist bei der Erstellung von Zertifikaten für diese Geräte das identische *Certificate Authority*-Zertifikat (s. Seite 37) zu verwenden.

Alternativ kann bei allen Geräten auch die identische PEM-Datei (s. Seite 41) 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 Zertifikatswiderruf erforderlich.
4. Jetzt wird das Zertifikat erstellt und unter dem Dateinamen *server.csr* gespeichert.

X509-Zertifikat erstellen und signieren

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

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

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

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

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

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

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

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

PEM-Datei erstellen

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

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

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

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

a. Linux

```
cat server.crt > gcdcd.pem
cat server.key >> gcdcd.pem
cat ca.crt >> gcdcd.pem
```

b. Windows

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

2. Durch die Kopieroperation(en) wird die Datei *gcdcd.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 37) verwenden, können die Geräte mit-einander kommunizieren.

So wählen Sie das zu verwendende SSL-Zertifikat:

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

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

5. Wählen Sie das zu verwendende Zertifikat aus:

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

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

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

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

Übertragen und aktivieren Sie anschließend das gewünschte Zertifikat:

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

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

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

6. Klicken Sie auf **Speichern**.

WICHTIG: Aus sicherheitsrelevanten Gründen sind in einem Backup Netzwerkzertifikate für die Webapplikation (s. Seite 36 ff.) und gegebenenfalls zusätzliche Benutzerzertifikate für die KVM-Verbindung **nicht** enthalten und müssen gegebenenfalls nach einem Restore erneut hinterlegt werden.

Durchführung von Firmware-Updates

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

Firmware-Update eines bestimmten Geräts

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

So aktualisieren Sie die Firmware eines bestimmten Geräts:

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

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

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

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

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

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

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

Firmware-Update mehrerer Geräte des KVM-Systems

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

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

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

4. Klicken Sie auf **Firmware-Dateien bereitstellen**.

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

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

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

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

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

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

WICHTIG: Schließen Sie **nicht** die Browser-Session, während die Geräte aktualisiert werden! Schalten Sie die Produkte während dem Update **nicht** aus, und trennen Sie sie **nicht** von der Stromversorgung.

Wiederherstellung der Werkseinstellungen

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

So stellen Sie die Werkseinstellungen wieder her:

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

Alle Einstellungen zurücksetzen:	Alle Einstellungen des Gerätes zurücksetzen.
Nur Einstellungen des lokalen Netzwerkes zurücksetzen:	Ausschließlich die lokalen Netzwerkeinstellungen zurücksetzen.
Nur Einstellungen der KVM-Anwendungen zurücksetzen:	Alle Einstellungen außer den lokalen Netzwerkeinstellungen zurücksetzen.

4. Klicken Sie auf **Werkseinstellungen**.

Neustart des Gerätes durchführen

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

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

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

Netzwerkfunktionen der Geräte

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

Für 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 61 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-Switches**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.

4. Wählen Sie den Bereich **NTP-Server** und erfassen Sie folgende Daten:

Allgemein	
NTP-Zeitsynchronisation:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Zeitsynchronisation aus- und einschalten: <ul style="list-style-type: none">▪ Deaktiviert (<i>Standard</i>)▪ Aktiviert
Zeitzone:	Wählen Sie aus dem Pull-Down-Menü die Zeitzone Ihres Standorts aus.
NTP-Server 1	
Adresse:	Geben Sie die Adresse eines Zeitserver ein.
Authentifizierung:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Authentifizierung aus- und einschalten: <ul style="list-style-type: none">▪ Deaktiviert (<i>Standard</i>)▪ SHA1
Schlüssel-ID:	Geben Sie nach Aktivierung der Authentifizierung die Schlüssel-ID ein, die für die Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann.
Schlüssel	Geben Sie den Schlüssel in Form von bis zu 40 Hexadezimalstellen ein.
NTP-Server 2	
Adresse:	Geben Sie <i>optional</i> die Adresse eines zweiten Zeitserver ein.
Authentifizierung:	Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü können Sie die Authentifizierung aus- und einschalten: <ul style="list-style-type: none">▪ Deaktiviert (<i>Standard</i>)▪ SHA1
Schlüssel-ID:	Geben Sie nach Aktivierung der Authentifizierung die Schlüssel-ID ein, die für die Schlüsselauthentifizierung mit dem NTP-Server verwendet werden kann.
Schlüssel	Geben Sie den Schlüssel in Form von bis zu 40 Hexadezimalstellen ein.

5. Klicken Sie auf **Speichern**.

Manuelle Einstellung von Uhrzeit und Datum

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

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

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

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

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

7. Klicken Sie auf **Speichern**.

Protokollierung von Syslog-Meldungen

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

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

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

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

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

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

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

Lokale Protokollierung der Syslog-Meldungen

So konfigurieren Sie die lokale Protokollierung von Syslog-Meldungen:

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

Syslog lokal:	<p>Durch Auswahl des entsprechenden Eintrags im Pull-Down-Menü schalten Sie die lokale Protokollierung von Syslog-Meldungen aus oder ein:</p> <ul style="list-style-type: none"> ▪ Deaktiviert ▪ Aktiviert (<i>Standard</i>)
Log-Level:	<p>Wählen Sie in diesem Pull-Down-Menü aus, ab welchem Schweregrad eine Log-Meldung zu protokollieren ist (<i>Standard: 6 - Info</i>).</p> <p>Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.</p>
<p>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.</p>	

5. Klicken Sie auf **Speichern**.

Versand von Syslog-Meldungen an einen Server

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

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

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

5. Klicken Sie auf **Speichern**.

Lokale Syslog-Meldung einsehen und speichern

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

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

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

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

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

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

Benutzerauthentifizierung mit Verzeichnisdiensten

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WICHTIG: Bei Verwendung der Zwei-Faktor-Authentifizierung (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät (Option)* ab Seite 56) kann der Fallback-Mechanismus **nicht** genutzt werden.

So konfigurieren Sie die Authentifizierung von Benutzerkonten:

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

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

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

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

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

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

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

HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 70).

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

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

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

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

WICHTIG: Bei Verwendung der Zwei-Faktor-Authentifizierung (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät (Option)* auf Seite 56) kann der Fallback-Mechanismus **nicht** genutzt werden.

6. Klicken Sie auf **Speichern**.

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

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

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

WICHTIG: Wenn Sie keinen Zugriff auf Ihren besitzbasierten Faktor mehr haben oder er kaputt geht, verlieren Sie den Zugang zum System. Sorgen Sie für diesen Fall vor, indem Sie z. B. bei Verwendung des internen OTP-Servers die Notfall-Codes geschützt an einem sicheren Ort aufbewahren und die Einstellungen so wählen, dass das Risiko eines Zugriffsverlusts minimiert wird (siehe *Aktivierung der Zwei-Faktor-Authentifizierung (Option)* ab Seite 71).

So aktivieren Sie die 2FA am Gerät:

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

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

2FA-Unterstützung:	<ul style="list-style-type: none"> ▪ Deaktiviert (<i>Standard</i>) ▪ Aktiviert
OTP-Server:	<p>Wählen Sie die Option Intern (<i>Standard</i>), wenn ein interner, im Gerät bereitgestellter Authentifizierungsserver zum Einsatz kommen soll.</p> <p>Möchten Sie einen bestimmten externen Verzeichnisdienst nutzen, wählen Sie den entsprechenden Eintrag aus dem Pull-Down-Menü aus:</p> <ul style="list-style-type: none"> ▪ LDAP ▪ Active Directory ▪ Radius ▪ TACACS+ <p>Erfassen Sie nach der Auswahl eines externen Verzeichnisdienstes die Einstellungen des Verzeichnisdienst-Servers in der sich öffnenden entsprechenden Dialogmaske.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe <i>Anlegen eines neuen Benutzerkontos</i> ab Seite 70).</p> </div>
Login nur für Benutzer mit konfigurierter 2FA:	<p>Kommt der interne OTP-Server zum Einsatz, kann festgelegt werden, ob ein Login von Benutzern ohne eine aktivierte 2FA zulässig ist (<i>Standard</i>) oder verhindert werden soll. Mit dieser Option kann z. B. eine Übergangszeit zur Einrichtung der OTPs ermöglicht werden.</p> <ul style="list-style-type: none"> ▪ Nein (<i>Standard</i>) ▪ Ja <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>WICHTIG: Kommt ein externer Verzeichnisdienst zum Einsatz wird für jedes Benutzerprofil der zweite Faktor beim Login verlangt.</p> </div>

6. Klicken Sie auf **Speichern**.

WICHTIG: Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 47). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 49).

Informationen zur Aktivierung der Zwei-Faktor-Authentifizierung finden Sie auf Seite 71 ff.

Monitoring-Funktionen

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

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

KVM-Switches

Suche... X  

<input type="checkbox"/>	Name ^		Status	Main power	Temperature	
<input type="checkbox"/>	MUX ⓘ		Online	On	34.0	

Abbildung 5: Detailansicht einer exemplarischen Monitoring-Tabelle

Die, für die Tabellenansicht (siehe *Tabellenspalten konfigurieren* auf Seite 13) konfigurierten Werte, werden in der Tabelle aufgelistet.

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

Alle Monitoring-Werte einsehen

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

So öffnen Sie die Liste aller Monitoring-Werte:

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

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

4. Klicken Sie auf **Schließen**.

Monitoring-Werte deaktivieren

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

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

WICHTIG: Zu deaktivierten Monitoring-Werten erscheinen *keine* Warnungen in der Webapplikation und es werden *keine* SNMP-Traps hierzu versendet!

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

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

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

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

Erweiterte Funktionen zur Verwaltung der kritischen Geräte

Das Icon **Monitoring-Status** (siehe *Die Benutzeroberfläche* auf Seite 11) zeigt Ihnen auf den ersten Blick, ob alle Monitoringwerte im Normbereich sind (grünes Icon) oder mindestens ein Monitoring-Wert auffällig ist (gelbes oder rotes Icon).

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

Auflistung der kritischen Monitoring-Werte einsehen

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

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

Alarm eines kritischen Gerätes bestätigen

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

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

So bestätigen Sie die Monitoring-Meldungen eines Gerätes:

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

Geräteüberwachung via SNMP

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

Praktischer Einsatz des SNMP-Protokolls

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

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

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

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

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

Konfiguration des SNMP-Agents

So konfigurieren Sie den SNMP-Agent:

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

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

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

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

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

Access:	Aktivieren Sie den lesenden Zugriff (View) oder verweigern Sie den Zugriff (No) über das <i>SNMPv3</i> -Protokoll.
Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem <i>Network Management System</i> an.
Authentifizierungsprotokoll:	Wählen Sie das im <i>Network Management System</i> aktivierte Authentifizierungs-Protokoll aus: <ul style="list-style-type: none"> ▪ SHA-1 ▪ SHA-224 ▪ SHA-256 ▪ SHA-384 ▪ SHA-512 (Standard) ▪ MD5. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>HINWEIS: Da inzwischen bekannt ist, dass MD5 keine Kollisionsresistenz bietet, wird von der Verwendung abgeraten.</p> </div>
Authentifizierungspasswort:	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem <i>Network Management System</i> an.
Security-Level:	Wählen Sie zwischen einer der folgenden Optionen: <ul style="list-style-type: none"> ▪ noAuthNoPriv: Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll deaktiviert ▪ authNoPriv: Benutzer-Authentifizierung aktiviert, <i>Privacy</i>-Protokoll deaktiviert ▪ authPriv: Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll aktiviert
Privacy-Protokoll:	Wählen Sie das im <i>Network Management System</i> aktivierte Privacy-Protokoll aus: <ul style="list-style-type: none"> ▪ AES128 ▪ AES192 ▪ AES256 (Standard) ▪ DES. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>HINWEIS: Aufgrund der geringen Schlüssellänge von DES wird von der Verwendung abgeraten.</p> </div>
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem <i>Network Management System</i> an.

Engine-ID-Methode:	<p>Wählen Sie, nach welcher Methode die <i>SnmpEngineID</i> vergeben werden soll:</p> <ul style="list-style-type: none"> ▪ Random: Die <i>SnmpEngineID</i> wird bei jedem Neustart des Gerätes neu vergeben. ▪ Fix: Die <i>SnmpEngineID</i> entspricht der MAC-Adresse der ersten Netzwerkschnittstelle des Gerätes. ▪ User: Der im Feld <i>Engine-ID</i> eingetragene String wird als <i>SnmpEngineID</i> verwendet.
Engine-ID	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**.

Hinzufügen und Konfiguration von SNMP-Traps

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

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

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

Log-Level:	Wählen Sie den Schweregrad eines Ereignisses aus, ab welchem ein SNMP-Trap zu versenden ist. Der von Ihnen ausgewählte Schweregrad sowie alle niedrigeren Schweregrade werden protokolliert.
HINWEIS: Wählen Sie den Schweregrad <i>2-Kritisch</i> , so werden bei Ereignissen dieses, wie auch der Schweregrade <i>1-Alarm</i> und <i>0-Notfall</i> , SNMP-Traps ausgesendet.	
Version:	Wählen Sie, ob die Traps gemäß der Protokollversion <i>SNMPv2c (v2c)</i> oder <i>SNMPv3 (v3)</i> erstellt und versendet werden.
Benachrichtigungsart:	Wählen Sie, ob die Ereignisse als <i>Trap-</i> oder <i>Inform-Paket</i> versendet werden.
HINWEIS: <i>Inform-Pakete</i> erfordern eine Bestätigung des <i>Network Management Systems</i> . Liegt diese nicht vor, wird die Übertragung wiederholt.	

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

WICHTIG: Das Passwort (<i>Community</i>) der Pakete der Protokollversion <i>SNMPv2c</i> wird unverschlüsselt übertragen und kann daher leicht abgehört werden! Verwenden Sie ggf. die Protokollversion <i>SNMPv3</i> (s. u.) und einen hohen <i>Security-Level</i> , um eine sichere Übertragung der Daten zu erreichen.	
--	--

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

Benutzername:	Geben Sie den Benutzernamen für die Kommunikation mit dem <i>Network Management System</i> an.
Authentifizierungsprotokoll:	Wählen Sie das im <i>Network Management System</i> aktivierte Authentifizierungs-Protokoll aus: <ul style="list-style-type: none"> ▪ SHA-1 ▪ SHA-224 ▪ SHA-256 ▪ SHA-384 ▪ SHA-512 ▪ MD5 (Standard)
HINWEIS: Da inzwischen bekannt ist, dass MD5 keine Kollisionsresistenz bietet, wird von der Verwendung abgeraten.	
Authentifizierungspasswort:	Geben Sie das Authentifizierungs-Passwort für die Kommunikation mit dem <i>Network Management System</i> an.

Security-Level:	Wählen Sie zwischen einer der folgenden Optionen: <ul style="list-style-type: none">▪ noAuthNoPriv: Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll deaktiviert▪ authNoPriv: Benutzer-Authentifizierung aktiviert, <i>Privacy</i>-Protokoll deaktiviert▪ authPriv: Benutzer-Authentifizierung und <i>Privacy</i>-Protokoll aktiviert
Privacy-Protokoll:	Wählen Sie das im <i>Network Management System</i> aktivierte Privacy-Protokoll aus: <ul style="list-style-type: none">▪ AES128▪ AES192▪ AES256▪ DES (Standard).
HINWEIS: Aufgrund der geringen Schlüssellänge von DES wird von der Verwendung abgeraten.	
Privacy-Passwort:	Geben Sie das Privacy-Passwort für die gesicherte Kommunikation mit dem <i>Network Management System</i> an.
Engine-ID:	Geben Sie die <i>Engine-ID</i> des Trap-Receiver ein.

8. Klicken Sie auf **Speichern**.

So löschen Sie einen vorhandenen Trap:

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

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

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

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

Benutzer und Gruppen

Effizienter Einsatz der Rechteverwaltung

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

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

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

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

Das Effektivrecht

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

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

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

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

Recht	Benutzer <i>Muster</i>	Gruppe <i>Office</i>	Gruppe <i>Geräte- konfiguration</i>	Effektivrecht
Config Panel Login	Nein	Ja	Ja	Ja
Eigenes Pass- wort ändern	Nein	Ja	Nein	Ja
CPU-Zugriff	Ja	Ansicht	Nein	Ja

Das Effektivrecht der Rechte *Config Panel Login* und *Eigenes Passwort ändern* resultieren aus den Rechten der Benutzergruppen. Das Recht *CPU-Zugriff* wurde hingegen direkt im Benutzerkonto vergeben. In den Dialogmasken der Webapplikation wird hinter jeder Einstellung zusätzlich das Effektivrecht angezeigt.

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

Effizienter Einsatz der Benutzergruppen

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

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

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

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

BEISPIEL: Sollen einige Benutzer der Gruppe *Office* die Berechtigung zur *Gerätekonfiguration* erhalten, bieten sich folgende Möglichkeiten an, dies mit Benutzergruppen zu realisieren:

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

In beiden Fällen erhält der Benutzer durch die Gruppen das Effektivrecht *Ja* für die *Gerätekonfiguration*.

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

Verwaltung von Benutzerkonten

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

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

Anlegen eines neuen Benutzerkontos

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

WICHTIG: Falls individuelle Passwort-Richtlinien berücksichtigt werden sollen, müssen Sie die Konfiguration der Passwort-Komplexität vor der Anlage eines neuen Benutzerkontos vornehmen (siehe *Passwort-Komplexität* auf Seite 19).

So erstellen Sie ein neues Benutzerkonto:

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

Name:	Geben Sie den gewünschten Benutzernamen ein.
HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe <i>Benutzerauthentifizierung mit Verzeichnisdiensten</i> ab Seite 53).	
Passwort:	Geben Sie das Passwort des Benutzerkontos ein.
Passwort bestätigen:	Wiederholen Sie das oben eingegebene Passwort.
Klartext:	Aktivieren Sie ggf. dieses Kontrollkästchen, um die beiden eingegebenen Passwörter im Klartext sehen und prüfen zu können.
Vollständiger Name:	Geben Sie hier – falls gewünscht – den vollständigen Namen des Benutzers ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Benutzerkonto.
Aktiviert:	Aktivieren Sie dieses Kontrollkästchen, um das Benutzerkonto zu aktivieren.
HINWEIS: Ist das Benutzerkonto deaktiviert, wird dem Benutzer der Zugriff auf das KVM-System verweigert.	

4. Klicken Sie auf **Speichern**.

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

5. Falls die Zwei-Faktor-Authentifizierung am Gerät aktiviert ist (s. Seite 56), sind im Folgenden die Einstellungen für das Benutzerkonto vorzunehmen (s. Seite 71).

Aktivierung der Zwei-Faktor-Authentifizierung (Option)

HINWEIS: Für die Verwendung der optionalen Zwei-Faktor-Authentifizierung (2FA) muss zunächst die Einrichtung am Gerät erfolgen (s. Seite 56).

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

WICHTIG: Kommt ein externer Verzeichnisdienst zum Einsatz (siehe *Einrichtung der Zwei-Faktor-Authentifizierung am Gerät (Option)* ab Seite 56), wird für jedes Benutzerprofil innerhalb der Datenbank die 2FA automatisch aktiviert. Somit ist ein Login am Gerät nur möglich, sofern der externe OTP-Server die identischen Benutzerprofile bereithält und den zweiten Faktor erfolgreich validiert.

WICHTIG: Um die 2FA für ein Benutzerprofil zu aktivieren oder zu deaktivieren, benötigt der Anwender Superuser-Rechte (s. Seite 82), oder der Anwender muss mit dem entsprechenden Benutzerprofil angemeldet sein (s. Seite 82) und über das Recht *Eigenes Passwort ändern* (s. Seite 83) verfügen.

WICHTIG: Verwenden Sie die Zeitsynchronisation mit einem NTP-Server (s. Seite 47). Alternativ können Sie die Uhrzeit und das Datum manuell einstellen (s. Seite 49).

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

So aktivieren Sie die 2FA im Benutzerkonto:

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

5. Erfassen Sie im Menü folgende Daten:

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

6. Klicken Sie auf **Speichern**.

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

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

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

Der 2-Faktor-Authentifizierungscode (TOTP) wird über den konfigurierten, externen OTP-Server validiert.

Ändern Sie ggf. die Rechte dieses speziellen Benutzerkontos, um die Berechtigung von Benutzern ohne eigenes Konto einzustellen (siehe *Änderung der Rechte eines Benutzerkontos* ab Seite 76).

Deaktivieren Sie den Benutzer *RemoteAuth*, um die Anmeldung von Benutzern ohne eigenes Benutzerkonto im KVM-System zu verhindern (siehe *Aktivierung oder Deaktivierung eines Benutzerkontos* auf Seite 78).

Nachdem die 2FA im Benutzerkonto erfolgreich aktiviert wurde, wird beim Login (siehe *Start der Webapplikation* auf Seite 9) zusätzlich zur Eingabe des Benutzernamens und des Passwortes der 2-Faktor-Authentifizierungscode (TOTP) abgefragt.

Änderung des Namens eines Benutzerkontos

So ändern Sie den Namen eines Benutzerkontos:

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

HINWEIS: Zu beachten ist, dass Benutzernamen bei Verwendung von Verzeichnisdiensten einer Namenskonvention unterliegen können (siehe *Benutzerauthentifizierung mit Verzeichnisdiensten* ab Seite 53).

Änderung des Passworts eines Benutzerkontos

HINWEIS: Voraussetzung für die Änderung des Passworts eines Benutzerkontos ist das aktivierte *Superuser*-Recht (siehe *Berechtigung zum uneingeschränkten Zugriff (Superuser)* ab Seite 82) oder das Recht *Eigenes Passwort ändern* (siehe *Berechtigung zur Änderung des eigenen Passworts* ab Seite 83).

HINWEIS: Bei der Änderung des Passworts werden ggf. die festgelegten Passwort-Richtlinien (siehe *Passwort-Komplexität* auf Seite 19) berücksichtigt.

So ändern Sie das Passwort eines Benutzerkontos:

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

Aktuelles Passwort:	Geben Sie das bisherige Passwort ein.
<p>HINWEIS: Bei Benutzern mit aktiviertem Superuser-Recht (s. Seite 82 ff.) ist in diesem Feld keine Eingabe notwendig.</p>	
Passwort:	Geben Sie das neue Passwort ein.
Passwort bestätigen:	Wiederholen Sie das neue Passwort.
Klartext:	Aktivieren Sie dieses Kontrollkästchen, um die eingegebenen Passwörter im Klartext sehen und prüfen zu können.
Verifikationscode:	Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
<p>HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet (s. Seite 56 ff.) und aktiviert wurde (s. Seite 71 ff.).</p>	

4. Klicken Sie auf **Speichern**.

Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

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

System-Rechte

Bezeichnung	Berechtigung	Seite
Superuser-Recht	Zugriff auf die Konfiguration des Systems uneingeschränkt möglich	Seite 82
Config Panel Login	Login mit der Webapplikation <i>ConfigPanel</i>	Seite 82
EasyControl Login	Zugriff auf das <i>EasyControl</i> -Tool	Seite 83
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 83
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 83

Globale Geräterechte

Bezeichnung	Berechtigung	Seite
Persönliches Profil ändern	Änderung der Einstellungen des persönlichen Profils eines Benutzers	Seite 125
Gerätekonfiguration	Konfiguration des KVM-Switches	Seite 126
Zugriff auf USB-Geräte	USB-Zugriffsberechtigung	Seite 126

Individuelle CPU-Rechte

Bezeichnung	Berechtigung	Seite
Zugriff	Zugriff auf einen Rechner	Seite 125
Zugriff auf USB-Geräte	USB-Zugriffsberechtigung	Seite 126

Scripting-Rechte und Scripting-Gruppenrechte

Bezeichnung	Berechtigung	Seite
Ausführung	Ausführung von Scripts und Script-Gruppen	Seite 136

Änderung der Gruppenzugehörigkeit eines Benutzerkontos

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

So ändern Sie die Gruppenzugehörigkeit eines Benutzerkontos:

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

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

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

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

6. Klicken Sie auf **Speichern**.

Aktivierung oder Deaktivierung eines Benutzerkontos

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

So aktivieren oder deaktivieren Sie ein Benutzerkonto:

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

Löschen eines Benutzerkontos

So löschen Sie ein Benutzerkonto:

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

Verwaltung von Benutzergruppen

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

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

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

Anlegen einer neuen Benutzergruppe

Innerhalb des Systems können Sie bis zu 256 Benutzergruppen erstellen.

So erstellen Sie eine neue Benutzergruppe:

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

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

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

4. Klicken Sie auf **Speichern**.

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

Änderung des Namens einer Benutzergruppe

So ändern Sie den Namen einer Benutzergruppe:

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

Änderung der Rechte einer Benutzergruppe

Den verschiedenen Benutzergruppen können differenzierte Berechtigungen erteilt werden.

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

System-Rechte

Bezeichnung	Berechtigung	Seite
Superuser-Recht	Zugriff auf die Konfiguration des Systems uneingeschränkt möglich	Seite 82
Config Panel Login	Login mit der Webapplikation <i>ConfigPanel</i>	Seite 82
EasyControl Login	Zugriff auf das <i>EasyControl</i> -Tool	Seite 83
Eigenes Passwort ändern	Änderung des eigenen Passworts	Seite 83
Monitoring-Alarm bestätigen	Bestätigung eines Monitoring-Alarms	Seite 83

Globale Geräterechte

Bezeichnung	Berechtigung	Seite
Persönliches Profil ändern	Änderung der Einstellungen des persönlichen Profils eines Benutzers	Seite 125
Gerätekonfiguration	Konfiguration des KVM-Switches	Seite 126
Zugriff auf USB-Geräte	USB-Zugriffsberechtigung	Seite 126

Individuelle CPU-Rechte

Bezeichnung	Berechtigung	Seite
Zugriff	Zugriff auf einen Rechner	Seite 125
Zugriff auf USB-Geräte	USB-Zugriffsberechtigung	Seite 126

Scripting-Rechte und Scripting-Gruppenrechte

Bezeichnung	Berechtigung	Seite
Ausführung	Ausführung von Scripts und Script-Gruppen	Seite 136

Mitgliederverwaltung einer Benutzergruppe

So verwalten Sie die Mitglieder einer Benutzergruppe:

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

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

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

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

6. Klicken Sie auf **Speichern**.

Aktivierung oder Deaktivierung einer Benutzergruppe

So aktivieren oder deaktivieren Sie eine Benutzergruppe:

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

Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe:

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

System-Rechte

Berechtigung zum uneingeschränkten Zugriff (Superuser)

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

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

So ändern Sie die Berechtigung zum uneingeschränkten Zugriff:

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

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

5. Klicken Sie auf **Speichern**.

Berechtigung zum Login in die Webapplikation

So ändern Sie die Berechtigung zum Login mit der Webapplikation:

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

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

5. Klicken Sie auf **Speichern**.

Berechtigung zum Zugriff auf das EasyControl-Tool

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

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

Ja:	Zugriff auf das <i>EasyControl</i> -Tool erlaubt
Nein:	Zugriff auf das <i>EasyControl</i> -Tool untersagt

5. Klicken Sie auf **Speichern**.

Berechtigung zur Änderung des eigenen Passworts

So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:

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

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

5. Klicken Sie auf **Speichern**.

Berechtigung zur Bestätigung eines Monitoring-Alarms

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

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

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

5. Klicken Sie auf **Speichern**.

Erweiterte Funktionen des KVM-Systems

Identifizierung eines Gerätes durch Aktivierung der Identification-LED

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

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

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

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

Sicherung der Konfigurationseinstellungen

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

So sichern Sie die Konfigurationseinstellungen des KVM-Systems:

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

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

Sicherung der Konfigurationseinstellungen mit der Auto-Backup-Funktion

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

So verwenden Sie die Auto-Backup-Funktion:

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

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

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

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

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

WICHTIG: Ob der Test erfolgreich war, sehen Sie in den Syslog-Meldungen (siehe *Protokollierung von Syslog-Meldungen* ab Seite 50).

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

Wiederherstellung der Konfigurationseinstellungen

So stellen Sie die Konfigurationseinstellungen des KVM-Systems wieder her:

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

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

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

7. Klicken Sie auf **Restore**.

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

Freischaltung kostenpflichtiger Zusatzfunktionen

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

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

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

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

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

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

HINWEIS: Alternativ können Sie den Klartext-Inhalt des Feature-Keys manuell in das Textfeld kopieren.
--

5. Klicken Sie auf **Speichern**.

Im Menü *KVM-Switches* der Webapplikation können Sie verschiedene Einstellungen der KVM-Switches konfigurieren und Sie auch Informationen über das Gerät einsehen.

2 KVM-Switches

Grundkonfiguration der KVM-Switches

Änderung des Namens eines KVM-Switches

So ändern Sie den Namen eines KVM-Switches:

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

Änderung des Kommentares eines KVM-Switches

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

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

So ändern Sie den Kommentar eines KVM-Switches:

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

Einen KVM-Switch aus dem KVM-System löschen

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

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

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

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

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

Konfigurationseinstellungen der KVM-Switches

Gerätekonfiguration

Betriebsart wählen (OpenAccess bzw. Standard)

In der Standardeinstellung des KVM-Switches ist die **OpenAccess**-Betriebsart aktiviert. In diesem Modus ist die Benutzer-Anmeldung im OSD deaktiviert. Alle Benutzer des Arbeitsplatzes verwenden dieselben Einstellungen.

WICHTIG: In der Standardeinstellung (*OpenAccess*) ist der KVM-Switch nicht durch eine Passwortabfrage gesichert!

Alternativ können Sie auf die Standard-Betriebsart umschalten. In diesem Modus ist die Benutzer-Anmeldung im OSD erforderlich. Jeder Benutzer verwendet seine individuellen Zugangsdaten und Einstellungen.

So ändern Sie die Betriebsart des KVM-Switches:

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

Open-Access-Console:	In der OpenAccess -Betriebsart ist die Benutzer-Anmeldung im OSD deaktiviert. Alle Benutzer dieses Arbeitsplatzes verwenden dieselben Einstellungen.
Standard:	In der Standard -Betriebsart ist die Benutzer-Anmeldung im OSD aktiviert. Jeder Benutzer verwendet seine individuellen Einstellungen.

4. Klicken Sie auf **Speichern**.

Änderung des Hotkeys zum Aufruf des On-Screen-Displays (OSD)

Der Hotkey zum Aufruf des OSD wird verwendet, um das OSD zur Bedienung und Konfiguration des Systems zu öffnen.

HINWEIS: In der Standardeinstellung ist der Hotkey **Strg + Num** voreingestellt.

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

Sowohl die Hotkey-Modifiziertaste **Strg** als auch die Hotkey-Taste **Num** des Hotkeys können von Ihnen verändert werden.

So ändern Sie den Hotkey zum Aufruf des OSD:

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

- **Strg** (*Standard*)
- **Alt**
- **Alt Gr**
- **Win**
- **Shift**

4. Wählen Sie im Feld **Hotkey** eine der folgenden Optionen:

Num:	<i>Num-Taste (Standard)</i>
Pause:	<i>Pause-Taste</i>
Einfg:	<i>Einfg-Taste</i>
Entf:	<i>Entf-Taste</i>
Pos1:	<i>Pos 1-Taste</i>
Ende:	<i>Ende-Taste</i>
Bild auf:	<i>Bild ↑-Taste</i>
Bild ab:	<i>Bild ↓-Taste</i>
Leertaste:	<i>Leertaste</i>

5. Klicken Sie auf **Speichern**.

OSD mit doppeltem Tastendruck starten

Alternativ zum Öffnen des OSD mit der Tastenkombination **Strg+Num** (*Standard*) können Sie das OSD durch die zweifache, aufeinanderfolgende Betätigung einer bestimmten Taste (s. unten) öffnen.

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

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

Aus:	OSD-Aufruf via doppeltem Tastendruck deaktiviert. (<i>Standard</i>)
Strg:	OSD-Aufruf via doppeltem Druck der Strg -Taste.
Alt:	OSD-Aufruf via doppeltem Druck der Alt -Taste.
Alt Gr:	OSD-Aufruf via doppeltem Druck der Alt Gr -Taste.
Win:	OSD-Aufruf via doppeltem Druck der Win -Taste.
Shift:	OSD-Aufruf via doppeltem Druck der Leertaste .
Druck:	OSD-Aufruf via doppeltem Druck der Druck -Taste.
Pfeil links:	OSD-Aufruf via doppeltem Druck der Pfeil links -Taste.
Pfeil rechts	OSD-Aufruf via doppeltem Druck der Pfeil rechts -Taste.
Pfeil oben	OSD-Aufruf via doppeltem Druck der Pfeil oben -Taste.
Pfeil unten	OSD-Aufruf via doppeltem Druck der Pfeil unten -Taste.

4. Klicken Sie auf **Speichern**.

Änderung der Select-Keys

In der Standardeinstellung sind die Select-Keys 1 bis 3 zur Umschaltung zwischen den am KVM-Switch angeschlossenen Rechnern aktiv.

BEISPIEL: Die Umschaltung zu Rechner 2 erfolgt in der Standardeinstellung mit der Tastenkombination **Alt+2**.

Falls eine der aus dem Select-Key-Set resultierenden Tastenkombinationen mit einer Tastenkombination eines eingesetzten Anwendungsprogramms kollidiert, können sowohl der Select-Key-Modifizierer als auch die Select-Keys geändert werden.

So ändern Sie die Select-Keys:

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

- **Strg**
- **Alt (Standard)**
- **Alt Gr**
- **Win**
- **Shift**

5. Wählen Sie im Feld **Erlaubte Select-Keys** eine der aufgelisteten Optionen:

Nur Zahlen:	<i>nur Zifferntasten sind als Select-Keys zulässig</i>
Nur Buchstaben:	<i>nur Buchstabentasten sind als Select-Keys zulässig</i>
Zahlen und Buchstaben:	<i>Ziffern- und Buchstabentasten sind als Select-Keys zulässig</i>

WICHTIG: Die ausgewählte Tastenart steht in Kombination mit der/den von Ihnen ausgewählten Select-Key-Modifizierertaste(n) *nicht* als Tastenkombination unter dem Betriebssystem und den Anwendungsprogrammen des Rechners zur Verfügung.

6. Klicken Sie in der Kanaltabelle in die Spalte **Select-Keys** eines Kanals und geben Sie anschließend das bzw. die gewünschte(n) Zeichen ein.
7. Weisen Sie die Select-Keys der anderen Kanäle nacheinander wie in Schritt 6. beschrieben zu.
8. Klicken Sie auf **Speichern**.

Switching (de)aktivieren

Die Umschaltung auf einen bestimmten Kanal kann über diverse Möglichkeiten erfolgen. Falls gewünscht, können Sie die Möglichkeiten der Umschaltung einschränken.

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

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

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

4. Klicken Sie auf **Speichern**.

Reinitialisierung von USB-Eingabegeräten

Sobald Sie eine USB-Tastatur bzw. -Maus an den KVM-Switch anschließen, wird das Eingabegerät initialisiert und kann ohne Einschränkungen verwendet werden. Einige USB-Eingabegeräte erfordern eine Reinitialisierung der USB-Verbindung nach einer bestimmten Zeit.

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

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

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

4. Klicken Sie auf **Speichern**.

Änderung des Scancode-Sets einer PS/2-Tastatur

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

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

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

So ändern Sie die Einstellung des Scancode-Sets:

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

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

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

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

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

DDC/CI-Unterstützung (de)aktivieren

Der KVM-Switch wurde 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.

HINWEIS: Die Unterstützung kann *nicht* für alle Monitor-Modelle garantiert werden.

So konfigurieren Sie die DDC/CI-Übertragung:

HINWEIS: Die **DDC/CI**-Übertragung wird für jeden Videokanal des KVM-Switches separat eingestellt. Bei Multichannel-Geräten kann die folgende Option für jeden Videokanal separat eingestellt werden.

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

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

4. Klicken Sie auf **Speichern**.

Allgemeine OSD-Konfiguration

Verwendung des OSD an-/ausschalten

Mit dieser Funktion wählen Sie, ob Benutzer des KVM-Switches das OSD aufrufen und verwenden dürfen.

So (de)aktivieren Sie die Verwendung des OSD:

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

Nein:	OSD verfügbar (<i>Standard</i>)
Ja:	OSD gesperrt

4. Klicken Sie auf **Speichern**.

OSD-Auflösung einstellen

In der Standardeinstellung des KVM-Switches wird das OSD auf dem Arbeitsplatzmonitor mit einer Auflösung von 1024 × 768 Bildpunkten dargestellt, wenn der Monitor diese Auflösung unterstützt. Falls der Monitor diese Auflösung nicht unterstützt, wird eine Auflösung von 640 × 480 Bildpunkten verwendet.

Sie können alternativ eine feste OSD-Auflösung (s. Tabelle unten) wählen.

So stellen Sie die OSD-Auflösung ein:

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

Auto:	Wenn vom Monitor unterstützt, wird das OSD mit einer Auflösung von 1024 × 768 Bildpunkten dargestellt. Unterstützt der Monitor diese Auflösung nicht, wird eine Auflösung von 640 × 480 Bildpunkten verwendet (<i>Standard</i>).
640×480/60:	OSD-Darstellung mit einer Auflösung von 640 × 480 Bildpunkten
720×400/70:	OSD-Darstellung mit einer Auflösung von 720 × 400 Bildpunkten
1024×768/60:	OSD-Darstellung mit einer Auflösung von 1024 × 768 Bildpunktensystem

4. Klicken Sie auf **Speichern**.

Tastaturlayout für Eingaben innerhalb des OSD auswählen

Werden bei der Eingabe von Zeichen auf der Tastatur des Arbeitsplatzes andere Zeichen am Bildschirm 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 KVM-Switches.

So wählen Sie das Tastaturlayout der Arbeitsplatztastatur aus:

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

Deutsch (*Standard*)

Englisch (USA)

Englisch (Großbritannien)

Französisch

Spanisch

Lat. Amerikanisch

Portugiesisch

Schwedisch

Schweiz-Französisch

Dänisch

4. Klicken Sie auf **Speichern**.

Persönliche Einstellungen (Persönliches Profil)

Anzeige der Informationseinblendung

Standardmäßig erfolgt bei jeder Kanalaufschaltung eine temporäre (5 Sekunden) Informationseinblendung. Die Einblendung auf dem Monitor des Arbeitsplatzes informiert über die Namen des Kanals sowie des KVM-Switches und enthält gegebenenfalls weitere Informationen.

Alternativ zur temporären Einblendung kann die Informationseinblendung permanent erfolgen oder ausgeschaltet werden.

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

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **OSD-Info anzeigen** zwischen folgenden Optionen:

5 Sekunden:	temporäre Informationseinblendung (<i>Standard</i>)
Permanent:	permanente Informationseinblendung
Aus:	Informationseinblendung ausschalten

5. Klicken Sie auf **Speichern**.

Transparenz des OSD einstellen

In der Standardeinstellung wird das 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 OSD 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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **OSD-Transparenz** zwischen folgenden Optionen:

Hoch:	hohes Durchscheinen des Bildschirminhalts
Mittel:	mittleres Durchscheinen des Bildschirminhalts (<i>Standard</i>)
Niedrig:	leichtes Durchscheinen des Bildschirminhalts
Aus:	überdeckende Darstellung des OSD

5. Klicken Sie auf **Speichern**.

Farbe der Informationseinblendung ändern

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

Folgende Farben werden unterstützt:

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

So ändern Sie die Einstellung der Informationseinblendung:

1. Klicken Sie im Menü auf **Benutzer**.
2. Klicken Sie auf das zu konfigurierende Benutzerkonto und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Farbe OSD-Info** die gewünschte Farbe.
5. Klicken Sie auf **Speichern**.

Automatisches Schließen des OSDs (de)aktivieren

In der Standardeinstellung des KVM-Switches wird das OSD solange angezeigt, bis der Anwender eine Schaltfunktion ausführt oder das OSD schließt.

Alternativ können Sie eine Zeitspanne angeben, nach deren Ablauf das OSD automatisch geschlossen wird.

So (de)aktivieren Sie das automatische Schließen des OSDs:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Geben Sie im Feld **Timeout OSD-Sitzung** eine gewünschte Zeitspanne zwischen **5** und **99** Sekunden ein.

HINWEIS: Die Eingabe der Ziffer **0** deaktiviert das automatische Schließen.

5. Klicken Sie auf **Speichern**.

Standard-Menü-Modus ändern

In der Standardeinstellung zeigt das OSD nach dem Aufruf das *Auswahl*-Menü zur Auswahl eines Kanals an. Falls gewünscht, können Sie in Ihrem persönlichen Profil einstellen, dass nach dem Start des OSD das Script-Menü angezeigt wird.

TIPP: Unabhängig von der Standardeinstellung können Sie jederzeit mit der Schnellwahltaste **Strg+X** zwischen dem Auswahl- und dem Script-Menü wechseln.

So ändern Sie den Standard-Menü-Modus:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Standard-OSD-Menü** zwischen folgenden Optionen:

Select:	Das <i>Auswahl</i> -Menü wird nach dem Start des OSD angezeigt (<i>Standard</i>).
Script:	Das <i>Script</i> -Menü wird nach dem Start des OSD angezeigt.

5. Klicken Sie auf **Speichern**.

Umschaltswelle für Änderung des Menü-Modus per Maus

Zusätzlich zum Wechsel des Menü-Modus per Schnellwahltaste **Strg+X** können Sie auch den Wechsel des Menü-Modus per Maus aktivieren.

TIPP: Nach der Aktivierung des Wechsels des Menü-Modus per Maus können Sie per Links-/Rechtsbewegung der Maus im *Auswahl*- und im *Script*-Menü zwischen beiden Modi wechseln.

WICHTIG: Der Wechsel des Menü-Modus per Maus ist *nicht* möglich, wenn im *Auswahl*- und/oder im *Script*-Menü kein Eintrag vorhanden ist!

So (de)aktivieren Sie die Umschaltswelle und/oder stellen deren Empfindlichkeit 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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Select- /Szenario-Menü Maus-Umschaltung** zwischen folgenden Optionen:

Aus:	Mausumschaltung des OSD-Menü-Modus deaktiviert (<i>Standard</i>)
Sensitivity 1:	geringste Empfindlichkeitsstufe für die Mausumschaltung des OSD-Menü-Modus
Sensitivity 10:	maximale Empfindlichkeitsstufe für die Mausumschaltung des OSD-Menü-Modus
Sensitivity 2-8:	weitere Empfindlichkeitsstufen für das Fine-Tuning der Mausumschaltung des OSD-Menü-Modus

5. Klicken Sie auf **Speichern**.

Verweildauer der Autoscan- bzw. Autoskip-Funktion konfigurieren

Standardmäßig wird jede automatische Umschaltung 10 Sekunden gehalten, bevor die Verbindung getrennt und der nächste Kanal aufgeschaltet wird.

Den Zeitraum der Verweildauer einer Umschaltung können Sie im Bereich von 1 bis 99 Sekunden festlegen.

So ändern Sie die Verweildauer einer Umschaltung:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Geben Sie in der Zeile **Scantime** die gewünschte Verweildauer innerhalb des Bereichs von 1 bis 99 Sekunden.
5. Klicken Sie auf **Speichern**.

Step-Keys auswählen

Nach Aktivierung des *Stepscan*-Modus schalten Sie auf Tastendruck den nächsten bzw. vorherigen Computer auf.

In der Standardeinstellung des KVM-Switches sind die Tasten **Hoch** und **Runter** hierfür vorgesehen. Alternativ können Sie ein anderes Set aus hierfür vorgesehenen Tasten auswählen.

So wählen Sie die Tasten zur Verwendung mit der Stepscan-Funktion:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Stepscan-Keys** zwischen folgenden Optionen:

Hoch Runter:	Mit der Hoch -Taste einen Kanal aufwärts und mit der Runter -Taste einen Kanal abwärts schalten.
Bild hoch Bild runter:	Mit der Bild hoch -Taste einen Kanal aufwärts und mit der Bild runter -Taste einen Kanal abwärts schalten.
Num hoch Num runter:	Mit der Num hoch -Taste einen Kanal aufwärts und mit der Num runter -Taste einen Kanal abwärts schalten.
Num Bild hoch Num Bild runter:	Mit der Num Bild hoch -Taste einen Kanal aufwärts und mit der Num Bild runter -Taste einen Kanal abwärts schalten.
Num+ Num-:	Mit der Num+ -Taste einen Kanal aufwärts und mit der Taste Num- einen Kanal abwärts schalten.
F10 F9:	Mit der F10 -Taste einen Kanal aufwärts und mit der F9 -Taste einen Kanal abwärts schalten.
0 9:	Mit der 0 -Taste einen Kanal aufwärts und mit der 9 -Taste einen Kanal abwärts schalten.
Num 0 Num 9:	Mit der Num 0 -Taste einen Kanal aufwärts und mit der Num 9 -Taste einen Kanal abwärts schalten.
K I:	Mit der K -Taste einen Kanal aufwärts und mit der I -Taste einen Kanal abwärts schalten.

5. Klicken Sie auf **Speichern**.

Automatisches Aufschalten des zuletzt aufgeschalteten Kanals

Aktivieren Sie im persönlichen Profil die Funktion **Letzte CPU merken**, um beim Logout des Benutzers den Kanal zu merken, auf den der Benutzer zuletzt aufgeschaltet war. Bei der nächsten Anmeldung des Benutzers wird er automatisch auf den gemerkten Kanal aufgeschaltet.

HINWEIS: Das Ausschalten des KVM-Switches wird wie ein Logout behandelt.

WICHTIG: Bei Aktivierung der Funktion **Letzte CPU merken** wird eine möglicherweise konfigurierte Standard-CPU bzw. ein Standard-Script des Benutzers ignoriert.

So (de)aktivieren Sie die automatische Aufschaltung des zuletzt aufgeschalteten Kanals:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Letzte CPU merken** zwischen folgenden Optionen:

Aus: Nach der Anmeldung wird der konfigurierte Standard-Kanal aufgeschaltet.

Ist kein Standard-Kanal konfiguriert, erscheint das Auswahl-Menü (*Standard*).

An: Nach der Anmeldung des Benutzers wird der gemerkte Kanal aufgeschaltet.

5. Klicken Sie auf **Speichern**.

Standardaktion nach der Benutzeranmeldung konfigurieren

Nach der Anmeldung des Benutzers erscheint üblicherweise das OSD auf dem Bildschirm des Arbeitsplatzes.

Die Konfigurationseinstellung **Standardausführung** erlaubt Ihnen die Festlegung eines Kanals, der automatisch nach der Benutzeranmeldung aufgeschaltet oder eines Skripts, das automatisch ausgeführt wird.

HINWEIS: Diese neue Funktion ersetzt die Funktion **After power-up switch to** der Firmware-Version 1.0.000.

So wählen Sie einen Kanal, der automatisch nach der Benutzeranmeldung aufgeschaltet 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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Standardausführung** die Option **Standard-CPU**.
5. Scrollen Sie zum Bereich **Standard-CPU**.
6. Schalten Sie den Schieberegler der gewünschten Standard-CPU in der Spalte **Standard-CPU** nach rechts (aktiviert).

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

7. Klicken Sie auf **Speichern**.

So wählen Sie ein Standard-Script (alternativ eine -Script-Gruppe), das automatisch nach der Benutzeranmeldung ausgeführt 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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Standardausführung** die Option **Standard-Script/Script-Gruppe**.
5. Scrollen Sie zum Bereich **Standard-Script/Script-Gruppe**.
6. Schalten Sie den Schieberegler des gewünschten Standard-Scripts/der gewünschten -Script-Gruppe in der Spalte **Standard-Script/Script-Gruppe** nach rechts (aktiviert).

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

7. Klicken Sie auf **Speichern**.

So deaktivieren Sie die konfigurierte Standardaktion:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Persönliches Profil**.
4. Wählen Sie im Feld **Standardausführung** die Option **Keine**.
5. Klicken Sie auf **Speichern**.

Kanal-Konfiguration

Änderung des Namens eines Kanals

So ändern Sie einen Kanalnamen:

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

Änderung des Kommentares eines Kanals

So ändern Sie den Kommentar eines Kanals:

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

Aktivierung/Deaktivierung eines Kanals

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

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

So (de)aktivieren Sie einen Kanal:

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

Aktivierung/Deaktivierung des Tastatur-Signals

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

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

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

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

Aktiviert:	Die Tastatur-Signale werden an den Rechner dieses Kanals übertragen (<i>Standard</i>)
Deaktiviert:	Die Tastatur-Signale werden <i>nicht</i> an den Rechner dieses Kanals übertragen.

6. Klicken Sie auf **Speichern**.

Unterstützung für Multimedia- und Sondertasten

Die Tasten der Standardtastatur wurden bei einigen USB-Tastaturen verschiedener Hersteller ergänzt.

So sind einige USB-Tastaturen mit Multimedia-Sondertasten ausgestattet, die die komfortable Bedienung spezieller Multimedia-Funktionen des Rechners ermöglichen. Die Tastatur des *Apple Mac mini* beispielsweise ist mit einer Taste zum Öffnen des DVD-Laufwerks ausgestattet.

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

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

PC Standard:	Standard-Tastaturmodus
PC Multimedia:	Unterstützung für Multimedia-Sondertasten (<i>Standard</i>)
Apple A1243:	Tastaturmodus für Apple-Rechner
LK463:	LK463-kompatible Tastatur

6. Klicken Sie auf **Speichern**.

Failover-Switching einrichten

Die Funktion **Failover-Switching** schaltet bei Statuswechsel des aktiven Kanals von *Online* zu *Offline* automatisch auf den konfigurierten *Failover*-Kanal.

Die OSD-Meldung **Failover switching** informiert Sie über die automatische Umschaltung auf den Failover-Kanal.

In der Standardeinstellung ist diese Funktion deaktiviert. Sie können die Funktion für jeden Kanal separat konfigurieren, indem Sie den gewünschten Failover-Kanal festlegen.

HINWEIS: Die Einrichtung einer *Failover-Schaltkette* ist möglich, indem Sie beispielsweise den Failover-Kanal jeweils auf den nächsten Kanal festlegen.

Wenn bei Eingriff des Failover-Switchings auch der Failover-Kanal offline ist, wird auf dessen Failover-Kanal geschaltet (usw.).

Wenn kein weiterer Kanal online ist, wird das Failover-Switching beendet.

So konfigurieren Sie einen Failover-Kanal für einen KVM-Kanal:

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

Kein:	keine automatische Umschaltung (<i>Standard</i>)
[Kanalnr.]:	automatische Umschaltung auf den ausgewählten Kanal

6. Klicken Sie auf **Speichern**.

Videokanal-Konfiguration

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

Änderung des Namens eines Videokanals

So ändern Sie den Namen eines Videokanals:

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

Änderung des Kommentares eines Videokanals

So ändern Sie den Kommentar eines Videokanals:

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

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-Switch üblicherweise unverändert über Enhanced-DDC (*Enhanced Display Data Channel*) an den Rechner weitergeleitet.

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

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

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

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

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

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

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

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

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

6. Klicken Sie auf **Speichern**.

EDID-Profil eines Monitores exportieren

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Klicken Sie auf den zu konfigurierenden KVM-Switch und anschließend auf **Konfiguration**.
3. Klicken Sie auf **Kanäle**.
4. Klicken Sie auf den zu konfigurierenden Kanal und anschließend auf **Konfiguration**.
5. Wählen Sie das zu exportierende **EDID-Profil**.
6. Klicken Sie auf **EDID exportieren**.
7. Ändern Sie ggf. im Datei-Dialog den Namen der zu exportierenden bin-Datei.
8. Klicken Sie auf **Speichern**.

Verwendung des Freeze-Modus

Bei einer Unterbrechung der Verbindung zwischen dem Rechner und dem KVM-Switch im laufenden Betrieb, wird in der Standardeinstellung des KVM-Switches kein Bild auf dem Monitor des Arbeitsplatzes dargestellt.

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

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

So konfigurieren Sie die Einstellung des Freeze-Modus:

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

Aus:	Kein Bild bei Verbindungsabbruch anzeigen (<i>Standard</i>).
An OSD-Timer + Rahmen	Anzeige des letzten Bildes bei Verbindungsabbruch. Der Verbindungsabbruch wird durch die Einblendung der vergangenen Zeit seit dem Verbindungsabbruch sowie der Anzeige eines farbigen Rahmens signalisiert.
An OSD-Timer	Anzeige des letzten Bildes bei Verbindungsabbruch. Der Verbindungsabbruch wird durch die Einblendung der vergangenen Zeit seit dem Verbindungsabbruch signalisiert.
An Rahmen	Anzeige des letzten Bildes bei Verbindungsabbruch. Der Verbindungsabbruch wird durch die Anzeige eines farbigen Rahmens signalisiert.

6. Klicken Sie auf **Speichern**.

Aktivierung/Deaktivierung von DisplayPort-Power

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

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

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

Deaktiviert:	DisplayPort-Power ist deaktiviert (<i>Standard</i>).
Aktiviert:	DisplayPort-Power ist aktiviert.

6. Klicken Sie auf **Speichern**.

Erweiterte Funktionen für KVM-Switches

Konfigurationseinstellungen übertragen (Gerät ersetzen)

Wird ein KVM-Switch durch ein anderes Gerät ersetzt, können Sie die Konfigurationseinstellungen des bisherigen Switches auf den neuen übertragen. Nach der Übertragung der Konfigurationseinstellungen ist das neue Gerät unmittelbar einsatzbereit.

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

So übertragen Sie die Konfigurationseinstellungen eines KVM-Switches:

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

Umschaltung des Kanals

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

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

So schalten Sie die Signalübertragung auf einen Rechner:

1. Klicken Sie im Menü auf **KVM-Switches**.
2. Markieren Sie auf den zu schaltenden KVM-Switch.
3. Klicken Sie auf **Schalten**.
4. Klicken Sie auf den aufzuschaltenden Kanal (z. B. **CPU_3**).

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

Monitoring-Werte konfigurieren

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

Auswahl der zu überwachenden Monitoring-Werte

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

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

So verwalten Sie die zu überwachenden Monitoring-Werte:

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

<p>HINWEIS: Um <i>alle</i> Werte aus- oder einzuschalten können Sie das Kontrollkästchen im Kopf der Spalten Aktiviert verwenden.</p>

5. Klicken Sie auf **Speichern**.

Rechteverwaltung

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Globale Geräterechte**.
4. Wählen Sie im Feld **Persönliches Profil editieren** zwischen folgenden Optionen:

Ja:	Einsehen und Editieren des eigenen Benutzerprofils erlaubt
Nein:	Einsehen und Editieren des eigenen Benutzerprofils untersagt

5. Klicken Sie auf **Speichern**.

Zugriffsrecht auf einen KVM-Kanal

So ändern Sie das Zugriffsrecht auf einen KVM-Kanal:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Individuelle Rechte**.
4. Wählen Sie im Feld **Zugriff** zwischen folgenden Optionen:

Nein:	Zugriff auf den KVM-Kanal untersagt
Ansicht:	Ansicht des Monitorbildes des am KVM-Kanal angeschlossenen Computers erlaubt
Ja:	Zugriff auf den KVM-Kanal erlaubt

5. Klicken Sie auf **Speichern**.

Berechtigung zur Konfiguration des KVM-Switches

So ändern Sie die Berechtigung für das Einsehen und Editieren der Konfiguration des KVM-Switches:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Globale Geräterechte**.
4. Wählen Sie im Feld **Gerätekonfiguration** zwischen folgenden Optionen:

Nein:	Einsehen und Editieren der Konfiguration des KVM-Switches untersagt
Ja:	Einsehen und Editieren der Konfiguration des KVM-Switches erlaubt

5. Klicken Sie auf **Speichern**.

Zugriff auf USB-Geräte

In der Standardeinstellung des KVM-Switches haben die Benutzer Zugriff auf die USB-Geräte. Falls gewünscht, kann diese Berechtigung durch die Änderung des Rechtes *Zugriff auf USB* eines Benutzerkontos oder eine Benutzergruppe aufgehoben werden.

Die Zugriffsberechtigung auf die USB-Geräte eines bestimmten Kanals kann entweder global (für alle Kanäle, auf welche ein Benutzer bzw. Benutzergruppe Zugriff hat) *oder* nur für bestimmte Kanäle entzogen werden.

HINWEIS: Die Zugriffsberechtigung wird anhand des Effektivrechts des Benutzers ermittelt. Das Effektivrecht ist das höchste Recht, das aus dem Individualrecht des Benutzerkontos und den Rechten der zugeordneten Gruppe(n) resultiert.

So ändern Sie die USB-Zugriffsberechtigung für alle Kanäle:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Globale Geräterechte**.
4. Wählen Sie im Feld **Zugriff auf USB-Geräte** zwischen folgenden Optionen:

Nein:	Zugriff auf die USB-Geräte untersagt
Ja:	Zugriff auf die USB-Geräte erlaubt

5. Klicken Sie auf **Speichern**.

So ändern Sie die USB-Zugriffsberechtigung für einen bestimmten Kanal:

HINWEIS: Die USB-Zugriffsberechtigung kann nur konfiguriert und angewendet werden, wenn das Benutzerkonto oder die Benutzergruppe auch die entsprechenden allgemeinen Zugriffsrechte (s. Seite 125) für den KVM-Switch besitzt!

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Individuelle Rechte**.
4. Wählen Sie den Kanal, dessen Zugriffsrecht Sie ändern möchten.
5. Wählen Sie im Feld **Zugriff auf USB-Geräte** zwischen folgenden Optionen:

Nein:	Zugriff auf die USB-Geräte untersagt
Ja:	Zugriff auf die USB-Geräte erlaubt

6. Klicken Sie auf **Speichern**.

Statusinformationen eines KVM-Switches einsehen

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

So können Sie die Statusinformationen eines KVM-Switches einsehen:

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

KVM Switch	
Name:	Name des KVM-Switches
Geräte-ID:	physikalische ID des KVM-Switches
Status:	aktueller Status (Online oder Offline) des KVM-Switches
Klasse:	Geräteklasse des KVM-Switches

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

Aktive Features
In diesem Bereich werden alle aktivierten Zusatzfunktionen aufgelistet.

Link-Status	
Link detected:	Verbindung zum Netzwerk hergestellt (Ja) oder unterbrochen (Nein).
Auto-negotiation:	Die Übertragungsgeschwindigkeit und das Duplex-Verfahren wurden automatisch (Ja) oder manuell vom Administrator konfiguriert (Nein).
Speed:	Übertragungsgeschwindigkeit
Duplex:	Duplexverfahren (Full bzw. Half)

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

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

Scripting-Funktion

Mit der Scripting-Funktion können Sie Scripts anlegen, verwalten und ausführen.

Ein Script ist ein XML-Dokument, das einen oder mehrere Befehle enthält, die vom Matrixswitch ausgeführt werden.

BEISPIELSCRIPT ZUR AUFSCHALTUNG EINES KANALS

```
<?xml version="1.0" encoding="utf-8"?>
<root>
  <connectmux>3</connectmux>
</root>
```

Der Aufbau eines gültigen XML-Dokuments und die möglichen Befehle sowie deren Syntax werden im Kapitel *XML-Steuerung des KVM-Switches* des separaten Handbuchs *Installation und Bedienung* beschrieben.

Die im KVM-Switch gespeicherten Scripts können Sie über das OSD des KVM-Switches ausführen.

Scripts konfigurieren

Die Konfiguration der Scripting-Funktion erledigen Sie komfortabel mit einem Assistenten. Klicken auf das Menü **Erweiterte Funktionen** und wählen Sie **Scripts und Script-Gruppen**.

WICHTIG: Nur Benutzer mit **Superuser**-Rechten können Scripts in der Webapplikation erstellen, ändern und löschen.

Schritt 1: Option »Scripts« wählen

- Wählen Sie die Option **Scripts**, um einzelne Scripts zur Steuerung eines Geräts anzulegen, zu bearbeiten oder zusammenzufügen.

Schritt 2: Scripts anlegen, bearbeiten, zusammenfügen oder löschen

So legen Sie ein neues Script an:

1. Klicken Sie auf **Script hinzufügen**.
2. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Script-Namen ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Script.

3. Klicken Sie auf **Speichern**.

So löschen Sie ein vorhandenes Script:

1. Markieren Sie das zu löschende Script und klicken Sie auf **Löschen**.
2. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

So führen Sie existierende Scripts zu einem neuen Script zusammen:

1. Markieren Sie die existierenden Scripts, die Sie zusammenführen möchten.

TIPP: Halten Sie die **Strg**-Taste gedrückt, um mehrere Scripts aus der Liste auszuwählen.

2. Klicken Sie auf **Zusammenfügen**.
3. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Script-Namen des zusammengeführten Scripts ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Script.

4. Falls gewünscht, können Sie die Reihenfolge der zusammenzuführenden Scripts ändern. Markieren Sie hierzu ein Script und klicken Sie auf  (*Pfeil hoch*) oder  (*Pfeil runter*). Das ausgewählte Script wird nach oben bzw. unten verschoben.

HINWEIS: Die XML-Dokumente der ausgewählten Scripts werden in der ausgewählten Reihenfolge in ein neues Script kopiert. Im neuen Script können Sie das (aus den Einzel-Scripts entstandene) XML-Dokument beliebig editieren.

5. Klicken Sie auf **Speichern**.

Schritt 3: Script bearbeiten

HINWEIS: Die Script-Befehle werden in einem XML-Dokument gespeichert. Jedes XML-Dokument kann einen oder mehrere Befehle enthalten.

Der Aufbau eines gültigen XML-Dokuments und die möglichen Befehle sowie deren Syntax werden im Kapitel *XML-Steuerung des KVM-Switches* des separaten Handbuchs *Installation und Bedienung* beschrieben.

So bearbeiten Sie ein Script:

1. Markieren Sie das zu bearbeitende Script und klicken Sie auf **Speichern und weiter**.
2. Erfassen bzw. aktualisieren Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Script-Namen ein.
Aktiviert:	Aktivieren oder deaktivieren Sie die Ausführung <i>und</i> Anzeige des Scripts im Script-Menü.
Ausführungs- verzögerung:	Sie können die Ausführung des Scripts nach dessen Aufruf um bis zu 999 Sekunden verzögern. Geben Sie die gewünschte Verzögerungszeit in Sekunden ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zum Script.
XML-Code	Geben Sie den XML-Code mit den Script-Befehlen ein.

3. Klicken Sie auf **Speichern**.

Schritt 4: Besitzer festlegen

Ein Script darf ausgeführt werden, wenn der ausführende Benutzer *Besitzer* des Scripts ist oder er das Ausführungsrecht für das Script besitzt.

HINWEIS: Nur Scripts ohne Besitzer können zu Script-Gruppen hinzugefügt werden!

- Aktivieren Sie den Schieberegler **Besitzer** in der Zeile des Benutzers, der als Besitzer des Scripts eingetragen werden soll.

Schritt 5: Script-Verfügbarkeit

Klicken Sie auf **Speichern und weiter**.

Schritt 6: Ziel-Gerät

Sie können in der Script-Konfiguration festlegen, ob das Script lokal oder auf einem anderen Gerät ausgeführt werden soll.

HINWEIS: Voraussetzung für die Ausführung auf einem Matrixswitch ist, dass auf dem Ziel-Matrixswitch die kostenpflichtigen Zusatzfunktion **IP-Control-API** aktiviert ist.

- Aktivieren Sie den Schieberegler **Auf diesem Gerät ausführen** *oder* geben Sie die IP-Adresse und Port von einem anderen Gerät ein.
- Aktivieren Sie den Schieberegler **Geräteantwort ignorieren**, falls die Antwort des Geräts *nicht* ausgewertet werden soll.

Script-Gruppen konfigurieren

Die Konfiguration der Scripting-Funktion erledigen Sie komfortabel mit einem Assistenten. Klicken auf das Menü **Erweiterte Funktionen** und wählen Sie **Scripts und Script-Gruppen**.

WICHTIG: Nur Benutzer mit **Superuser**-Rechten können Script-Gruppen in der Webapplikation erstellen, ändern und löschen.

Schritt 1: Option »Script-Gruppen« wählen

- Wählen Sie die Option **Script-Gruppen**, um mehrere vorhandene Scripts in einer Script-Gruppe zu organisieren.

Schritte 2: Script-Gruppen anlegen, bearbeiten oder löschen

So legen Sie eine neue Script-Gruppe an:

1. Klicken Sie auf **Script-Gruppe hinzufügen**.
2. Erfassen Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Script-Gruppen-Namen ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zur Script-Gruppe.

3. Klicken Sie auf **Speichern**.

So löschen Sie eine vorhandene Script-Gruppe:

1. Markieren Sie die zu löschende Script-Gruppe und klicken Sie auf **Löschen**.
2. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Schritte 3: Script-Gruppe bearbeiten

So bearbeiten Sie eine vorhandene Script-Gruppe:

1. Markieren Sie die zu bearbeitende Script-Gruppe und klicken Sie auf **Speichern und weiter**.
2. Erfassen bzw. aktualisieren Sie folgende Daten innerhalb der Dialogmaske:

Name:	Geben Sie den gewünschten Script-Namen ein.
Aktiviert:	Aktivieren oder deaktivieren Sie die Ausführung <i>und</i> Anzeige der Script-Gruppe im Script-Menü.
Ausführungs- verzögerung:	Sie können die Ausführung der Script-Gruppe nach deren Aufruf um bis zu 999 Sekunden verzögern. Geben Sie die gewünschte Verzögerungszeit in Sekunden ein.
Kommentar:	Erfassen Sie hier – falls gewünscht – einen beliebigen Kommentar zur Script-Gruppe.

3. Klicken Sie auf **Speichern**.

Schritt 4: Scripts zur Gruppe hinzufügen oder aus der Gruppe entfernen

Der Dialog listet alle Scripts des KVM-Switches auf, denen kein Besitzer zugeordnet wurde.

- Aktivieren Sie den Schieberegler **Hinzufügen** in der Zeile der Scripts, die Sie zur Gruppe hinzufügen möchten.
- Deaktivieren Sie den Schieberegler **Hinzufügen** in der Zeile der Scripts, die Sie aus der Gruppe entfernen möchten.

HINWEIS: Verwenden Sie die Option **Hinzufügen** im Spaltenkopf, um die Schalter aller Scripts umzulegen.

Schritt 5: Reihenfolge der Script-Ausführung festlegen

- Falls gewünscht, können Sie die Reihenfolge der Scripts innerhalb der Gruppe ändern. Markieren Sie hierzu ein Script und klicken Sie auf  (*Pfeil hoch*) oder  (*Pfeil runter*). Das ausgewählte Script wird nach oben bzw. unten verschoben.

Schritt 6: Verfügbarkeit der Script-Gruppe

Klicken Sie auf **Speichern und weiter**.

Berechtigung für das Ausführen von Scripts und Script-Gruppen einstellen

HINWEIS: Benutzer haben jederzeit das Recht *eigene* Scripts (**Besitzer**) auszuführen und zu löschen. Hierfür sind keine zusätzlichen Rechte erforderlich.

Für die Ausführung eines nicht dem eigenen Benutzerkonto zugeordneten Scripts ist das **Script-Ausführungsrecht** für das Script erforderlich. Dies gilt ebenso für Script-Gruppen.

Das **Script-Ausführungsrecht** können Sie in den Einstellungen eines Benutzerkontos erteilen. Alternativ können Sie das Recht über Benutzergruppen verwalten (siehe *Effizienter Einsatz der Rechteverwaltung* auf Seite 67).

Ausführungsrecht für ein Script festlegen

So ändern Sie das Ausführungsrecht für ein bestimmtes Script:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Script-Rechte**.
4. Wählen Sie im Listenfeld des Abschnitts **Scripting-Rechte** auf der linken Seite das gewünschte Script aus.

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

5. Wählen Sie im Feld **Ausführung** auf der rechten Seite zwischen folgenden Optionen:

Ja:	Ausführung des Script erlaubt.
Nein:	Ausführung des Script verboten.

6. Klicken Sie auf **Speichern**.

Ausführungsrecht für eine Script-Gruppe festlegen

So ändern Sie das Ausführungsrecht für eine bestimmte Script-Gruppe:

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-Switch-Systeme** und anschließend auf die Bereichsauswahl **Script-Gruppen-Rechte**.
4. Wählen Sie im Listenfeld des Abschnitts **Script-Gruppenrechte** auf der linken Seite die gewünschte Script-Gruppe aus.

TIPP: Verwenden Sie ggf. das *Suchen*-Feld, um die im Auswahlfenster anzuzeigenden Script-Gruppen einzuzugrenzen.

5. Wählen Sie im Feld **Ausführung** auf der rechten Seite zwischen folgenden Optionen:

Ja:	Ausführung der Script-Gruppe erlaubt.
Nein:	Ausführung der Script-Gruppe verboten.

6. Klicken Sie auf **Speichern**.

Script-Keys konfigurieren und zuordnen

Nach der Einrichtung der Script-Key-Modifiziertaste(n) und eines Script-Key-Sets sowie der Aktivierung eines Script-Key-Sets im Benutzerkonto, kann die Ausführung eines Scripts über Tastenkombinationen an der Tastatur des Arbeitsplatzes erfolgen.

Funktion der Script-Keys am Arbeitsplatzmodul

Bei Verwendung von Script-Keys zur Ausführung von Scripts ist der Aufruf des OSD nicht erforderlich. Die Ausführung kann daher – bei Kenntnis der Script-Keys – deutlich schneller durchgeführt werden.

So führen Sie ein Script mit Script-Keys im OSD aus:

1. Betätigen Sie die im KVM-Switch eingerichtete(n) Script-Key-Modifiziertaste(n) und den, dem Script zugewiesenen, Script-Key.

BEISPIEL:

- Script-Key-Modifiziertasten: **Win + Shift**
- Script-Key für Script: **1**

Halten Sie die Tasten **Win+Shift** gedrückt, während Sie den Script-Key **1** betätigen. Sobald die Tasten losgelassen werden, erfolgt die Ausführung des Scripts.

Verwaltung der Script-Keys

Im KVM-Switch können 20 globale oder pro Benutzer 10 weitere, individuelle Script-Key-Sets angelegt werden.

Innerhalb der Script-Key-Sets können Sie den von Ihnen gewünschten Scripts individuelle Script-Keys zur Ausführung festlegen.

HINWEIS: Globale Script-Key-Sets sind für alle Benutzer des KVM-Switches verfügbar.

Die Verwaltung der Script-Key-Sets erledigen Sie komfortabel mit einem Assistenten. Klicken auf das Menü **Erweiterte Funktionen** und wählen Sie **Script-Keys**. Zum Start des Assistenten klicken Sie auf **Konfigurieren**.

WICHTIG: Nur Benutzer mit **Superuser**-Rechten können Script-Keys in der Webapplikation verwalten.

Die folgende Abschnitte fassen die Konfigurationsoptionen des Assistenten kurz zusammen.

Schritt 1: Gerät auswählen

- Wählen Sie den KVM-Switch, auf dem die Konfiguration des Script-Key-Sets abgelegt wird.
- Wählen Sie im Feld **Script-Key-Modifizierer** *mindestens* eine der aufgeführten Modifizierertasten durch Markierung des entsprechenden Kontrollkästchens:

▪ Strg	▪ Win
▪ Alt	▪ Shift
▪ Alt Gr	

- Wählen Sie im Feld **Erlaubte Script-Keys** eine der aufgelisteten Optionen:

Nur Zahlen:	<i>nur Zifferntasten</i> werden bei gemeinsamer Betätigung mit dem Script-Key-Modifizierer als Script-Keys interpretiert
Nur Buchstaben:	<i>nur Buchstabentasten</i> werden bei gemeinsamer Betätigung mit dem Script-Key-Modifizierer als Script-Keys interpretiert
Zahlen und Buchstaben:	<i>Ziffern- und Buchstabentasten</i> werden bei gemeinsamer Betätigung mit dem Script-Key-Modifizierer als Script-Keys interpretiert

Schritt 2: Scripte zuordnen und Script-Key-Sets editieren

- Tragen Sie die gewünschten Tastenkombinationen zur Ausführung der Scripts bzw. Script-Gruppen ein.

NOTIZEN

A grid of small dots for taking notes.

NOTIZEN

A large grid of small, evenly spaced dots covering the majority of the page, intended for taking handwritten notes. The grid is composed of approximately 25 columns and 35 rows of dots.



G&D. FEELS RIGHT.

Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

Obere Leimbach 9 | D-57074 Siegen | Germany

Phone +49 271 23872-0

sales@gdsys.com | www.gdsys.com

US-Büro | US-Office

G&D North America Inc.

4540 Kendrick Plaza Drive, Suite 100 | Houston, TX 77032 | USA

Phone +1-346-620-4362

sales.us@gdsys.com | www.gdsys.com