# G&D VisionXS-IP-F-TypeC-UHR

**DE** Installation und Bedienung

**EN** Installation and Operation




A9100413-1.32

## 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

- USB Type-C® und USB-C® sind eingetragene Marken des USB Implementers Forum.
- Alle weiteren 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 2026. Alle Rechte vorbehalten.

**Version 1.32 – 24.07.2026**
Firmware: 1.8.000

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

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

www.gdsys.com
sales@gdsys.com

## FCC-Erklärung

Das Gerät entspricht Teil 15 der FCC-Bestimmungen. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Störungen verursachen und (2) dieses Gerät muss alle empfangenen Störungen aufnehmen, einschließlich Störungen, die den Betrieb beeinträchtigen.

**HINWEIS:** Dieses Gerät wurde getestet und entspricht den Bestimmungen für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Bestimmungen. Diese Grenzwerte bieten angemessenen Schutz vor schädlichen Störungen beim Betrieb des Geräts in Wohngebieten.

Dieses Gerät erzeugt und nutzt Hochfrequenzenergie und kann diese ausstrahlen Wenn es nicht gemäß der Anleitung installiert wird, kann es Funkstörungen verursachen. Es wird jedoch keinerlei Garantie dafür übernommen, dass die Störungen bei einer bestimmten Installation nicht auftreten.

Wenn dieses Gerät Störungen beim Rundfunk- oder Fernsehempfang verursacht, was durch Aus- und Einschalten des Geräts ermittelt werden kann, beheben Sie die Störung mithilfe einer oder mehrerer der folgenden Maßnahmen:

- Verändern Sie die Position der Empfangsantenne oder richten Sie diese neu aus.
- Erhöhen Sie den Abstand zwischen Gerät und Empfänger.
- Schließen Sie das Gerät an eine andere Steckdose oder einen anderen Stromkreis als den, mit dem das Empfangsgerät verbunden ist, an.
- Kontaktieren Sie den Händler oder einen erfahrenen Rundfunk-/Fernsehtechniker.

# Inhaltsverzeichnis

**Sicherheitshinweise** ..... **1**

**Die VisionXS-IP-F-TypeC-UHR-Serie** ..... **5**
Verwendung als Extender- oder Matrixswitch-Module ..... 5
Lieferumfang ..... 6

**Secure-KVM-over-IP-Lösung** ..... **7**
Mögliche Sicherheitslücken, Bedrohungen und Gefahren ..... 7
Schutz der KVM-Systeme vor Angriffen (von außen und innen) ..... 7
Sicherheitsanforderungen bei KVM-over-IP ..... 7
Die sichere Lösung von G&D ..... 8
Trusted-Computing-Platform ..... 10
Monitoring, SNMP und Syslog ..... 10
Update und Backup/Restore ..... 10
Weitere sicherheitsrelevante Aspekte ..... 11
2-Faktor-Authentifizierung (2FA) ..... 11
Optionale sicherheitsrelevante Zusatzfunktionen ..... 12
SecureCert ..... 12

**Signalübertragung und Übertragungslänge** ..... **13**

**Anforderung an den Netzwerk-Switch** ..... **13**
Voraussetzungen der Netzwerk-Switches ..... 13

**Installation** ..... **15**
Vorbereitung ..... 15
Installation des Rechnermoduls ..... 16
Installation des Arbeitsplatzmoduls ..... 24

**Inbetriebnahme** ..... **31**
Spannungsversorgung herstellen ..... 31
Startvorgang ..... 31
Spannungsversorgung trennen ..... 31
Bedienung ..... 32
Anmeldung am Arbeitsplatz ..... 33
Konfiguration der Passwort-Komplexität ..... 34
Konfiguration der Anmeldeoptionen ..... 36
Anzeigen von Nutzungsbedingungen ..... 38
Abmeldung am Arbeitsplatz ..... 39

**Ersteinrichtung der KVM-over-IP™-Verbindung** ..... **40**
Werkseinstellung der Module ..... 40
KVM-over-IP-Verbindung des Rechnermoduls konfigurieren ..... 41
Konfiguration der Netzwerkschnittstelle ..... 42
Konfiguration der globalen Netzwerkeinstellungen ..... 43
Konfiguration der KVM-over-IP-Verbindung ..... 44

KVM-over-IP-Verbindung des Arbeitsplatzmoduls konfigurieren ..... 45
Konfiguration der Netzwerkschnittstelle ..... 45
Konfiguration der globalen Netzwerkeinstellungen ..... 47
Konfiguration der KVM-over-IP-Verbindung ..... 48
Anlegen, Konfig. und Löschen einer Gegenstelle ..... 49
Erweiterte Einstellungen der KVM-over-IP-Verbindung ..... 51
Bandbreite limitieren ..... 51
Klassifizierung der IP-Pakete (DiffServ) ..... 52
Signale (de)aktivieren ..... 53
Beschränkung der KVM-over-IP-Gegenstelle (UID-Locking) ..... 54

**IP-MUX-Funktionalität ..... 55**
Aufschaltung einer Gegenstelle über das OSD ..... 55
Aufschaltung einer Gegenstelle mit Select-Keys ..... 56
Verbindung zu einer Gegenstelle beenden ..... 57

**Erstkonfiguration der Netzwerkeinstellungen ..... 58**
Konfiguration der Netzwerkschnittstelle ..... 59
Konfiguration der globalen Netzwerkeinstellungen ..... 61
Erreichbarkeit eines Hosts im Netzwerk prüfen (Ping) ..... 63
Link-Aggregation ..... 64
Status der Netzwerkschnittstellen auslesen ..... 66

**On-Screen-Display ..... 67**
Grundlegende Bedienung des On-Screen-Displays ..... 67
Anzeige des entfernten OSD ..... 68
Anzeige des lokalen OSD ..... 68
Aufbau des OSD ..... 68
Bedienung des OSD per Tastatur oder Maus ..... 69
Funktionen des OSD ..... 71
Suchfunktion ..... 71
Sortierung der Listeneinträge ändern ..... 71
Übersicht der Menüs des entfernten OSD ..... 72
Konfigurationsmenü ..... 72
Persönliches Profile-Menü ..... 74
Bedienung-Menü ..... 74
Information-Menü ..... 75
Übersicht der Menüs des lokalen OSD ..... 75
Auswahl-Menü ..... 75
Konfigurationsmenü ..... 76

**Freischaltung einer erworbenen Zusatzfunktion ..... 76**

**Webapplikation Config Panel ..... 77**
Grundlegende Bedienung der Webapplikation ..... 77
Start der Webapplikation ..... 77
Sprache der Webapplikation auswählen ..... 79
Webapplikation beenden ..... 79

**Benutzer und Gruppen** ..... **80**
Effizienter Einsatz der Rechteverwaltung ..... 80
Das Effektivrecht ..... 80
Effizienter Einsatz der Benutzergruppen ..... 81
Verwaltung von Benutzerkonten ..... 82
Anlegen eines neuen Benutzerkontos ..... 82
Änderung des Namens eines Benutzerkontos ..... 83
Änderung des Passworts eines Benutzerkontos ..... 84
Änderung der Rechte eines Benutzerkontos ..... 85
Änderung der Gruppenzugehörigkeit eines Benutzerkontos ..... 86
Aktivierung oder Deaktivierung eines Benutzerkontos ..... 87
Löschen eines Benutzerkontos ..... 87
Verwaltung von Benutzergruppen ..... 88
Anlegen einer neuen Benutzergruppe ..... 88
Änderung des Namens einer Benutzergruppe ..... 89
Änderung der Rechte einer Benutzergruppe ..... 89
Mitgliederverwaltung einer Benutzergruppe ..... 90
Aktivierung oder Deaktivierung einer Benutzergruppe ..... 91
Löschen einer Benutzergruppe ..... 91
System-Rechte ..... 92
Berechtigung zum uneingeschränkten Zugriff (Superuser) ..... 92
Berechtigung zum Ändern der Einstellungen des »Persönliches Profil«-Menüs ..... 93
Berechtigung zum Login in die Webapplikation ..... 93
Berechtigung zur Änderung des eigenen Passworts ..... 94
Zugriffsrecht auf ein Rechnermodul ..... 94
Zugriffsrecht auf USB-Geräte ..... 95

**Konfiguration** ..... **96**
Übersicht der Funktionen und Standardeinstellungen ..... 96
Konfigurationseinstellungen ..... 98
Betriebsarten von Arbeitsplatzmodulen ..... 98
Änderung des Namens des Arbeitsplatzmoduls ..... 99
Änderung des Namens des Rechnermoduls ..... 99
Änderung des eigenen Passworts ..... 100
Sprache auswählen ..... 101
Änderung des Hotkeys ..... 102
Änderung der OSD-Taste ..... 103
OSD mit doppeltem Tastendruck starten ..... 104
Kanalumschaltung bei Verwendung eines DH-Rechnermoduls ..... 105
Betriebsmodus der RS232-Schnittstelle einstellen ..... 106
Auswahl des EDID-Modus des KVM-Extenders ..... 107
Reduzierung der Farbtiefe der zu übertragenden Bilddaten ..... 108
Verwendung des Freeze-Modus ..... 109
DDC/CI-Unterstützung (de)aktivieren ..... 110
USB-Tastaturmodus oder »Generic USB« de(aktivieren) ..... 111
USB-Gerät für einen Neustart priorisieren ..... 113
Reinitialisierung von USB-Eingabegeräten ..... 114
Wartezeit des Bildschirmschoners einstellen ..... 115

Konfigurationseinstellungen (*Fortsetzung*)

Automatische Abmeldung der Benutzer einstellen ..... 115
Tastaturlayout für Eingaben innerhalb des OSD auswählen ..... 116
Wiederherstellung der Standardeinstellungen ..... 117
Reset der Netzfilterregeln ..... 118
Farbe der Informationseinblendung ändern ..... 119
Anzeige der Informationseinblendung ..... 120
Transparenz des OSD einstellen ..... 120
Automatisches Schließen des OSD nach Inaktivität ..... 121
Position der Informationseinblendung ändern ..... 121
Position des OSD ändern ..... 122

**Weiterführende Informationen** ..... **123**
DDC-Weiterleitung mit Cache-Funktion ..... 123
Ermittlung der Netzwerkeinstellungen über den Service-Port ..... 124
Installation des Gerätetreibers ..... 124
Einrichten einer Verbindung im Terminalemulationsprogramm ..... 124
Ermittlung der IP-Adresse ..... 125
Pin-Belegung der RS232-Schnittstelle ..... 125

**Statusanzeigen** ..... **126**
LED an der Frontseite des Rechnermoduls ..... 126
LED an der Vorderseite des Arbeitsplatzmoduls ..... 127
LEDs an der Rückseite ..... 128

**Verwendete Netzwerk-Ports und Protokolle** ..... **128**

**Technische Daten** ..... **129**
Allgemeine Eigenschaften der Serie ..... 129
Spezifische Eigenschaften der Geräte ..... 132
Eigenschaften der Übertragungsmodule ..... 136

# Sicherheitshinweise

Bitte lesen Sie die folgenden Sicherheitshinweise aufmerksam durch, bevor Sie das G&D-Produkt in Betrieb nehmen. Die Hinweise helfen Schäden am Produkt zu vermeiden und möglichen Verletzungen vorzubeugen.

Halten Sie diese Sicherheitshinweise für alle Personen griffbereit, die dieses Produkt benutzen werden.

Befolgen Sie alle Warnungen oder Bedienungshinweise, die sich am Gerät oder in dieser Bedienungsanleitung befinden.

### ⚠ Trennen Sie alle Spannungsversorgungen

**VORSICHT:** Risiko elektrischer Schläge!

Stellen Sie vor der Installation sicher, dass das Gerät von allen Stromquellen getrennt ist. Ziehen Sie alle Netzstecker und alle Spannungsversorgungen am Gerät ab.

### ⚠ Disconnect all power sources

**CAUTION:** Shock hazard!

Before installation, ensure that the device has been disconnected from all power sources. Disconnect all power plugs and all power supplies of the device.

### ⚠ Débranchez toutes les sources d'alimentation

**ATTENTION:** Risque de choc électrique!

Avant l'installation, assurez-vous que l'appareil a été débranché de toutes les sources d'alimentation. Débranchez toutes les fiches d'alimentation et toutes les alimentations électrique de l'appareil.

### ⚠ Vorsicht vor Stromschlägen

Um das Risiko eines Stromschlags zu vermeiden, sollten Sie das Gerät nicht öffnen oder Abdeckungen entfernen. Im Servicefall wenden Sie sich bitte an unsere Techniker.

### ⚠ Ständigen Zugang zu den Netzsteckern der Geräte sicherstellen

Achten Sie bei der Installation der Geräte darauf, dass die Netzstecker der Geräte jederzeit zugänglich bleiben.

### ⚠ Lüftungsöffnungen nicht verdecken

Bei Gerätevarianten mit Lüftungsöffnungen ist eine Verdeckung der Lüftungsöffnungen unbedingt zu vermeiden.

### ⚠ Korrekte Einbaulage bei Geräten mit Lüftungsöffnungen sicherstellen

Aus Gründen der elektrischen Sicherheit ist bei Geräten mit Lüftungsöffnungen grundsätzlich nur eine waagerechte, horizontale Einbauweise zulässig. Ein senkrechter, vertikaler Einbau ist nur mit passenden Geräteträgern von G&D zulässig.

### ⚠ Keine Gegenstände durch die Öffnungen des Geräts stecken

Stecken Sie keine Gegenstände durch die Öffnungen des Geräts. Es können gefährliche Spannungen vorhanden sein. Leitfähige Fremdkörper können einen Kurzschluss verursachen, der zu Bränden, Stromschlägen oder Schäden an Ihren Geräten führen kann.

### ⚠ Stolperfallen vermeiden

Vermeiden Sie bei der Verlegung der Kabel Stolperfallen.

### ⚠ Geerdete Spannungsquelle verwenden

Betreiben Sie dieses Gerät nur an einer geerdeten Spannungsquelle.

### ⚠ Verwenden Sie ausschließlich die G&D-Netzteile

Betreiben Sie dieses Gerät nur mit den mitgelieferten oder in der Bedienungsanleitung aufgeführten Netzteilen.

### ⚠ Keine mechanischen oder elektrischen Änderungen am Gerät vornehmen

Nehmen Sie keine mechanischen oder elektrischen Änderungen an diesem Gerät vor. Die Guntermann & Drunck GmbH ist nicht verantwortlich für die Einhaltung von Vorschriften bei einem modifizierten Gerät.

### ⚠ Geräteabdeckung nicht entfernen

Das Entfernen der Abdeckung darf nur von einem G&D-Service-Techniker durchgeführt werden. Bei unbefugtem Entfernen erlischt die Garantie. Die Nichtbeachtung dieser Vorsichtsmaßnahme kann zu Verletzungen und Geräteschäden führen!

### ⚠ Betreiben Sie das Gerät ausschließlich im vorgesehenen Einsatzbereich

Die Geräte sind für eine Verwendung im Innenbereich ausgelegt. Vermeiden Sie extreme Kälte, Hitze oder Feuchtigkeit.

## Hinweise zum Umgang mit Lithium-Knopfzellen

- Dieses Produkt enthält eine Lithium-Knopfzelle. Ein Austausch durch den Anwender ist nicht vorgesehen!

**VORSICHT:** Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Batterie-Typ ersetzt wird.

Entsorgen Sie gebrauchte Batterien umweltgerecht. Gebrauchte Batterien dürfen nicht in den Hausmüll geworfen werden.

Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

- This product contains a lithium button cell. It is not intended to be replaced by the user!

**CAUTION:** Risk of explosion if the battery is replaced by an incorrect battery type.

Dispose of used batteries in an environmentally friendly manner. Do not dispose of batteries in municipal waste.

Check local regulations for the disposal of electronic products.

- Ce produit contient une batterie au lithium. Il n'est pas prévu que l'utilisateur remplace cette batterie.

**ATTENTION:** Il y a danger d'explosion s'il y a remplacement incorrect de la batterie.

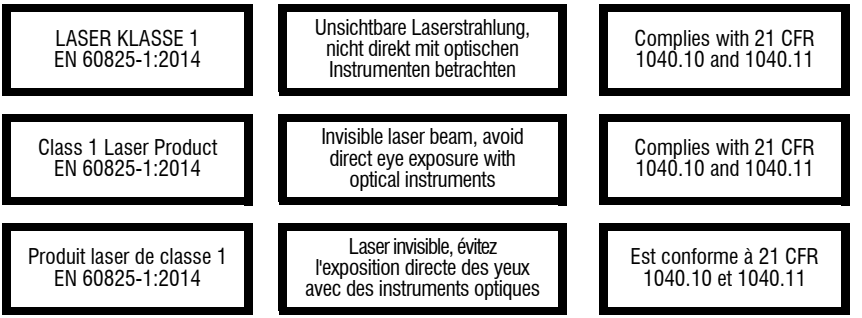
Mettre au rebut les batteries usagées conformêment aux instructions du fabricant et de manière écologique. Les batteries usagées ne doivent pas être jetées dans les ordures ménagères.

Respectez les prescriptions valables pour l'élimination des produits électroniques.

## Besondere Hinweise zum Umgang mit Laser-Technologie

Die Geräte der **VisionXS-IP-F-TypeC-UHR**-Serie verwenden Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 oder besser entsprechen.

Sie erfüllen dabei die Richtlinien gemäß **EN 60825-1:2014** sowie **U.S. CFR 1040.10** und **1040.11**.




Beachten Sie zum sicheren Umgang mit der Laser-Technologie folgende Hinweise:

### ⚠ Blickkontakt mit dem unsichtbaren Laserstrahl vermeiden

Betrachten Sie die unsichtbare Laserstrahlung niemals mit optischen Instrumenten!

### ⚠ Optische Anschlüsse stets verbinden oder mit Schutzkappen abdecken

Decken Sie die optischen Anschlüsse der *Transmission*-Buchsen und die Kabelstecker stets mit einer Schutzkappe ab, wenn diese nicht verbunden sind.

### ⚠ Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden

Es ist nicht zulässig, Lichtwellen-Module zu verwenden, die nicht der Laser-Klasse 1 gemäß **EN 60825-1:2014** entsprechen. Durch die Verwendung solcher Module kann die Einhaltung von Vorschriften und Empfehlungen zum sicheren Umgang mit Laser-Technologie nicht sichergestellt werden.

Die Gewährleistung zur Erfüllung aller einschlägigen Bestimmungen kann nur in der Gesamtheit der Originalkomponenten gegeben werden. Aus diesem Grund ist der Betrieb der Geräte ausschließlich mit solchen Übertragungsmodulen zulässig, die von G&D zertifiziert wurden.

# Die VisionXS-IP-F-TypeC-UHR-Serie

**WICHTIG:** Die Datenübertragung der Geräte der **IP**-Serien ist *nicht* kompatibel zu G&D-Geräten anderer Serien! Innerhalb der KVM-over-IP-Produktfamilien sind die Geräte untereinander kompatibel.

Die KVM-Extender der **VisionXS-IP-F-TypeC-UHR**-Serie bestehen aus einem Rechnermodul und einem Arbeitsplatzmodul.

An das Rechnermodul (**VisionXS-IP-CPU**) schließen Sie den zu bedienenden Rechner an. Den entfernten Arbeitsplatz schließen Sie an das Arbeitsplatzmodul (**VisionXS-IP-CON**).

Das Rechner- und das Arbeitsplatzmodul werden mit zwei Glasfasern über ein IP-basiertes Gigabit-Ethernet verbunden.

**HINWEIS:** Alternativ können Sie das Rechnermodul mittels einer direkten Verkabelung mit dem Arbeitsplatzmodul verbinden.

Die Signale von Tastatur und Maus sowie das Videosignal (DP1.2 Alt-Mode) des angeschlossenen Rechners werden über diese Fasern übertragen und erlauben die entfernte Bedienung des Rechners.

## Verwendung als Extender- oder Matrixswitch-Module

Sie können die Module wahlweise als Extender- oder Matrixswitch-Module verwenden:

- **Extender-Module:** Konfigurieren Sie eine KVM-over-IP-Verbindung zwischen dem Rechner- und dem Arbeitplatzmodul. Die konfigurierte Verbindung zwischen den Modulen wird bei jedem Neustart der Module wiederhergestellt.

**TIPP:** Verwenden Sie die **IP-MUX**-Funktionalität (s. Seite 55 ff.), um bis zu 20 Rechner über separate Rechnermodule im OSD verfügbar zu machen.

- **Matrixswitch-Module:** In Kombination mit dem IP-Matrixswitch **ControlCenter-IP** oder **ControlCenter-IP-XS** können Sie die Module als Endgeräte des Matrixswitches einsetzen.

In diesem Fall konfigurieren Sie für die Module eine KVM-over-IP-Verbindung zum IP-Matrixswitch.

In dieser Konfiguration ermöglicht der IP-Matrixswitch die flexible Aufschaltung eines Arbeitsplatzmoduls auf ein Rechnermodul.

# Lieferumfang

## Standardlieferumfang Rechnermodule

- 1 × Rechnermodul (**VisionXS-IP-CPU**), inkl. Übertragungsmodul/SFP-Transceiver
- 1 × TypeC-Anschlusskabel (*TypeC-Cable-M/M-2*)
- 1 × USB-Gerätekabel (*USB-AM/BM-2*)
- 1 × Sicherheitshinweise-Flyer
- 1 × Flyer »Korrekte Stromversorgung«

## Zusätzlicher Lieferumfang erweiterter Varianten

Die erweiterten Varianten der Rechnermodule der **VisionXS-IP-F-TypeC-UHR**-Serie werden *zusätzlich* mit den unten aufgeführten Kabeln ausgeliefert.

| **DT-VARIANTEN** |
|---|
| 1 × Stromversorgungskabel (PowerCable-2 Standard) |

| **A-VARIANTEN** |
|---|
| 1 × Audio-Kabel (Audio-M/M-2) |

| **AR-VARIANTEN** |
|---|
| 1 × Audio-Kabel (Audio-M/M-2) |
| 1 × serielles Anschlusskabel (RS232-M/F-2) |

## Standardlieferumfang Arbeitsplatzmodule

- 1 × Arbeitsplatzmodul (**VisionXS-IP-CON**), inkl. Übertragungsmodul/SFP-Transceiver
- 1 × Sicherheitshinweise-Flyer
- 1 × Flyer »Korrekte Stromversorgung«

## Zusätzlicher Lieferumfang erweiterter Varianten

Die erweiterten Varianten der Arbeitsplatzmodule der **VisionXS-IP-F-TypeC-UHR**-Serie werden *zusätzlich* mit den unten aufgeführten Kabeln ausgeliefert.

| **DT-VARIANTEN** |
|---|
| 1 × Stromversorgungskabel (PowerCable-2 Standard) |

# Secure-KVM-over-IP-Lösung

## Mögliche Sicherheitslücken, Bedrohungen und Gefahren

KVM-Lösungen sind das Rückgrat der IT-Infrastruktur. Entsprechend wichtig ist die Absicherung der gesamten KVM-Installation. Die Sicherheit der KVM-Systeme hängt insbesondere von zwei Faktoren ab. Zum einen müssen die Systeme bestmöglich vor Angriffen (von außen oder innen) geschützt sein. Zum anderen sind die Qualität und Zuverlässigkeit der eingesetzten KVM-Produkte und KVM-Installationen wichtig.

## Schutz der KVM-Systeme vor Angriffen (von außen und innen)

Durch den technischen Fortschritt, die vermehrte Digitalisierung von Prozessen und die immer stärkere Vernetzung von IT-Systemen entstehen auch neue Sicherheitslücken. Auf der einen Seite kann effizienter gearbeitet werden, auf der anderen Seite steigt die Anfälligkeit für Bedrohungen und Angriffe.

KVM-Matrixsysteme ermöglichen den Zugriff von mehreren Arbeitsplätzen auf mehrere Computer. Dies hat große Vorteile: der Workflow wird verbessert, die Steuerung vereinfacht und eine zentralisierte Administration ermöglicht. Ein erster großer und genereller Sicherheitsvorteil von KVM-Lösungen ist die Möglichkeit, die Rechner vom Arbeitsplatz zu entfernen und in einen zugangsgeschützten Technikraum auszulagern. Hierdurch wird Unbefugten der physische Rechner-Zugriff deutlich erschwert.

## Sicherheitsanforderungen bei KVM-over-IP

Klassische KVM-Systeme nutzen für die Übertragung CAT-x-Kupferkabel oder Glasfaser. Bei solchen KVM-Systemen ist in der Regel ein physischer Zugriff notwendig, um etwas manipulieren zu können, z. B. aktiv weitere unerwünschte Geräte zu integrieren.

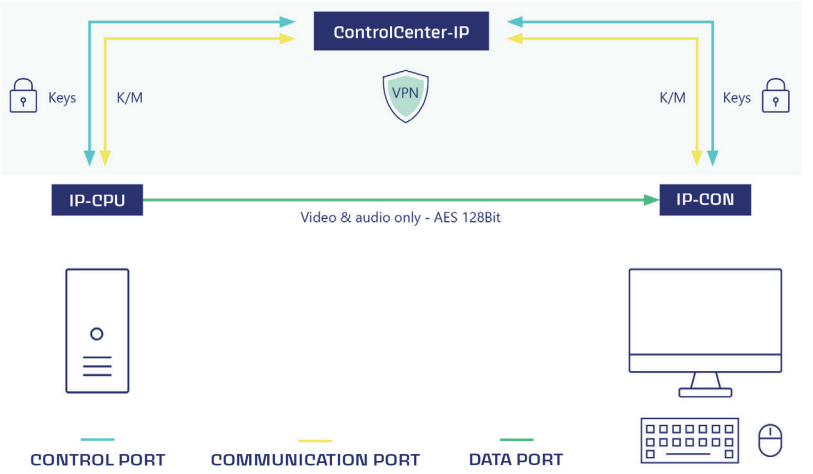
Bei KVM-over-IP-Systemen erfolgt die Übertragung IP-basiert über Ethernet-Netzwerke (OSI-Schichtenmodell Layer 3). Mit KVM-over-IP hat man aufgrund der Flexibilität und einfachen Erweiterbarkeit eine zukunftssichere Lösung. Jedoch steigt mit der IP-Übertragung auch das Sicherheitsrisiko. Es besteht hierbei eine zusätzliche Gefahr von außen, über das Internet oder intern über den einfacheren Zugang zum Netzwerk.

Mit entsprechender Software ist es grundsätzlich möglich, das komplette interne Netzwerk nach sogenannten Sicherheitslücken abzuscannen. Meistens wird als Ziel eines solchen Angriffs das schwächste Glied in der Kette anvisiert und attackiert. Dies können z. B. sogenannte Man-in-the-Middle-Attacken sein, bei denen der komplette Netzwerkverkehr an Dritte weitergegeben wird. Daher sind Netztrennung und Netzsegmentierung wichtige Werkzeuge, um die Anwendung vor Cyber-Angriffen zu schützen.

Bei KVM-over-IP-Systemen müssen sowohl Tastatur- und Mauseingaben als auch Video-, Audio-, USB- und RS232-Daten verschlüsselt werden, um zu verhindern, dass Unbefugte die Datenübertragungen abhören und so an interne Informationen, wie z. B. Logins und Passwörter, gelangen können. Ein regelmäßiger Austausch der Sicherheitsschlüssel ist obligatorisch. Um unerwünschte Zugriffe zu vermeiden, sind auch die Nutzung von VPN, VLANs und sicheren Verschlüsselungen erforderlich.

## Die sichere Lösung von G&D

G&D verwendet für die Datenübertragung im IP-Netzwerk verschiedene Ports. Jedes Endgerät (IP-CPU/IP-CON) wird über einen VPN-Tunnel mit der jeweiligen Gegenstelle oder einer KVM-over-IP-Matrix ControlCenter-IP oder ControlCenter-IP-XS verbunden. Es kommt ein AES256 Galois/Counter Mode (GCM) verschlüsselter IPSec VPN-Tunnel zum Einsatz (GCM basiert auf Counter Mode CTR, bietet aber zusätzlich einen integrierten Integritätsschutz). Es gibt zudem eine Abwärtskompatibilität für AES128-GCM.




Der erste Port, welcher von allen KVM-over-IP-Endgeräten zur jeweiligen Gegenstelle oder zur Matrix aufgebaut wird, ist der sogenannte Control-Port. Hier wird mittels eines selbstentwickelten Authentication-Plugins die Kommunikation der Endgeräte untereinander oder mit der Matrix ausgehandelt. Hierbei wird sichergestellt, dass nur Geräte von G&D auf Basis ihrer UID, Seriennummer und dem Trusted-Platform-Modul eine Verbindung herstellen können. Der Control-Port wird auch für den Austausch der jeweiligen Sicherheitsschlüssel, welche im Matrixbetrieb von der KVM-over-IP-Matrix oder im Extenderbetrieb vom Rechnermodul für jedes einzelne Endgerät generiert werden, genutzt.

Über den zweiten Port, den sogenannten Communication-Port, werden die Tastatur- und Mausdaten bidirektional übertragen.

Der Schlüsselaustausch für die sehr sicherheitsrelevanten Tastatur- und Mausdaten sowie die Steuerdaten erfolgt volldynamisch alle 40 bis 80 Minuten.

Die Videodaten werden vom Rechnermodul generiert und via UDP und MultiCast/ UniCast direkt zum Arbeitsplatzmodul übertragen (Data-Port). Für die Audio-, GenericUSB- und RS232-Daten sowie den Video-Stream, welcher vor dem Versenden in das G&D-eigene proprietäre Protokoll umgewandelt wird, wird AES128-Counter Mode (CTR) verwendet. Durch einen geheimen Geräteschlüssel, der benötigt wird, um die Videodaten zu entpacken, werden diese zusätzlich gesichert.

Das proprietäre Protokoll für dedizierte Verbindungen wird bei KVM-over-IP um eine volldynamische Verschlüsselung ergänzt. Der Schlüsselaustausch für diese Hochgeschwindigkeitsdaten erfolgt alle drei bis fünf Stunden oder bei Umschaltereignissen. Wenn sich ein Arbeitsplatzmodul mit einem Rechnermodul verbindet, wird ein Sicherheitsschlüssel für diese Verbindung generiert. Sobald sich im Matrixbetrieb ein weiteres Arbeitsplatzmodul auf dieses Rechnermodul aufschaltet, erhalten beide Arbeitsplatzmodule neue Sicherheitsschlüssel. Umgekehrt wird auch ein neuer Sicherheitsschlüssel an das verbleibende Arbeitsplatzmodul geschickt, wenn das andere Modul die Verbindung beendet.

Durch die Trennung der Kontrolldaten (Control-Port) und der Tastatur- und Mausdaten (Communication-Port) von Video-, Audio-, GenericUSB- und RS232-Daten (Data-Port) werden diverse Angriffszenarien, wie z. B. Man-In-The-Middle-Attacken bereits im Ansatz verhindert. Wird die Ziel-IP-Adresse oder der VPN-Tunnel kompromittiert, werden keine neuen Sicherheitsschlüssel mehr vergeben, die KVM-Endgeräte sowie das Matrix-System schalten in den Sicherheitsmodus und stoppen die Übertragung der Daten.

## Trusted-Computing-Platform

Der Bootloader, das Betriebssystem und die Firmware der Geräte bilden eine sogenannte Trusted Computing Platform. Basierend auf einem Bausteinkern nach Sicherheitsstandard FIPS140-2 sichert ein integriertes Trusted-Platform-Modul sämtliche Zugangs- und Konfigurationsdaten vor dem Ausspähen oder der Manipulation durch Dritte. Zum Einsatz kommt dabei ein RSA-Verschlüsselungsverfahren mit einer Schlüssellänge von 2048 Bit.

Sensible Informationen wie Anmeldeinformationen und Passwörter werden im Matrixbetrieb dauerhaft und verschlüsselt in der Datenbank des ControlCenter-IP oder ControlCenter-IP-XS gespeichert oder im Extenderbetrieb in der Datenbank des Rechnermoduls. Diese Datenbank ist im Betriebssystem von G&D implementiert, TPM-geschützt und basiert beim ControlCenter-IP zudem auf einem Hardware-Raid. Mögliche Modifikationen der Firmware können frühzeitig erkannt werden, was zu einer Unterbrechung des Bootvorgangs führt. Manipulationsversuche, wie z. B. das Ein-schmuggeln eines Keyboard-Sniffers, werden verhindert.

TPM stellt sicher, dass ein Gerät nur mit Software gebootet wird, die vom Hersteller als vertrauenswürdig eingestuft wurde.

## Monitoring, SNMP und Syslog

Die Features Monitoring und SNMP ermöglichen dem Systemverantwortlichen, den Status der installierten Geräte und der angeschlossenen Peripherie zu überwachen. Die Informationen werden über das Web-Interface der jeweiligen Geräte zur Verfügung gestellt. Durch die permanente Erkennung und Meldung besteht die Möglichkeit, frühzeitig auf kritische Zustände wie beispielsweise eine Temperatur-überschreitung, eine nicht mehr vorhandene Kommunikation auf der Keyboard-Schnittstelle oder ein gefährdetes Redundanzsystem zu reagieren. Hierdurch vermeiden Sie präventiv Systemausfälle. Verfügbarkeitszeiten werden erhöht, und sowohl Anwender als auch der Systemverantwortliche können effizienter arbeiten.

Über Syslog (System Logging Protocol) werden verschiedene Ereignisse als Reaktion auf sich ändernde Bedingungen generiert. Die Ereignisse werden lokal protokolliert und können von einem Administrator überprüft und analysiert werden. Die Syslog-Meldungen können zusätzlich an einen Syslog-Server versendet werden. Mit Syslog lassen sich so beispielsweise relevante Systemänderungen, Anmeldungen und Anmeldefehlversuche protokollieren.

## Update und Backup/Restore

Konfigurationseinstellungen können über die Backup-Funktion gesichert werden. Mit der Auto-Backup-Funktion kann in einem definierten Intervall ein automatisches Backup auf einem Netzlaufwerk erstellt werden. Somit muss kein manuelles Backup angelegt werden, nachdem eine Konfigurationsoption geändert wurde. Das Wiederherstellen der gesicherten Daten ist über die Restore-Funktion möglich.

## Weitere sicherheitsrelevante Aspekte

Alle Rechnermodule (CPUs) von G&D lassen sich so konfigurieren, dass automatisch eine Abmeldung am Betriebssystem des Computers erfolgt, sobald sich ein Benutzer am Arbeitsplatzmodul abmeldet. Dies verhindert, dass der Computer ungewollt im offenen Zugriff bleibt und sich ein anderer Benutzer ohne eigene Anmeldung auf den Rechner aufschalten kann.

Der Einsatz des optionalen UID-Locking schränkt die nutzbaren Endgeräte zuverlässig ein. Nach Aktivierung können keine weiteren Endgeräte hinzugefügt oder ausgetauscht werden.

Optionale USB2.0-Datenverbindungen können zudem über das intelligente Benutzermanagement auf Hardware-Ebene deaktiviert werden.

Ein weiterer wichtiger Aspekt ist die Gerätesicherheit auf der Benutzerseite. KVM-Endgeräte von G&D speichern keine Informationen ab. Es ist also nicht möglich, ein physisch entwendetes Gerät auszulesen, um zwischengespeicherte Anmeldedaten zu erhalten.

Zur Einhaltung individueller Passwort-Richtlinien und zur Verbesserung der Sicherheit kann systemweit die Passwort-Komplexität (minimale Passwortlänge Mindestanzahl an Groß-/Kleinbuchstaben, Mindestanzahl an Ziffern, Mindestanzahl an Sonderzeichen, Mindestanzahl an zu verändernden Zeichen im Vergleich zum vorherigen Passwort) konfiguriert werden.

Zur Verbesserung der Sicherheit stehen im Bereich der Anmeldeoptionen weitere Konfigurationsmöglichkeiten zur Verfügung. Es kann festgelegt werden, wie viele Fehlversuche bei der Passworteingabe akzeptiert werden und wie lange ein Benutzer nach dem Überschreiten der Anzahl maximaler Fehlversuche gesperrt wird. In diesem Bereich kann auch bestimmt werden, wie viele gleichzeitige Superuser-Sitzungen erlaubt sind.

Zudem können Nutzungsbedingungen hinterlegt werden, die ein Benutzer vor jedem (erneuten) Gerätezugriff akzeptieren muss.

## 2-Faktor-Authentifizierung (2FA)

Um die Sicherheit zu erhöhen, kann durch die Zwei-Faktor-Authentifizierung (2FA) ein zweiter, besitzbasierter Faktor abgefragt werden.

Hierbei kommt ein Time-Based-One-Time-Password (TOTP) zum Einsatz, wobei es sich um ein zeitlich begrenzt gültiges und nur einmalig nutzbares Passwort handelt. Es können Authenticator-Apps oder Hardware-Tokens verwendet werden.

# Optionale sicherheitsrelevante Zusatzfunktionen

## SecureCert

Mit dem SecureCert Feature können bei den Produktgruppen ControlCenter-IP, ControlCenter-IP-XS, VisionXS-IP, VisionXS-IP 2.0, Vision-IP und RemoteAccess-IP-CPU zertifizierte Sicherheitsfunktionen aktiviert werden, die im Rahmen der Zertifizierungen FIPS 140-3, DoDIN APL und CC EAL2+ zur Verfügung gestellt werden. Geräte mit aktiviertem SecureCert-Feature entsprechen den Anforderungen der genannten Standards und wurden in entsprechenden Prozessen konform getestet und zertifiziert.

**WICHTIG:** Das SecureCert-Feature kann ausschließlich in der Produktion programmiert werden. Daher ist die Beauftragung des Features nur zusammen mit einem Gerät möglich. Nachträglich ist das SecureCert-Feature **nicht** aktivierbar.

**TIPP:** Für den Matrixbetrieb stehen Ihnen weitere kostenpflichtige Zusatzfunktionen zur Verfügung. Ausführliche Hinweise hierzu finden Sie im Handbuch des Matrixswitches.

# Signalübertragung und Übertragungslänge

Die Signalübertragung zwischen dem Rechner- und dem Arbeitsplatzmodul erfolgt komprimiert und verschlüsselt mittels G&Ds **KVM-over-IP™**-Technologie (siehe *Die sichere Lösung von G&D* auf Seite 8) über das Gigabit-Ethernet (Layer 3). Alternativ können das Rechnermodul und das Arbeitsplatzmodul auch direkt miteinander verbunden werden. Hierbei ist die Übertragungslänge beschränkt (s. Abschnitt *Eigenschaften der Übertragungsmodule* des Kapitels *Technische Daten*).

Bei ausreichend nutzbarer Bandbreite des Gigabit-Ethernets wird das Videosignal mit verlustfreier Videoqualität und nahezu latenzfrei wiedergegeben. Mittels manuellem Bandbreiten-Management können Sie die Übertragung an unterschiedliche Bandbreitenanforderungen anpassen (siehe *Bandbreite limitieren* auf Seite 51).

Bei Beachtung der max. Länge von Teilstrecken zwischen zwei *aktiven* Netzwerkkomponenten (s. Abschnitt *Eigenschaften der Übertragungsmodule* des Kapitels *Technische Daten*) ist die gesamte Übertragungslänge unbeschränkt.

# Anforderung an den Netzwerk-Switch

**HINWEIS:** Im Extenderbetrieb ist keine *Multicast*-Übertragung vorgesehen. Hierdurch werden deutlich weniger Anforderungen an den Netzwerkswitch gestellt als dies im Matrixbetrieb der Fall ist.

**WICHTIG:** Die Netzwerk-Switches sollten im Hinblick auf eine Systemerweiterung möglichst auch die Anforderungen für einen Matrixbetrieb erfüllen (*Multicast*, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* und *Spanning Tree TCN Flooding*). Weitere Informationen hierzu finden Sie im Installationshandbuch des Matrixswitches.

## Voraussetzungen der Netzwerk-Switches

Folgende Voraussetzungen gelten für das Netzwerk:

- Mindestens **Layer-2-Managed-Switch**
- **VLAN-Unterstützung** um den KVM-over-IP-Datenverkehr von anderen Netzwerkoperationen zu trennen

- **QoS mit DiffServ-/DSCP-Unterstützung** zur Performance-Steigerung und Priorisierung: Quality-of-Service (QoS) ist eine Paketpriorisierung, die sicherstellt, dass zeitlich kritische oder wichtige Anwendungen ihre Daten bevorzugt über das Netzwerk erhalten. Dank DiffServ-/DSCP-Unterstützung werden Datenpakete markiert und entsprechend der Konfiguration vom Netzwerk verarbeitet. DSCP spezifiziert, wie genau mit einem Paket verfahren wird.

  **HINWEIS:** Berücksichtigen Sie, dass einige Netzwerkswitches für *alle* Datenpakete automatisch die Service-Klasse **Network Control** (DSCP-Name: **CS6**) vergeben. In solchen Umgebungen darf die Option **DSCP 48** nicht ausgewählt werden!

- **Ausreichende Performance** des Netzwerkswitches **sicherstellen**: Forwarding-Bandbreite, Switching-Kapazität und Forwarding-Performance überprüfen.

  **BEISPIEL:** Typische Bandbreitenanforderungen bei KVM-over-IP

  VisionXS-IP-Modelle gibt es in mehreren Varianten: DVI-I, DP-HR und DP-HR-DH mit 1 Gbit; DP-UHR und TypeC-UHR mit Multi-Gbit (1-10 Gbit). Die Bandbreite ist standardmäßig unbegrenzt, kann aber optional begrenzt werden.

  - 1920 × 1080 = 300-400 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung: z. B. VisionXS-IP-DVI-I)
  - 2560 × 1440 = 500-600 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung: z. B. VisionXS-IP-DP-HR)
  - 2 × 2560 × 1440 = 800-900 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung: z. B. VisionXS-IP-DP-HR-DH)
  - 3840 × 2160 = 2000-2500 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung: z. B. VisionXS-IP-DP-UHR)
    die maximale Videobandbreitennutzung beträgt 5 Gbit/s
  - Standbild: 25 Mbit/s bei 3840 × 2160

  **WICHTIG:** Es ist darauf zu achten, dass der Uplink von Access-Switch zu Core-/Main-Switch ausreichend für die Anzahl und den Betriebsmodus der verbundenen Endgeräte dimensioniert ist.

  **BEISPIEL:**

  - 30 × *VisionXS-IP-DP-HR-CPU* bei 10Gbit-Uplink
  - Uplink mit 10 Gbit/s ist ein Nadelöhr, da 30 × 1Gbit/s bei den CPUs sichergestellt werden müsste.

# Installation

**WICHTIG:** Die Geräte verwenden Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 entsprechen.

Sie erfüllen die Richtlinien gemäß **EN 60825-1:2014** sowie **U.S. CFR 1040.10** und **1040.11**.

Beachten Sie diesbezüglich folgende Sicherheitshinweise:

- *Blickkontakt mit dem unsichtbaren Laserstrahl vermeiden* auf Seite 4
- *Optische Anschlüsse stets verbinden oder mit Schutzkappen abdecken* auf Seite 4

## Vorbereitung

**WICHTIG:** Stellen Sie bei der Standortwahl der Geräte sicher, dass die zulässige Umgebungstemperatur (siehe *Technische Daten* auf Seite 129) in der unmittelbaren Nähe eingehalten und nicht durch andere Geräte beeinflusst wird.

Sorgen Sie für eine ausreichende Luftzirkulation.

**WICHTIG:** Bei Gerätevarianten mit Lüftungsöffnungen ist eine Verdeckung der Lüftungsöffnungen zu vermeiden. Aus Gründen der elektrischen Sicherheit ist bei diesen Gerätevarianten nur eine waagerechte, horizontale Einbauweise zulässig. Ein senkrechter, vertikaler Einbau ist nur mit passenden Geräteträgern von G&D zulässig.

Betreiben Sie Geräte mit Lüftungsöffnungen nicht in einer staubhaltigen Umgebung. Staub im Gehäuse kann die Elektronik im Inneren beschädigen und zu Fehlfunktionen des Gerätes führen!

1. Stellen Sie sicher, dass der an das Rechnermodul anzuschließende Rechner ausgeschaltet ist. Falls der Rechner mit einer Tastatur und einer Maus verbunden ist, ziehen Sie die Kabel der Eingabegeräte aus den Schnittstellen.
2. Platzieren Sie das Rechnermodul (**VisionXS-IP-CPU**) in der Nähe des Rechners.

   **HINWEIS:** Die maximale Kabellänge zwischen dem Rechnermodul und dem anzuschließenden Rechner beträgt *zwei* Meter.

3. Platzieren Sie das kompatible Arbeitsplatzmodul in der Nähe des entfernten Arbeitsplatzes.

   **HINWEIS:** Die maximale Kabellänge zwischen dem Arbeitsplatzmodul und den Geräten des Arbeitsplatzes beträgt *zwei* Meter.

4. Entnehmen Sie die mitgelieferten Kabel der Verpackung und legen Sie diese für die Installation der Geräte bereit.

# Installation des Rechnermoduls

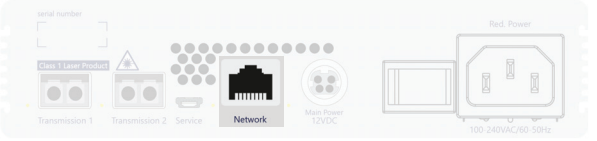
**HINWEIS:** Alle Gerätevarianten der **VisionXS-IP**-Serie können mit einer *externen* Spannungsversorgung an der **Power**-Schnittstelle (bei DT-Varianten: **Main Power**) betrieben werden.

Die Geräte unterstützen USB Power Delivery. Sie können nur als Energieempfänger (Senke) eingesetzt werden (siehe *Stromversorgung herstellen* auf Seite 20).

Die Abbildungen in diesem Kapitel zeigen die DT-Variante der Geräteserie. Diese Variante ist zusätzlich mit einem *internen* Netzteil (**Red. Power**) ausgestattet.

An das Rechnermodul **VisionXS-IP-CPU** schließen Sie den Rechner an, dessen Signale an den entfernten Arbeitsplatz übertragen werden.

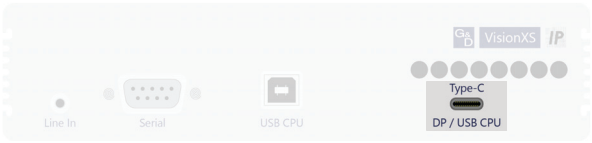
## Verbindung mit einem lokalen Management-Netzwerk herstellen




**HINWEIS:** Verbinden Sie diese Netzwerkschnittstelle – falls gewünscht – mit einem lokalen Netzwerk, um aus diesem Netzwerk auf die Webapplikation **Config Panel** zuzugreifen und beispielsweise Syslog-Meldungen in diese Netzwerke zu senden.

**Network:** Stecken Sie das als Zubehör erhältliche Twisted-Pair-Kabel der Kategorie 5 (oder höher) ein. Verbinden Sie das andere Ende des Kabels mit dem lokalen Netzwerk.

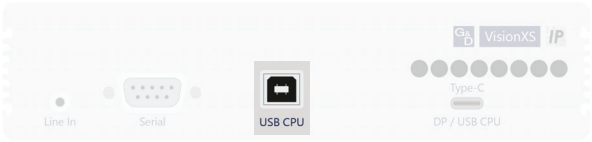
## Tastatur- und Maussignale des Rechners anschließen




**Type-C DP/USB CPU:** Verbinden Sie eine USB-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *TypeC-Cable-M/M-2*.

**HINWEIS:** Die **Type-C DP/USB CPU**-Schnittstelle wird primär zum Einspeisen von Videodaten verwendet. Sie verarbeitet aber auch USB-Daten. Somit muss keine separate USB-Verbindung gesteckt werden.

**WICHTIG:** Falls dennoch eine separate USB-Verbindung über die **USB-CPU**-Schnittstelle gesteckt wird, wird diese vorrangig verwendet.



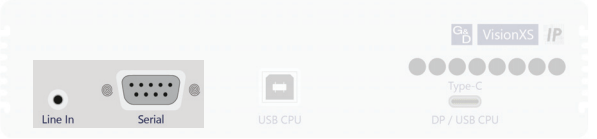

**USB CPU:** Verbinden Sie eine USB-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *USB-AM/BM-2*.

## Videoausgang des Rechners anschließen




**Type-C/DP/USB CPU:** Verbinden Sie eine USB-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *TypeC-Cable-M/M-2*.

## Audio- und RS232-Schnittstellen verbinden (modellabhängig)



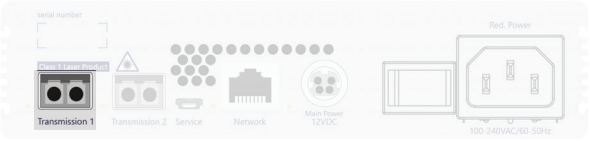

**HINWEIS:** In der *Standard*einstellung werden die Audio-Daten vom KVM-Extender übertragen. Die Übertragung der RS232-Daten ist deaktiviert.

Sie können im OSD die Übertragung der RS232-Daten aktivieren und/oder die Übertragung der Audio-Daten deaktivieren (siehe *Signale (de)aktivieren* auf Seite 53).

**Line In:** Verbinden Sie die *Line-Out*-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu ein Audio-Anschlusskabel *Audio-M/M-2*.

**Serial:** Verbinden Sie eine 9-polige serielle Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *RS232-M/F-2*.

## Verbindung mit dem Gigabit-Ethernet herstellen




**WICHTIG:** Das Gerät verwendet Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 entsprechen.

Betrachten Sie die unsichtbare Laserstrahlung niemals mit optischen Instrumenten!

**HINWEIS:** Entfernen Sie die Schutzkappen der *Transmission*-Schnittstellen und der Kabelstecker.

**Transmission 1|Tx:** Stecken Sie den LC-Stecker des als Zubehör erhältlichen Glasfaserkabels ein. Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

**Transmission 1|Rx:** Stecken Sie den LC-Stecker des als Zubehör erhältlichen Glasfaserkabels ein. Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

**HINWEIS:** Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy**-Features aktiviert die **Transmission 2**-Schnittstelle.

Für die Verwendung der **Transmission 2**-Schnittstelle benötigen Sie einen zusätzlichen kostenpflichtig erhältlichen **SFP-Transceiver**. Wählen Sie passend zu Ihrer Variante der **VisionXS-IP-F-TypeC-UHR**-Serie den passenden SFP-Transceiver. Die **Transm. Redundancy Optionen** beinhalten *sowohl* einen entsprechenden **SFP-Transceiver** *als auch* das **Transm. Redundancy-Feature**.

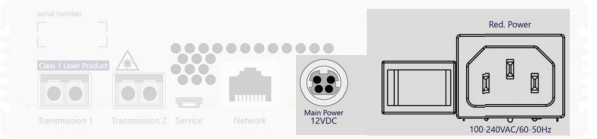
Verwenden Sie diese Schnittstelle um eine redundante *Transmission*-Verbindung (*Link Aggregation*) mit dem Gigabit-Netzwerk herzustellen.

## Stromversorgung herstellen

**HINWEIS:** Alle Gerätevarianten der **VisionXS-IP**-Serie können mit einer *externen* Spannungsversorgung an der **Power**-Schnittstelle (bei DT-Varianten: **Main Power**) betrieben werden.

Die Abbildungen in diesem Kapitel zeigen die DT-Variante der Geräteserie. Diese Variante ist zusätzlich mit einem *internen* Netzteil (**Red. Power**) ausgestattet.

**WICHTIG:** Die DT-Varianten beziehen die Spannung konstruktionsbedingt bevorzugt über das *externe* Netzteil (**Main Power**). Sollte das *externe* Netzteil ausfallen oder beispielsweise aufgrund eines Austausches vorübergehend nicht verfügbar sein, wird das Gerät automatisch über das *interne* Netzteil (**Red. Power**) mit der erforderlichen Spannung versorgt.




**Power/Main Power:** Schließen Sie die externe Spannungsversorgung an diese Buchse an.

**Red. Power:** Stecken Sie ein Kaltgerätekabel ein. Hierdurch wird eine zweite, redundante Stromversorgung des Gerätes erreicht.

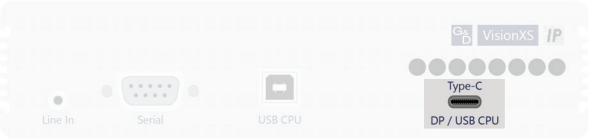
**WICHTIG:** Alle G&D-Geräte enthalten aufgedruckte Informationen zur jeweiligen Stromaufnahme. Vergewissern Sie sich bitte, dass das zu verwendende Netzteil mindestens die erforderliche Leistung bereitstellt.

Unser Support unterstützt Sie gern bei der Sicherstellung der korrekten Stromversorgung.

Eine Stromversorgung mit unzureichender Leistung kann zu unerwartetem Verhalten führen und den Betrieb des Geräts dauerhaft beeinträchtigen!

**HINWEIS:** Das Gerät unterstützt USB Power Delivery. Es kann nur als Energieempfänger (Senke) eingesetzt werden.

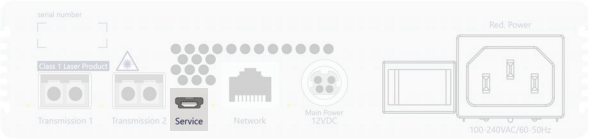
**WICHTIG:** Zur Durchführung von Updates ist die alleinige Spannungsversorgung über USB Power Delivery **nicht** ausreichend.



**Type-C DP/USB CPU:** Verbinden Sie eine USB-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *TypeC-Cable-M/M-2*.

## Service-Schnittstelle

Das Gerät besitzt an der Rückseite eine Service-Schnittstelle. Diese Schnittstelle hat für den Benutzer im normalen Betrieb keine relevante Funktion.




In einem Terminalemulationsprogramm (beispielsweise *HyperTerminal* oder *PuTTY*) können Debug-, Fehler- und Statusmeldungen angezeigt werden. Über ein Service-Menü haben Techniker die Möglichkeit, Informationen über das Gerät auszulesen, eine temporäre Deaktivierung der Netzfilterregeln durchzuführen, das Gerät auf die Werkseinstellungen zurückzusetzen oder einen Neustart durchzuführen.

Das Service-Menü wird über ein beliebiges Terminalemulationsprogramm bedient. Der Rechner auf dem das Terminalemulationsprogramm installiert ist, wird über ein Service-Kabel mit der Service-Buchse des Geräts verbunden.

**So richten Sie eine Verbindung im Terminalemulationsprogramm ein:**

**HINWEIS:** Installieren Sie vor der Einrichtung der Verbindung im Terminalemulationsprogramm den Gerätetreiber *CP210x USB to UART Bridge VCP*.

Dieser Treiber stellt die per Servicekabel verbundene *Service*-Buchse des **VisionXS-IP**-Systems als virtuelle serielle Schnittstelle (COM-Port) zur Verfügung. Die virtuelle Schnittstelle kann anschließend im Terminalemulationsprogramm zum Verbindungsaufbau ausgewählt werden.

Der Treiber steht auf der Website **www.gdsys.com/de** im Bereich **Service > Downloads > Tools & Treiber** zum Download zur Verfügung.

1. Starten Sie ein beliebiges Terminalemulationsprogramm (z. B. *HyperTerminal* oder *PuTTY*).

2. Erstellen Sie eine neue Verbindung im Terminalemulationsprogramm und erfassen Sie die folgenden Verbindungseinstellungen:
   - Bits pro Sekunde: 460.800
   - Datenbits: 8
   - Parität: Keine
   - Stoppbits: 1
   - Flusssteuerung: Keine
3. Verwenden Sie ein Datenkabel, um den Rechner mit der Service-Buchse an der Rückseite des **VisionXS-IP** zu verbinden.

**HINWEIS:** Der Login für das Service-Menü erfolgt über den Benutzernamen *service* und das Passwort *service*. Bei Geräten mit aktiviertem *SecureCert Feature* ist das Service-Menü frei zugänglich

4. Im Service-Menü stehen folgende Optionen zur Verfügung:
   - Quit (**nicht** sichtbar bei Geräten mit aktiviertem *SecureCert Feature*)
   - System information
   - Set system defaults: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.
   - Reboot: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.
   - Temporary deactivation of the network filter rules: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.

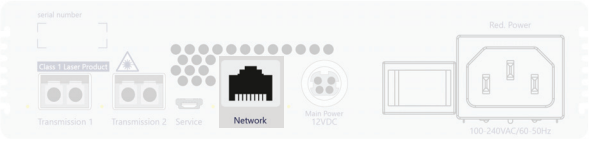
# Installation des Arbeitsplatzmoduls

**HINWEIS:** Alle Gerätevarianten der **VisionXS-IP**-Serie können mit einer *externen* Spannungsversorgung an der **Power**-Schnittstelle (bei DT-Varianten: **Main Power**) betrieben werden.

Die Abbildungen in diesem Kapitel zeigen die DT-Variante der Geräteserie. Diese Variante ist zusätzlich mit einem *internen* Netzteil (**Red. Power**) ausgestattet.

An das Arbeitsplatzmodul **VisionXS-IP-CON** schließen Sie den entfernten Arbeitsplatz an. An diesem Arbeitsplatz können Sie den am Rechnermodul angeschlossenen Rechner bedienen.

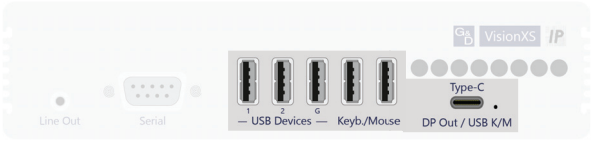
## Verbindung mit einem lokalen Management-Netzwerk herstellen




**HINWEIS:** Verbinden Sie diese Netzwerkschnittstelle – falls gewünscht – mit einem lokalen Netzwerk, um aus diesem Netzwerk auf die Webapplikation **Config Panel** zuzugreifen und beispielsweise Syslog-Meldungen in diese Netzwerke zu senden.

**Network:** Stecken Sie ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5 (oder höher) ein. Verbinden Sie das andere Ende des Kabels mit dem lokalen Netzwerk.

## Tastatur und Maus des Arbeitsplatzes sowie weitere Geräte anschließen




**Keyb./Mouse:** Schließen Sie die USB-Maus und/oder die -Tastatur des Arbeitsplatzes an.

**USB Devices:** In der Standardeinstellung können Sie an diese Schnittstellen weitere USB-Eingabegeräte, USB-Massenspeichergeräte und/oder ein unterstütztes Display bzw. Tablet anschließen.

Aktivieren Sie den **Generic-USB**-Modus (siehe *USB-Tastaturmodus oder »Generic USB« de(aktivieren)* auf Seite 111), wenn Sie ein anderes USB-Eingabegerät oder ein USB-Massenspeichergerät anschließen möchten. Die Daten des USB-Gerätes werden in diesem Modus *unverändert* an das Rechnermodul übertragen.

**WICHTIG:** Bei aktiviertem **Generic-USB**-Modus kann das OSD mit einer Tastatur an den **USB Devices**-Buchsen nicht bedient werden.

**WICHTIG:** Das Produkt erlaubt die gleichzeitige Nutzung von bis zu fünf Generic-USB-Geräten über ein Arbeitsplatzmodul. Hierfür muss sowohl das eingesetzte Arbeitsplatzmodul als auch das eingesetzte Rechnermodul die Nutzung von bis zu fünf GenericUSB-Geräten unterstützen.

Es können nur bis zu drei HighSpeed-Geräte (z. B. USB-Flashdrive) und zwei FullSpeed-Devices verwendet werden. Werden darüber hinaus weitere High-Speed-Geräte verbunden, werden diese nicht akzeptiert.

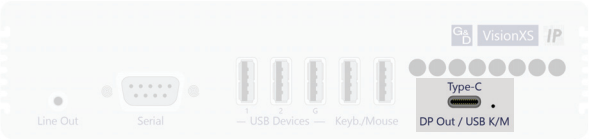
**HINWEIS:** Am Arbeitsplatzmodul stehen Ihnen *drei* **Generic**-Schnittstellen zur Verfügung. Für den Anschluss von *vier* oder *fünf* Generic-USB-Geräten benötigen Sie daher einen USB-Hub oder ein USB-Verbundgerät.

Die zwei **Keyb./Mouse**-Schnittstellen können *nicht* für den **Generic-USB**-Modus verwendet werden.

**HINWEIS:** Die USB-Type-C-Schnittstelle, welche primär zur Ausgabe von Videodaten verwendet wird, bietet auch die Möglichkeit USB-K/M-Daten anzunehmen. Somit können USB-Tastatur und USB-Maus mit einem USB-Hub eines Monitors verbunden werden.

**Type-C/DP Out/USB K/M:** Schließen Sie den Monitor des Arbeitsplatzes an

## Monitor des Arbeitsplatzes anschließen




**Type-C/DP Out/USB K/M:** Schließen Sie den Monitor des Arbeitsplatzes an

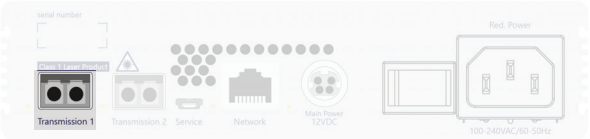
## Audio- und RS232-Schnittstellen verbinden (modellabhängig)




**Line Out:** Schließen Sie die Lautsprecher oder ein anderes Audioausgabegerät des Arbeitsplatzes an.

**Serial:** Verbinden Sie das serielle Endgerät mit dieser Schnittstelle.

## Verbindung mit dem Gigabit-Ethernet herstellen




**WICHTIG:** Das Gerät verwendet Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 entsprechen.

Betrachten Sie die unsichtbare Laserstrahlung niemals mit optischen Instrumenten!

**HINWEIS:** Entfernen Sie die Schutzkappen der *Transmission*-Schnittstellen und der Kabelstecker.

**Transmission 1|Tx:** Stecken Sie den LC-Stecker des als Zubehör erhältlichen Glasfaserkabels ein. Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

**Transmission 1|Rx:** Stecken Sie den LC-Stecker des als Zubehör erhältlichen Glasfaserkabels ein. Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

**HINWEIS:** Die Freischaltung des kostenpflichtig erhältlichen **Transm. Redundancy**-Features aktiviert die **Transmission 2**-Schnittstelle.

Für die Verwendung der **Transmission 2**-Schnittstelle benötigen Sie einen zusätzlichen kostenpflichtig erhältlichen **SFP-Transceiver**. Wählen Sie passend zu Ihrer Variante der **VisionXS-IP-F-TypeC-UHR**-Serie den passenden SFP-Transceiver. Die **Transm. Redundancy Optionen** beinhalten *sowohl* einen entsprechenden **SFP-Transceiver** *als auch* das **Transm. Redundancy-Feature**.

Verwenden Sie diese Schnittstelle um eine redundante *Transmission*-Verbindung (*Link Aggregation*) mit dem Gigabit-Netzwerk herzustellen.

## Stromversorgung herstellen

**HINWEIS:** Alle Gerätevarianten der **VisionXS-IP**-Serie können mit einer *externen* Spannungsversorgung an der **Power**-Schnittstelle (bei DT-Varianten: **Main Power**) betrieben werden.

Die Abbildungen in diesem Kapitel zeigen die DT-Variante der Geräteserie. Diese Variante ist zusätzlich mit einem *internen* Netzteil (**Red. Power**) ausgestattet.

**WICHTIG:** Die DT-Varianten beziehen die Spannung konstruktionsbedingt bevorzugt über das *externe* Netzteil (**Main Power**). Sollte das *externe* Netzteil ausfallen oder beispielsweise aufgrund eines Austausches vorübergehend nicht verfügbar sein, wird das Gerät automatisch über das *interne* Netzteil (**Red. Power**) mit der erforderlichen Spannung versorgt.

**Power/Main Power:** Schließen Sie eine externe Spannungsversorgung an diese Buchse an.

**Red. Power:** Stecken Sie ein Kaltgerätekabel ein. Hierdurch wird eine zweite, redundante Stromversorgung des Gerätes erreicht.

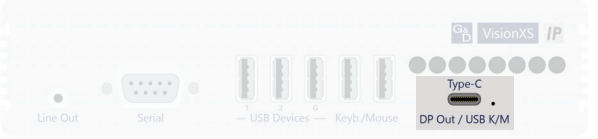
**WICHTIG:** Alle G&D-Geräte enthalten aufgedruckte Informationen zur jeweiligen Stromaufnahme. Vergewissern Sie sich bitte, dass das zu verwendende Netzteil mindestens die erforderliche Leistung bereitstellt.

Unser Support unterstützt Sie gern bei der Sicherstellung der korrekten Stromversorgung.

Eine Stromversorgung mit unzureichender Leistung kann zu unerwartetem Verhalten führen und den Betrieb des Geräts dauerhaft beeinträchtigen!

**HINWEIS:** Das Gerät unterstützt USB Power Delivery. Es kann nur als Energieempfänger (Senke) eingesetzt werden.

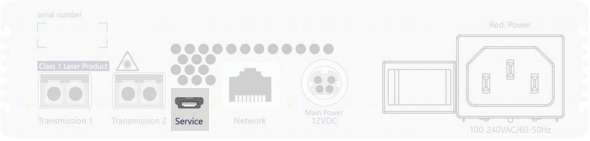
**WICHTIG:** Zur Durchführung von Updates ist die alleinige Spannungsversorgung über USB Power Delivery **nicht** ausreichend.




**Type-C/DP Out/USB K/M:** Schließen Sie den Monitor des Arbeitsplatzes an

## Service-Schnittstelle

Das Gerät besitzt an der Rückseite eine Service-Schnittstelle. Diese Schnittstelle hat für den Benutzer im normalen Betrieb keine relevante Funktion.




In einem Terminalemulationsprogramm (beispielsweise *HyperTerminal* oder *PuTTY*) können Debug-, Fehler- und Statusmeldungen angezeigt werden. Über ein Service-Menü haben Techniker die Möglichkeit, Informationen über das Gerät auszulesen, eine temporäre Deaktivierung der Netzfilterregeln durchzuführen, das Gerät auf die Werkseinstellungen zurückzusetzen oder einen Neustart durchzuführen.

Das Service-Menü wird über ein beliebiges Terminalemulationsprogramm bedient. Der Rechner auf dem das Terminalemulationsprogramm installiert ist, wird über ein Service-Kabel mit der Service-Buchse des Geräts verbunden.

**So richten Sie eine Verbindung im Terminalemulationsprogramm ein:**

**HINWEIS:** Installieren Sie vor der Einrichtung der Verbindung im Terminalemulationsprogramm den Gerätetreiber *CP210x USB to UART Bridge VCP*.

Dieser Treiber stellt die per Servicekabel verbundene *Service*-Buchse des **VisionXS-IP**-Systems als virtuelle serielle Schnittstelle (COM-Port) zur Verfügung. Die virtuelle Schnittstelle kann anschließend im Terminalemulationsprogramm zum Verbindungsaufbau ausgewählt werden.

Der Treiber steht auf der Website **www.gdsys.com/de** im Bereich **Service > Downloads > Tools & Treiber** zum Download zur Verfügung.

1. Starten Sie ein beliebiges Terminalemulationsprogramm (z. B. *HyperTerminal* oder *PuTTY*).

2. Erstellen Sie eine neue Verbindung im Terminalemulationsprogramm und erfassen Sie die folgenden Verbindungseinstellungen:
   - Bits pro Sekunde: 460.800
   - Datenbits: 8
   - Parität: Keine
   - Stoppbits: 1
   - Flusssteuerung: Keine
3. Verwenden Sie ein Datenkabel, um den Rechner mit der Service-Buchse an der Rückseite des **VisionXS-IP** zu verbinden.

**HINWEIS:** Der Login für das Service-Menü erfolgt über den Benutzernamen *service* und das Passwort *service*. Bei Geräten mit aktiviertem *SecureCert Feature* ist das Service-Menü frei zugänglich

4. Im Service-Menü stehen folgende Optionen zur Verfügung:
   - Quit (**nicht** sichtbar bei Geräten mit aktiviertem *SecureCert Feature*)
   - System information
   - Set system defaults: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.
   - Reboot: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.
   - Temporary deactivation of the network filter rules: Es wird eine Bestätigung *Are you sure? [y]es, [N]o* (*Standard*) angezeigt.

# Inbetriebnahme

Nach der ordnungsgemäßen Installation der KVM-Extender können diese sofort in Betrieb genommen werden.

**WICHTIG:** Die DT-Varianten beziehen die Spannung konstruktionsbedingt bevorzugt über das *externe* Netzteil (**Main Power**). Sollte das *externe* Netzteil ausfallen oder beispielsweise aufgrund eines Austausches vorübergehend nicht verfügbar sein, wird das Gerät automatisch über das *interne* Netzteil (**Red. Power**) mit der erforderlichen Spannung versorgt.

## Spannungsversorgung herstellen

Beachten Sie folgende Reihenfolge bei der Erstinbetriebnahme der Module:

1. Schließen Sie die *externe* Spannungsversorgung an das **Arbeitsplatzmodul** an *und/oder* schalten Sie das interne Netzteil (nur DT-Varianten) ein.
2. Schließen Sie die *externe* Spannungsversorgung an das **Rechnermodul** an *und/oder* schalten Sie das interne Netzteil (nur DT-Varianten) ein.
3. Schalten Sie den am Rechnermodul angeschlossenen **Rechner** ein.

**HINWEIS:** Die empfohlene Einschaltreihenfolge für die Erstinbetriebnahme stellt sicher, dass die KVM-Extender die Eigenschaften des angeschlossenen Monitors auslesen und an den Rechner weiterleiten können
(siehe *DDC-Weiterleitung mit Cache-Funktion* auf Seite 123).

## Startvorgang

Nach der Inbetriebnahme signalisieren die LEDs den Betriebszustand des Moduls.

Weitere Hinweise hierzu erhalten Sie im Kapitel *Statusanzeigen* ab Seite 126.

## Spannungsversorgung trennen

Beachten Sie folgende Reihenfolge beim Trennen der Spannungsversorgung:

1. Trennen Sie die *externe* Spannungsversorgung vom **Rechnermodul** *und/oder* schalten Sie das interne Netzteil (nur DT-Variante) aus.
2. Trennen Sie die *externe* Spannungsversorgung vom **Arbeitsplatzrmodul** *und/oder* schalten Sie das interne Netzteil (nur DT-Variante) aus.

## Bedienung

**WICHTIG:** *Standard*mäßig ist die OpenAccess-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart *nicht* durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

Den am Rechnermodul angeschlossene Rechner können Sie am entfernten Arbeitsplatz des Arbeitsplatzmoduls bedienen.

**HINWEIS:** Die Verbindung zwischen dem Rechner- und dem Arbeitsplatzmodul wird automatisch nach dem Start der Module aufgebaut.

**WICHTIG:** Bei Geräten mit aktiviertem *SecureCert Feature* ist *standardmäßig* die Standard-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

## Anmeldung am Arbeitsplatz

**WICHTIG:** Bevor Sie sich am Arbeitsplatz anmelden, stellen Sie bitte sicher, dass das richtige Tastaturlayout ausgewählt ist. Standardmäßig ist das deutsche Tastaturlayout eingestellt. Falls Sie ein anderes Layout benötigen, muss dies vor der Anmeldung manuell angepasst werden, damit Ihre Eingaben – insbesondere bei Passwörtern – korrekt erkannt werden
(siehe *Tastaturlayout für Eingaben innerhalb des OSD auswählen* ab Seite 116).

Alternativ kann das Tastaturlayout auch über die Webapplikation ConfigPanel geändert werden. Weitere Informationen hierzu finden Sie im separaten Handbuch zur Webapplikation.

**HINWEIS:** Falls anstelle der OpenAccess-Betriebsart (*Standard* im Extenderbetrieb, außer bei Geräten mit aktiviertem *SecureCert Feature*) die Betriebsart *Standard* eingestellt wurde, fordert das System nach dem Einschalten des Arbeitsplatzes zur Anmeldung des Benutzers auf.

**So melden Sie sich als Benutzer am System an:**

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

| | |
|---|---|
| **(Nutzungs-) Bedingungen:** | Betätigen Sie die **Eingabtaste**, um die Nutzungsbedingungen angezeigt zu bekommen. |
| **Akzeptieren (der Nutzungs-bedingungen):** | Betätigen Sie die **F8**-Taste, um die Nutzungsbedingungen zu akzeptieren. |
| **Benutzername:** | Geben Sie Ihren Benutzernamen ein. |
| **Passwort:** | Geben Sie das Passwort Ihres Benutzerkontos ein. |
| **2-Factor Auth Code (TOTP):** | Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein. |

2. Betätigen Sie die **Eingabetaste**, um die Anmeldung durchzuführen und das On-Screen-Display zu öffnen.

**WICHTIG:** Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde
(siehe *Anzeigen von Nutzungsbedingungen* auf Seite 38).

**WICHTIG:** Das Feld *2-Factor Auth Code (TOTP)* erscheint nur bei aktivierter 2-Faktor-Authentifizierung. Weitere Informationen hierzu finden Sie im separaten Handbuch zur Webapplikation.

## Konfiguration der 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* auf Seite 84) und Anlage eines neuen Benutzerkontos (siehe *Anlegen eines neuen Benutzerkontos* auf Seite 82) 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 stellen Sie die minimale Passwortlänge ein:**

1. Starten Sie das On-Screen-Display (OSD) mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. Länge** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte minimale Passwortlänge ein (*Standard*: 3 bzw. 15 bei aktiviertem *SecureCert-Feature*)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So stellen Sie die Mindestanzahl an Großbuchstaben innerhalb eines Passworts ein:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. Großbuchstaben** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Mindestanzahl an Großbuchstaben innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So stellen Sie die Mindestanzahl an Kleinbuchstaben innerhalb eines Passworts ein:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. Kleinbuchstaben** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Mindestanzahl an Kleinbuchstaben innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So stellen Sie die Mindestanzahl an Ziffern innerhalb eines Passworts ein:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. Ziffern** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Mindestanzahl an Ziffern innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So stellen Sie die Mindestanzahl an Sonderzeichen innerhalb eines Passworts ein:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. Sonderzeichen** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Mindestanzahl an Sonderzeichen innerhalb eines Passworts ein (*Standard*: 0 bzw. 1 bei aktiviertem *SecureCert-Feature*)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So stellen Sie die Mindestanzahl an unterschiedlichen Zeichen für eine Passwortänderung im Vergleich zum vorherigen Passwort ein:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Passwort-Komplexität** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Min. unterschiedlich** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Mindestanzahl an unterschiedlichen Zeichen für eine Passwortänderung im Vergleich zum vorherigen Passworts ein (*Standard*: 0 bzw. 8 bei aktiviertem *SecureCert-Feature*)

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

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der Anmeldeoptionen

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

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

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

**So legen Sie die Anzahl der maximalen Fehlversuche bei der Passworteingabe fest:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Anmeldeoptionen** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Max. Fehlversuche** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Anzahl an maximalen Fehlversuchen bei der Passworteingabe ein (*Standard*: 0 = aus/unbegrenzte Anzahl an Fehlversuchen bzw. 3 bei aktiviertem *SecureCert-Feature*, max. 1.000)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So legen Sie die Sperrzeit für den Fall fest, dass die Anzahl der maximalen Fehlversuche bei der Passworteingabe überschritten wird:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Anmeldeoptionen** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Sperrzeit** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Sperrzeit in Minuten an, für die ein Nutzer nach dem Überschreiten der Anzahl an maximalen Fehlversuchen bei der Passworteingabe gesperrt wird (*Standard*: 1 (wenn max. Fehlversuche > 0) bzw. 15 bei aktiviertem *SecureCert-Feature*, max. 1.440 Minuten)
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So legen Sie die maximale Anzahl gleichzeitiger Superuser-Sitzungen fest:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Anmeldeoptionen** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Max. Superuser-Sitzungen** und betätigen Sie die **Eingabetaste**.
5. Geben Sie die gewünschte Anzahl an maximalen Superuser-Sitzungen ein (*Standard*: 0 = aus/unbegrenzte Anzahl an Superuser-Sitzungen, max. 1.024)

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

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Anzeigen von Nutzungsbedingungen

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

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

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Nutzungsbedingungen-Konfig.** und betätigen Sie die **Eingabetaste**.
4. Markieren Sie die Zeile **Nutzungsbedingungen** wählen Sie mit der Taste **F8** zwischen folgenden Optionen:

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

5. Falls Sie im vorherigen Schritt *Benutzer* ausgewählt haben, sind im Folgenden die individuellen Nutzungsbedingungen zu erfassen. Wählen Sie die Zeile **Kurztext...** und betätigen Sie die **Eingabetaste**.
6. Erfassen Sie 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.
7. Betätigen Sie die **F2**-Taste zur Speicherung der Texteingabe.
8. Betätigen Sie die **Esc**-Taste, um wieder in die vorherige Maske zu gelangen.
9. Wählen Sie die Zeile **Langtext...** und betätigen Sie die Eingabetaste.
10. Erfassen Sie nun die gewünschten Nutzungsbedingungen. Dieses Textfeld ist auf 1.500 Zeichen begrenzt.
11. Betätigen Sie die **F2**-Taste zur Speicherung der Texteingabe.
12. Betätigen Sie die **Esc**-Taste und anschließend die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Abmeldung am Arbeitsplatz

Mit der *Benutzer abmelden*-Funktion melden Sie sich vom System ab. Wenn die Betriebsart *Standard* eingestellt wurde, wird nach der erfolgreichen Abmeldung die *Anmelden*-Maske angezeigt.

**WICHTIG:** Verwenden Sie immer die *Benutzer abmelden*-Funktion nach Abschluss Ihrer Arbeit am System. Der Arbeitsplatz sowie das System werden so gegen unautorisierten Zugriff geschützt.

**So melden Sie sich als Benutzer vom System ab:**

1. Starten Sie das On-Screen-Display mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F9**-Taste zum Aufruf des *Bedienung*-Menüs.
3. Betätigen Sie die Schnellwahltaste **E** oder markieren Sie die Zeile **E - Benutzer abmelden** und betätigen Sie die **Eingabetaste**.

**TIPP:** Bereits nach dem Aufruf des On-Screen-Displays können Sie mit der Tastenkombination **Strg+E** die *Benutzer abmelden*-Funktion durchführen.

# Ersteinrichtung der KVM-over-IP™-Verbindung

**WICHTIG:** Wenn Sie den KVM-Extender als Matrixswitch-Endgerät mit dem IP-Matrixswitch **ControlCenter-IP** oder **ControlCenter-IP-XS** verwenden, können Sie die **KVM-over-IP™-Verbindung** komfortabel über die Webapplikation des IP-Matrixswitches einrichten (s. Anleitung der *Webapplikation des IP-Matrixswitches*).

Die manuelle Konfiguration, wie in diesem Kapitel beschrieben, ist in diesem Fall *nicht* erforderlich.

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

Für die Kommunikation zweier Module miteinander sind verschiedene Einstellungen erforderlich. In der Werkseinstellung sind die Module so konfiguriert, dass ein Rechner- und ein Arbeitsplatzmodul sofort eine Direktverbindung aufbauen können.

Alle Rechnermodule werden mit der IP-Adresse **172.17.0.10** und alle Arbeitsplatzmodule mit der IP-Adresse **172.17.0.11** vorkonfiguriert.

**WICHTIG:** Ändern Sie die voreingestellten IP-Adressen, bevor Sie mehrere Rechner- bzw. Arbeitsplatzmodule in das Produktivnetzwerk integrieren!

**TIPP:** Falls Ihnen die IP-Adresse eines bereits konfigurierten Arbeitsplatz- oder Rechnermoduls unbekannt ist, können Sie diese über die Log-Ausgaben des Gerätes ermitteln. Weiterführende Informationen finden Sie im Abschnitt *Ermittlung der Netzwerkeinstellungen über den Service-Port* auf Seite 124.

## Werkseinstellung der Module

Die Werkseinstellung der Module ermöglicht den schnellen Aufbau einer Direktverbindung zwischen einem Rechner- und einem Arbeitsplatzmodul. Über das OSD können Sie die Konfiguration beider Module nach der Inbetriebnahme anpassen.

Die IP-Adressen und die **KVM-over-IP**-Einstellungen sind wie folgt vorkonfiguriert:

| WERKSEINSTELLUNG DES RECHNERMODULS (CPU) | |
|---|---|
| **IP-Adresse:** | 172.17.0.10 |
| **Netzmaske** | 255.255.0.0 |
| **Control Port:** | 18246 |
| **Communication Port:** | 18245 |
| **Data Port:** | 18244 |

| WERKSEINSTELLUNG DES ARBEITSPLATZMODULS (CON) | |
|---|---|
| **IP-Adresse:** | 172.17.0.11 |
| **Netzmaske** | 255.255.0.0 |
| **Local Control Port:** | 18246 |
| **Local Communication Port:** | 18245 |
| **Local Data Port:** | 18244 |
| **Remote Host:** | 172.17.0.10 |
| **Remote Control Port:** | 18246 |

**HINWEIS:** Für den Aufbau der **KVM-over-IP**-Verbindung durch das Arbeitsplatzmodul sind die Angabe der **IP-Adresse** des Rechnermoduls (Host) sowie die Angabe des **Control Ports** des Rechnermoduls erforderlich.

Die Konfiguration der **Communication Ports** und **Data Ports** werden automatisch zwischen beiden Modulen ausgetauscht.

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

## KVM-over-IP-Verbindung des Rechnermoduls konfigurieren

Die erforderlichen Konfigurationseinstellungen können Sie direkt am Arbeitsplatz durchführen.

**HINWEIS:** Sie können am Arbeitsplatz mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**) das lokale OSD des Arbeitsplatzmoduls und mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**) das entfernte OSD des Rechnermodus aufrufen und konfigurieren.

Während des Startvorgangs des Arbeitsplatzmoduls werden die Einstellungen beider Hotkeys angezeigt (siehe *Startvorgang* auf Seite 31).

**WICHTIG:** Das OSD des Rechnermoduls kann nur aufgerufen werden, wenn eine **KVM-over-IP**-Verbindung zum Rechnermodul aufgebaut ist.

Ändern Sie daher *zunächst* die Konfiguration des Rechnermoduls!

## Konfiguration der Netzwerkschnittstelle

**So konfigurieren Sie die Netzwerkschnittstelle:**

1. Verwenden Sie den Remote-Hotkey **Strg+Num** zum Aufruf des OSD.
2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.
4. Erfassen Sie im Abschnitt **Transmission** folgende Daten:

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

| | |
|---|---|
| **Betriebsmodus:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus der Schnittstelle:<br>▪ **aus:** Netzwerkschnittstelle ausschalten.<br>▪ **Statisch IPv4:** Es wird eine statische IPv4-Adresse zugeteilt.<br>▪ **DHCPv4:** Bezug der IPv4-Adresse von einem DHCP-Server. |
| **IP-Adresse:** | Geben Sie die IPv4-Adresse der Schnittstelle an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung autom. bezogen.* |
| **Netzmaske:** | Geben Sie die Netzmaske des Netzwerkes an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung automatisch bezogen.* |
| **IPv6:** | Betätigen Sie die **F8**-Taste um IPv6 zu aktivieren (**aktiviert**). Standardmäßig ist IPv6 deaktiviert (**aus**).<br>**HINWEIS:** Bei der Aktivierung von IPv6 wird gemäß RFC 4921 standardmäßig eine link-lokale IPv6-Adresse anhand der MAC-Adresse der Schnittstelle generiert. Diese link-lokale IPv6-Adresse ist vom Anwender nicht veränderbar. |
| **Statische IPv6-Adresse:** | Geben Sie die statische IPv6-Adresse der Schnittstelle an. |
| **Präfix:** | Geben Sie die Präfixlänge (*Standard*: 64) gemäß den Notationsregeln nach RFC 5952 für die Schnittstelle an. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der globalen Netzwerkeinstellungen

Die globalen Netzwerkeinstellungen stellen auch in komplexen Netzwerken sicher, dass der KVM-Extender aus allen Teilnetzwerken erreichbar ist.

**So konfigurieren Sie die globalen Netzwerkeinstellungen:**

1. Verwenden Sie den Remote-Hotkey **Strg**+**Num** zum Aufruf des Rechnermodul-OSD.
2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.
4. Erfassen Sie im Abschnitt **Main-Netzwerk** folgende Daten:

| | |
|---|---|
| **Globale Einstellungen:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus:<br>▪ **Statisch:** Verwendung von statischen Einstellungen.<br>▪ **Dynamisch:** Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6). |
| **Host-Name:** | Geben Sie den Host-Namen des Matrixswitches ein. |
| **Domain:** | Geben Sie die Domäne an, welcher der Matrixswitch angehören soll. |
| **Gateway IPv4:** | Geben Sie die IPv4-Adresse des Gateways an. |
| **Gateway IPv6:** | Geben Sie die IPv6-Adresse des Gateways an. |
| **DNS 1:** | Geben Sie die IP-Adresse des DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **DNS 2:** | Geben Sie optional die IP-Adresse eines weiteren DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **IPv6 Vorrang einräumen:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja**, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (*Standard*: **nein**). |
| **SLAAC verwenden:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*, wenn *SecureCert-Feature* nicht aktiviert), falls SLAAC verwendet werden soll. Ansonsten wählen Sie **nein** (*Standard* bei aktiviertem *SecureCert-Feature*). |

| | |
|---|---|
| **Mcast Echo Reply senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls ICMPv6 Echo Requests beantwortet werden sollen. Ansonsten wählen Sie **nein**. |
| **DestUnreach senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann. Ansonsten wählen Sie **nein**. |
| **Redirects verarbeiten (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen. Ansonsten wählen Sie **nein**. |
| **Dupl. addr. detection (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird. Ansonsten wählen Sie **nein**. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der KVM-over-IP-Verbindung

Für den Aufbau der **KVM-over-IP**-Verbindung durch das Arbeitsplatzmodul sind die Angabe der **IP-Adresse** des Rechnermoduls (Host) sowie die Angabe des **Control Ports** des Rechnermoduls erforderlich.

**HINWEIS:** Die Konfiguration der **Communication Ports** und **Data Ports** werden automatisch zwischen beiden Modulen ausgetauscht.

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

1. Verwenden Sie den Remote-Hotkey **Strg+Num** zum Aufruf des Rechnermodul-OSD.
2. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
3. Erfassen Sie im Abschnitt **Netzwerk-Einstellungen** folgende Daten:

| | |
|---|---|
| **Control-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |
| **Communication-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |
| **Data-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

# KVM-over-IP-Verbindung des Arbeitsplatzmoduls konfigurieren

Die erforderlichen Konfigurationseinstellungen können Sie direkt am Arbeitsplatz durchführen.

**HINWEIS:** Sie können am Arbeitsplatz mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**) das lokale OSD des Arbeitsplatzmoduls und mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**) das entfernte OSD des Rechnermodus aufrufen und konfigurieren.

Während des Startvorgangs des Arbeitsplatzmoduls werden die Einstellungen beider Hotkeys angezeigt (siehe *Startvorgang* auf Seite 31).

## Konfiguration der Netzwerkschnittstelle

**So konfigurieren Sie die Netzwerkschnittstelle:**

1. Verwenden Sie den lokalen Hotkey **Alt**+**Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **Netzwerk** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.

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

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

| | |
|---|---|
| **Betriebsmodus:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus der Schnittstelle:<br>▪ **aus:** Netzwerkschnittstelle ausschalten.<br>▪ **Statisch IPv4:** Es wird eine statische IPv4-Adresse zugeteilt.<br>▪ **DHCPv4:** Bezug der IPv4-Adresse von einem DHCP-Server. |
| **IP-Adresse:** | Geben Sie die IPv4-Adresse der Schnittstelle an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung autom. bezogen.* |
| **Netzmaske:** | Geben Sie die Netzmaske des Netzwerkes an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung automatisch bezogen.* |
| **IPv6:** | Betätigen Sie die **F8**-Taste um IPv6 zu aktivieren (**aktiviert**). Standardmäßig ist IPv6 deaktiviert (**aus**).<br>**HINWEIS:** Bei der Aktivierung von IPv6 wird gemäß RFC 4921 standardmäßig eine link-lokale IPv6-Adresse anhand der MAC-Adresse der Schnittstelle generiert. Diese link-lokale IPv6-Adresse ist vom Anwender nicht veränderbar. |
| **Statische IPv6-Adresse:** | Geben Sie die statische IPv6-Adresse der Schnittstelle an. |
| **Präfix:** | Geben Sie die Präfixlänge (*Standard*: 64) gemäß den Notationsregeln nach RFC 5952 für die Schnittstelle an. |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der globalen Netzwerkeinstellungen

Die globalen Netzwerkeinstellungen stellen auch in komplexen Netzwerken sicher, dass der KVM-Extender aus allen Teilnetzwerken erreichbar ist.

**So konfigurieren Sie die globalen Netzwerkeinstellungen:**

1. Verwenden Sie den lokalen Hotkey **Alt+Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **Netzwerk** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.
5. Erfassen Sie im Abschnitt **Main-Network** folgende Daten:

| | |
|---|---|
| **Globale Einstellungen:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus:<br>▪ **Statisch:** Verwendung von statischen Einstellungen.<br>▪ **Dynamisch:** Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6). |
| **Host-Name:** | Geben Sie den Host-Namen des Matrixswitches ein. |
| **Domain:** | Geben Sie die Domäne an, welcher der Matrixswitch angehören soll. |
| **Gateway IPv4:** | Geben Sie die IPv4-Adresse des Gateways an. |
| **Gateway IPv6:** | Geben Sie die IPv6-Adresse des Gateways an. |
| **DNS 1:** | Geben Sie die IP-Adresse des DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **DNS 2:** | Geben Sie optional die IP-Adresse eines weiteren DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **IPv6 Vorrang einräumen:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja**, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (*Standard*: **nein**). |
| **SLAAC verwenden:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*, wenn *SecureCert-Feature* nicht aktiviert), falls SLAAC verwendet werden soll. Ansonsten wählen Sie **nein** (*Standard* bei aktiviertem *SecureCert-Feature*). |

| | |
|---|---|
| **Mcast Echo Reply senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls ICMPv6 Echo Requests beantwortet werden sollen. Ansonsten wählen Sie **nein**. |
| **DestUnreach senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann. Ansonsten wählen Sie **nein**. |
| **Redirects verarbeiten (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen. Ansonsten wählen Sie **nein**. |
| **Dupl. addr. detection (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird. Ansonsten wählen Sie **nein**. |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der KVM-over-IP-Verbindung

Für den Aufbau der **KVM-over-IP**-Verbindung durch das Arbeitsplatzmodul sind die Angabe der **IP-Adresse** des Rechnermoduls (Host) sowie die Angabe des **Control Ports** des Rechnermoduls erforderlich.

**HINWEIS:** Die Konfiguration der **Communication Ports** und **Data Ports** werden automatisch zwischen beiden Modulen ausgetauscht.

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

1. Verwenden Sie den lokalen Hotkey **Alt+Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.

**WICHTIG:** Um die Konfiguration der KVM-over-IP-Verbindung vor ungewünschtem Zugriff zu schützen, empfehlen wir den Passwortschutz zu aktivieren. Wählen Sie die Zeile **Passwortschutz**, betätigen Sie die **F8**-Taste (**An**) und anschließend die **F2**-Taste zur Speicherung der durchgeführten Änderung.

4. Erfassen Sie im Abschnitt **Lokal** folgende Daten:

| | |
|---|---|
| **Control-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |
| **Communication-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |
| **Data-Port:** | Geben Sie die Nummer des zu verwendenden Ports ein. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Anlegen, Konfig. und Löschen einer Gegenstelle

**So legen Sie eine neue Gegenstelle an:**

1. Verwenden Sie den lokalen Hotkey **Alt+Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **IP-MUX** und betätigen Sie die **Eingabetaste**.
5. Betätigen Sie die **F3**-Taste zum Anlegen einer neuen Gegenstelle.
6. Erfassen Sie folgende Daten:

| | |
|---|---|
| **Name:** | Geben Sie den im *Select*-Menü anzuzeigenden Namen der Gegenstelle ein. |
| **Host-Name:** | Geben Sie die **IP-Adresse**/den **Host-Name** der Gegenstelle ein. |

**HINWEIS:** Im **Host-Name**-Feld können Sie mit der Tastenkombination **Strg+F8** den Dialog **Gefundene Geräte** öffnen. In diesem Dialog werden Ihnen alle *nicht* gekoppelten G&D-Gegenstellen (Rechnermodule und Matrixswitches) angezeigt.

Wählen Sie die gewünschte Gegenstelle aus und betätigen Sie die **Eingabetaste**, um die IP-Adresse der Gegenstelle zu übernehmen.

7. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So konfigurieren Sie eine Gegenstelle:**

1. Verwenden Sie den lokalen Hotkey **Alt+Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **IP-MUX** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie mit den Pfeiltasten die zu konfigurierende Gegenstelle und betätigen Sie **F5**-Taste.
6. Erfassen/bearbeiten Sie folgende Daten:

| | |
|---|---|
| **Name:** | Geben Sie den im *Select*-Menü anzuzeigenden Namen der Gegenstelle ein. |
| **Host-Name:** | Geben Sie die **IP-Adresse**/den **Host-Name** der Gegenstelle ein. |
| **Control-Port:** | Geben Sie die Nummer des in der Gegenstelle konfigurierten **Control Ports** ein. |
| **Select-Keys** | Erfassen Sie den gewünschten Select-Key. |

**HINWEIS:** Im **Host-Name**-Feld können Sie mit der Tastenkombination **Strg+F8** den Dialog **Gefundene Geräte** öffnen. In diesem Dialog werden Ihnen alle *nicht* gekoppelten G&D-Gegenstellen (Rechnermodule und Matrixswitches) angezeigt.

Wählen Sie die gewünschte Gegenstelle aus und betätigen Sie die **Eingabetaste**, um die IP-Adresse der Gegenstelle zu übernehmen.

7. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So löschen Sie eine Gegenstelle:**

1. Verwenden Sie den lokalen Hotkey **Alt+Num** zum Aufruf des Arbeitsplatzmodul-OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **IP-MUX** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie mit den Pfeiltasten die zu löschende Gegenstelle und betätigen Sie **F4**-Taste.
6. Bestätigen Sie die Sicherheitsabfrage, um die Gegenstelle zu löschen.

# Erweiterte Einstellungen der KVM-over-IP-Verbindung

## Bandbreite limitieren

In der *Standard*einstellung verwendet der KVM-Extender die maximal zur Verfügung stehende Bandbreite des Gigabit-Ethernets. Mittels manuellem Bandbreiten-Management können Sie die Übertragung an unterschiedliche Bandbreitenanforderungen anpassen.

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

1. Verwenden Sie den Remote-Hotkey **Strg**+**Num** zum Aufruf des Rechnermodul-OSD.
2. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
3. Geben Sie in der Zeile **Bandbreitenbeschränkgung (Mb/s)** das Bandbreiten-Limit in Mb/s für die KVM-over-IP-Verbindung ein.

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

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Klassifizierung der IP-Pakete (DiffServ)

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

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

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

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

1. Verwenden Sie den Remote-Hotkey **Strg+Num** zum Aufruf des Rechnermodul-OSD.
2. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
3. Erfassen Sie im Abschnitt **Netzwerk-Kontrolle** folgende Daten:

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

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

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

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Signale (de)aktivieren

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

Zusätzlich können Sie die Übertragung der RS232-Daten aktivieren und alternativ die Übertragung der Audio-Daten deaktivieren.

**So (de)aktivieren Sie die Übertragung des Audio- bzw. RS232-Signals:**

1. Verwenden Sie den Remote-Hotkey **Strg**+**Num** zum Aufruf des OSD.
2. Wählen Sie die Zeile **KVM-Verbindung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie in der Zeile **Aktivierte Signale** das Kontrollkästchen des zu (de)aktivierenden Signals mit den Pfeiltasten aus und betätigen Sie die **F8**-Taste.
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

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

In der *Standard*einstellung eines Rechnermoduls darf *jede* IP-Matrix und *jedes* Arbeitsplatzmodul eine KVM-over-IP-Verbindung zum Rechnermodul aufbauen.

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

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

1. Verwenden Sie den Remote-Hotkey **Strg+Num** zum Aufruf des OSD.
2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Systemsicherheit** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie in der Zeile **UID Locking** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **Keines** ‣ Alle Gegenstellen dürfen eine KVM-over-IP-Verbindung aufbauen (*Standard*).
   **UID** ‣ Nur die in der Liste angegebenen Gegenstellen dürfen eine KVM-over-IP-Verbindung herstellen.

5. Wählen Sie die Zeile **Alle angeschlossenen Geräte zulassen** und betätigen Sie die **Eingabetaste**, wenn Sie bei aktiviertem UID-Locking allen angeschlossenen Geräten eine KVM-over-IP-Verbindung ermöglichen wollen.
6. Wählen Sie die Zeile **Erlaubte Geräte verwalten** und betätigen Sie die **Eingabetaste**, wenn Sie Geräte entfernen oder hinzufügen möchten.

   **F4: Löschen** ‣ Markieren Sie das Gerät, das Sie aus der Liste entfernen wollen, betätigen Sie die **F4**-Taste und bestätigen Sie Ihre Auswahl.
   **F3: Neu** ‣ Betätigen Sie die **F3**-Taste.
   ‣ Wählen Sie in der Zeile **Gerätetyp** durch Betätigung der **F8**-Taste den gewünschten Gerätetyp aus.
   ‣ Geben Sie in der Zeile **Geräte-UID** die UID des Geräts ein.

7. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

# IP-MUX-Funktionalität

Die Module der **VisionXS-IP**-Serie bieten mit der **IP-MUX**-Funktion die Möglichkeit, *unterschiedliche* Rechnermodule (nacheinander) aufzuschalten.

**WICHTIG:** Ein Arbeitsplatzmodul kann immer nur mit einem Rechnermodul verbunden sein!

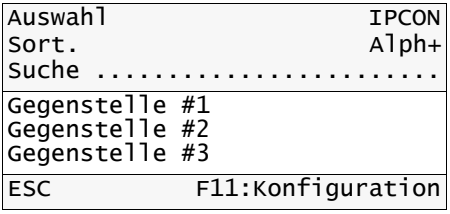
Zur Nutzung der Funktion können Sie maximal 20 Rechner an je ein separates Rechnermodul anschließen und diese Rechnermodule als Gegenstellen (s. Seite 49 ff.) im Arbeitsplatzmodul konfigurieren.

Die konfigurierten Gegenstellen können anschließend über das lokale OSD des Arbeitsplatzmoduls aufgeschaltet werden.

## Aufschaltung einer Gegenstelle über das OSD

**So schalten Sie eine bestimmte Gegenstelle auf:**

1. Starten Sie das lokale OSD mit dem Hotkey **Alt+Num** (*Standard*).




2. Wählen Sie im *Auswahl*-Menü die aufzuschaltende Gegenstelle mit den **Pfeiltasten** aus.
3. Betätigen Sie die **Eingabetaste**.

## Aufschaltung einer Gegenstelle mit Select-Keys

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

**So wählen Sie den Select-Key-Modifizierer und die zulässige Tastenart:**

1. Verwenden Sie den lokalen Hotkey **Alt**+**Num** zum Aufruf des OSD.
2. Betätigen Sie **F11** zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **Hotkey** und betätigen Sie die **Eingabetaste**.
4. Erfassen Sie im Abschnitt **Select-Key-Modifizierer** mindestens eine der aufgeführten Select-Key-Modifiziertasten durch Markierung des entsprechenden Kontrollkästchens mit den Pfeiltasten und anschließende Betätigung der **F8**-Taste aus:

| | |
|---|---|
| **Strg:** | *Strg*-Taste |
| **Alt:** | *Alt*-Taste |
| **Alt Gr:** | *Alt Gr*-Taste |
| **Win:** | *Windows*-Taste |
| **Shift:** | Umschalttaste |

5. Wählen Sie die Zeile **Gültige Target-Select-Keys** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **Num:** | *nur Zifferntasten* werden bei gemeinsamer Betätigung mit dem Select-Key-Modifizierer als Select-Keys interpretiert |
| **Alph:** | *nur Buchstabentasten* werden bei gemeinsamer Betätigung mit dem Select-Key-Modifizierer als Select-Keys interpretiert |
| **AlphNum:** | *Ziffern- und Buchstabentasten* werden bei gemeinsamer Betätigung mit dem Select-Key-Modifizierer als Select-Keys interpretiert |

**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. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**So schalten Sie sich mit Select-Keys auf eine Gegenstelle auf:**

1. Betätigen Sie die eingerichtete(n) Target-Select-Key-Modifiziertaste(n) und den, der Gegenstelle zugewiesenen, Select-Key (siehe *Anlegen, Konfig. und Löschen einer Gegenstelle* ab Seite 49).

**BEISPIEL:**

- Target-Select-Key-Modifiziertasten: **Alt Gr**+**Shift**
- Target-Select-Key für Gegenstelle: **S**

Halten Sie die Tasten **Alt Gr**+**Shift** gedrückt, während Sie den Select-Key **S** betätigen. Sobald die Tasten losgelassen werden, erfolgt die Umschaltung auf die Gegenstelle.

## Verbindung zu einer Gegenstelle beenden

**So beenden Sie die Verbindung zu einer Gegenstelle:**

1. Starten Sie das lokale OSD mit dem Hotkey **Alt**+**Num** (*Standard*).
2. Betätigen Sie die Tastenkombination **Strg**+**D**, um die aktive Verbindung zur Gegenstelle zu trennen.

# Erstkonfiguration der Netzwerkeinstellungen

Grundlegende Voraussetzung für den Zugriff auf die Webapplikation des KVM-Extenders ist die Konfiguration der Netzwerkeinstellungen des Rechner- und des Arbeitsplatzmoduls.

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

- IP-Adresse der *Netzwerkschnittstelle A* | *Interface A*: **192.168.0.1**
- globale Netzwerkeinstellungen: Dynamischer Bezug der Einstellungen

Die erforderlichen Konfigurationseinstellungen können direkt am Arbeitsplatz durchgeführt werden.

**WICHTIG:** Sie können am Arbeitsplatz mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**) das lokale OSD des Arbeitsplatzmoduls und mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**) das entfernte OSD des Rechnermoduls aufrufen und konfigurieren.

Während des Startvorgangs des Arbeitsplatzmoduls werden die Einstellungen beider Hotkeys angezeigt (siehe *Startvorgang* auf Seite 31).

## Konfiguration der Netzwerkschnittstelle

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

**So konfigurieren Sie die Netzwerkschnittstelle:**

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für Rechnermodul ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für Arbeitsplatzmodul ändern möchten.

2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.

3. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.

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

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

| | |
|---|---|
| **Betriebsmodus:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus der Schnittstelle:<br>▪ **Aus:** Netzwerkschnittstelle ausschalten.<br>▪ **Statisch IPv4:** Es wird eine statische IPv4-Adresse zugeteilt.<br>▪ **DHCPv4:** Bezug der IPv4-Adresse von einem DHCP-Server. |
| **IP-Adresse:** | Geben Sie die IPv4-Adresse der Schnittstelle an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung autom. bezogen.*<br>**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! |
| **Netzmaske:** | Geben Sie die Netzmaske des Netzwerkes an.<br>*Im Betriebsmodus DHCPv4 wird diese Einstellung automatisch bezogen.* |
| **IPv6:** | Betätigen Sie die **F8**-Taste um IPv6 zu aktivieren (**aktiviert**). Standardmäßig ist IPv6 deaktiviert (**aus**).<br>**HINWEIS:** Bei der Aktivierung von IPv6 wird gemäß RFC 4921 standardmäßig eine link-lokale IPv6-Adresse anhand der MAC-Adresse der Schnittstelle generiert. Diese link-lokale IPv6-Adresse ist vom Anwender nicht veränderbar. |
| **Statische IPv6-Adresse:** | Geben Sie die statische IPv6-Adresse der Schnittstelle an. |
| **Präfix:** | Geben Sie die Präfixlänge (*Standard*: 64) gemäß den Notationsregeln nach RFC 5952 für die Schnittstelle an. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Konfiguration der globalen Netzwerkeinstellungen

Die globalen Netzwerkeinstellungen stellen auch in komplexen Netzwerken sicher, dass der KVM-Extender aus allen Teilnetzwerken erreichbar ist.

**So konfigurieren Sie die globalen Netzwerkeinstellungen:**

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für Rechnermodul ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für Arbeitsplatzmodul ändern möchten.

2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.

3. Wählen Sie die Zeile **Schnittstellen** und betätigen Sie die **Eingabetaste**.

4. Erfassen Sie im Abschnitt **Main-Netzwerk** folgende Daten:

| | |
|---|---|
| **Globale Einstellungen:** | Betätigen Sie die **F8**-Taste zur Auswahl des Betriebsmodus:<br>▪ **Statisch:** Verwendung von statischen Einstellungen.<br>▪ **Dynamisch:** Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6). |
| **Host-Name:** | Geben Sie den Host-Namen des Matrixswitches ein. |
| **Domain:** | Geben Sie die Domäne an, welcher der Matrixswitch angehören soll. |
| **Gateway IPv4:** | Geben Sie die IPv4-Adresse des Gateways an. |
| **Gateway IPv6:** | Geben Sie die IPv6-Adresse des Gateways an. |
| **DNS 1:** | Geben Sie die IP-Adresse des DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **DNS 2:** | Geben Sie optional die IP-Adresse eines weiteren DNS-Servers an.<br>**HINWEIS:** Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das **%**-Zeichen hinter der link-lokalen IPv6-Adresse angefügt. |
| **IPv6 Vorrang einräumen:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja**, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (*Standard*: **nein**). |

| | |
|---|---|
| **SLAAC verwenden:** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*, wenn *SecureCert-Feature* nicht aktiviert), falls SLAAC verwendet werden soll. Ansonsten wählen Sie **nein** (*Standard* bei aktiviertem *SecureCert-Feature*). |
| **Mcast Echo Reply senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls ICMPv6 Echo Requests beantwortet werden sollen. Ansonsten wählen Sie **nein**. |
| **DestUnreach senden (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann. Ansonsten wählen Sie **nein**. |
| **Redirects verarbeiten (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen. Ansonsten wählen Sie **nein**. |
| **Dupl. addr. detection (IPv6):** | Betätigen Sie die **F8**-Taste und wählen Sie **ja** (*Standard*), falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird. Ansonsten wählen Sie **nein**. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Erreichbarkeit eines Hosts im Netzwerk prüfen (Ping)

Über das OSD können Sie die Erreichbarkeit eines bestimmten Hosts (z. B. eines Computers oder Netzwerkgeräts) im Netzwerk prüfen.

**So prüfen Sie die Erreichbarkeit eines Hosts im Netzwerk:**

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für Rechnermodul ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für Arbeitsplatzmodul ändern möchten.

2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Host pingen** und betätigen Sie die **Eingabetaste**.
4. Geben Sie im Feld **Host** die IP-Adresse oder den Namen des Hosts ein und betätigen Sie die **Eingabetaste**.
5. Das Ergebnis der Prüfung wird Ihnen in den folgenden Zeilen des Menüs angezeigt:

| | |
|---|---|
| **Übertragen:** | Anzahl der gesendeten Datenpakete |
| **Empfangen:** | Anzahl der empfangenen Datenpakete |
| **Verloren-gegangen:** | Anzahl der Datenpakete ohne Rückmeldung |
| **Min. RTT:** | kürzeste Paketumlaufzeit |
| **Durchschn. RTT:** | mittlere Paketumlaufzeit |
| **Max. RTT:** | längste Paketumlaufzeit |

**HINWEIS:** Falls der eingebene Name des Hosts nicht in eine IP-Adresse aufgelöst werden kann, erscheint eine entsprechende Meldung.

6. Betätigen Sie die **Esc**-Taste zum Verlassen des Menüs.

## Link-Aggregation

**WICHTIG:** Zur Erhöhung der Ausfallsicherheit können Sie die **Transmission 2**-Schnittstelle des KVM-Extenders mit dem kostenpflichtig erhältlichen **Transm. Redundancy**-Feature freischalten.

Beide Schnittstellen werden via *Link-Aggregation* zu einer Gruppe zusammengefasst. 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. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für Rechnermodul ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für Arbeitsplatzmodul ändern möchten.

2. Wählen Sie die Zeile **Netzwerk-Einrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste, wählen Sie die Zeile **Netzwerk** und betätigen Sie die **Eingabetaste** (lokales OSD).

3. Wählen Sie die Zeile **Link-Aggregation** und betätigen Sie die **Eingabetaste**.

4. Wählen Sie im Abschnitt **Parameter** zwischen folgenden Optionen:

| | |
|---|---|
| **Primärer Follower:** | Betätigen Sie die **F8**-Taste zur Auswahl der Optionen.<br>Wählen Sie, ob der Datenverkehr bevorzugt über die Schnittstelle **Transmission 1** bzw. **Transmission 2** erfolgen soll. Sobald die ausgewählte Schnittstelle verfügbar ist, wird diese Schnittstelle für den Datenverkehr verwendet.<br>Wählen Sie die Option **Keiner**, wird der Datenverkehr über eine beliebige Schnittstelle gesendet. Eine Umschaltung erfolgt nur, wenn die aktive Schnittstelle ausfällt. |
| **Link-Monitoring:** | Betätigen Sie die **F8**-Taste zur Auswahl der Optionen. 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.<br>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.<br>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.<br>Wählen Sie, ob bzw. welche der eingehenden ARP-Pakete validiert werden sollen. Betätigen Sie die **F8**-Taste zur Auswahl der Optionen.<br>▪ **Keines:** Die ARP-Pakete werden nicht validiert (*Standard*).<br>▪ **aktiv:** Ausschließlich die ARP-Pakete der aktiven Netzwerkschnittstelle werden validiert.<br>▪ **Backup:** Ausschließlich die ARP-Pakete der inaktiven Netzwerkschnittstelle werden validiert.<br>▪ **Alle:** Die ARP-Pakete aller Netzwerkschnittstellen der Gruppe werden validiert. |
| **ARP-Target:** | Die Tabelle enthält eine Liste aller konfigurierten ARP-Targets.<br>Verwenden Sie die Schaltflächen **F3: Neu**, **F4: Löschen** und **F5: Bearbeiten**, um die ARP-Targets zu verwalten. |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Status der Netzwerkschnittstellen auslesen

Den aktuellen Status der beiden Netzwerkschnittstellen des Gerätes können Sie im OSD auslesen.

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

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**), falls Sie die Einstellungen für Rechnermodul ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**), falls Sie die Einstellungen für Arbeitsplatzmodul ändern möchten.

2. Wählen Sie die Zeile **Netzwerk-Einrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste, wählen Sie die Zeile **Netzwerk** und betätigen Sie die **Eingabetaste** (lokales OSD).

3. Wählen Sie die Zeile **Link-Status** und betätigen Sie die **Eingabetaste**.

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

| | |
|---|---|
| **Link erkannt:** | Verbindung zum Netzwerk hergestellt (**ja**) oder unterbrochen (**nein**). |

5. Klicken Sie auf **ESC**, um die Seite zu verlassen.

# On-Screen-Display

Beim Start des Arbeitsplatzmoduls werden Informationen über den Startvorgang sowie die Firmware-Versionen und ID-Nummern der verbundenen Module auf dem Monitor des Arbeitsplatzes angezeigt.

Zusätzlich werden der **lokale Hotkey** (*Standard*: **Alt**+**Num**) zum Öffnen des lokalen OSD des Arbeitsplatzmoduls und der **Remote-Hotkey** (*Standard*: **Strg**+**Num**) zum Öffnen des entfernten OSD des Rechnermoduls angezeigt.

**TIPP:** Betätigen Sie die **Pause**-Taste, um den Vorgang anzuhalten. Ein Tastendruck auf die **Leertaste** führt den Vorgang fort.

## Grundlegende Bedienung des On-Screen-Displays

Im On-Screen-Display (OSD) – wie auch über die im folgenden Abschnitt erläuterte Webapplikation **Config Panel** – kann die Konfiguration des KVM-Extenders durch den Anwender geändert werden.

**HINWEIS:** Die tatsächlichen Konfigurationsmöglichkeiten durch den Anwender sind abhängig von den erteilten Berechtigungen (siehe *Änderung der Rechte eines Benutzerkontos* ab Seite 85).

Der Aufruf des OSD ist am Arbeitsplatzmodul über die konfigurierte Tastenkombination möglich. Die Einstellungen des KVM-Extenders können Sie nur im *entfernten OSD* des *Rechnermoduls* einsehen und editieren.

**WICHTIG:** *Standard*mäßig ist die OpenAccess-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart *nicht* durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

**WICHTIG:** Bei Geräten mit aktiviertem *SecureCert Feature* ist *standardmäßig* die Standard-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

**HINWEIS:** Sie können am Arbeitsplatz mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**) das entfernte OSD des Rechnermodus und mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**) das lokale OSD des Arbeitsplatzmoduls aufrufen und konfigurieren.

Während des Startvorgangs des Arbeitsplatzmoduls werden die Einstellungen beider Hotkeys angezeigt (siehe *Startvorgang* auf Seite 31).

## Anzeige des entfernten OSD

**So starten Sie das entfernte OSD:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

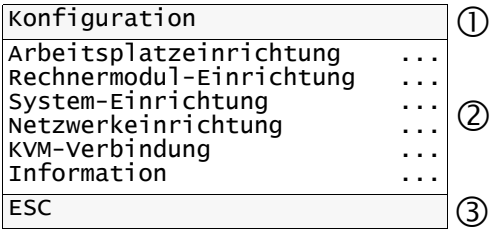
## Anzeige des lokalen OSD

**So starten Sie das lokale OSD:**

1. Starten Sie das OSD mit dem Hotkey **Alt+Num** (*Standard*).

## Aufbau des OSD

Nach der Ausführung des Remote-Hotkeys wird das OSD auf dem Monitor des Arbeitsplatzes angezeigt:




Die Menüansichten des OSD bestehen aus drei Hauptbereichen:

| | |
|---|---|
| **Kopfzeile** ① | Hier wird der Titel des aktuellen Menüs angezeigt. |
| **Listenfeld** ② | Im Listenfeld werden die Menüeinträge des ausgewählten Menüs aufgeführt.<br>Zu unterscheiden sind zwei Arten von Menüeinträgen:<br>▪ **Menüpunkte *mit* Untermenü:**<br>Diese Einträge werden mit drei Punkten (…) in der rechten Spalte dargestellt. Wählen Sie einen solchen Eintrag mit den **Pfeiltasten** aus und betätigen Sie die **Eingabetaste**, um das Untermenü zu öffnen.<br>▪ **Menüpunkte *ohne* Untermenü:**<br>Die aktuelle Einstellung wird hinter dem Menüeintrag angezeigt und kann direkt geändert werden. |
| **Fußzeile** ③ | In der Fußzeile werden die wichtigsten Tasten zur Bedienung des aktuell angezeigten Menüs und ggf. weitere Informationen aufgeführt. |

## Bedienung des OSD per Tastatur oder Maus

### Tastaturbedienung

Das OSD wird hauptsächlich mit der Tastatur des Arbeitsplatzes bedient. Nachfolgend finden Sie eine Auflistung der häufig verwendeten Tasten:

| | |
|---|---|
| **Pfeiltasten:** | Mit den Pfeiltasten **Hoch** und **Runter** (in einigen Menüs auch **Links** und **Rechts**) bewegen Sie die Positionsmarke zwischen verschiedenen Menüeinträgen. |
| **Eingabetaste:** | Diese Taste wird zur Bestätigung von Eingaben oder zum Aufruf eines Untermenüs verwendet. |
| **Esc:** | Diese Taste schließt die aktuell angezeigte Menüansicht und zeigt das übergeordnete Menü an.<br>Falls Eingaben geändert, aber nicht gespeichert wurden, erhalten Sie diesbezüglich eine Meldung. |
| **Tabulatortaste:** | Verwenden Sie diese Taste, um die Positionsmarke innerhalb des Listenfeldes von einem Menüeintrag zum nächsten (oder umgekehrt) zu bewegen. |
| **F2:** | Betätigen Sie diese Taste zur Speicherung Ihrer Eingaben.<br>Die aktuell angezeigte Menüansicht wird nach der Speicherung der Daten geschlossen und das übergeordnete Menü angezeigt. |
| **F8:** | Betätigen Sie diese Taste, um zwischen den verschiedenen Optionen eines Menüeintrags zu wechseln. |
| **Strg+F8:** | Konfigurationseinstellungen mit vielen verfügbaren Optionen unterstützen diese Tastenkombination zum Aufruf einer übersichtlichen Liste aller Optionen. |

## Mausbedienung

Alternativ zur Bedienung des OSD mit der Tastatur des Arbeitsplatzes kann die Maus des Arbeitsplatzes verwendet werden, um folgende Operationen durchzuführen:

| | |
|---|---|
| **Mausbewegung »Hoch«:** | Mit dieser Mausbewegung bewegen Sie die Positionsmarke im Listenfeld zwischen den verschiedenen Menüeinträgen *aufwärts*. |
| **Mausbewegung »Runter«:** | Mit dieser Mausbewegung bewegen Sie die Positionsmarke im Listenfeld zwischen den verschiedenen Menüeinträgen *abwärts*. |
| **linke Maustaste:** | Diese Maustaste wird zur Bestätigung von Eingaben (z. B. in der Login-Maske) oder zum Aufruf eines Untermenüs verwendet. |
| **rechte Maustaste:** | Diese Maustaste schließt die aktuell angezeigte Menüansicht und zeigt das übergeordnete Menü an.<br>Falls Eingaben geändert, aber nicht gespeichert wurden, erhalten Sie diesbezüglich eine Meldung. |

# Funktionen des OSD

## Suchfunktion

Einige Menüs bieten eine Suchfunktion, um den gewünschten Eintrag im Listenfeld schnell auswählen zu können.

**So suchen Sie nach einem bestimmten Eintrag, dessen Name Ihnen bekannt ist:**

1. Starten Sie das lokale OSD mit dem Hotkey **Alt**+**Num** (*Standard*).
2. Betätigen Sie ggf. die **Tabulator**-Taste zur Auswahl des Listenfeldes.
3. Geben Sie den Namen – oder die Anfangsbuchstaben des Namens, die eine eindeutige Zuordnung ermöglichen – des gesuchten Eintrags ein. Die eingegebenen Zeichen werden im Feld **Suche** der Kopfzeile ausgegeben.

> **HINWEIS:** Nach der Eingabe *jedes* Zeichens wird im Listenfeld der erste Eintrag markiert, der mit dem bzw. den eingegebenen Zeichen beginnt.
>
> Die Verwendung von Platzhaltern wird nicht unterstützt.

## Sortierung der Listeneinträge ändern

In der *Standard*einstellung werden die Listeneinträge der Mehrzahl der Menüs in alphabetisch aufsteigender Reihenfolge (Einstellung: **Alph+**) sortiert.

**So ändern Sie das Sortierkriterium und/oder die Reihenfolge der Darstellung:**

1. Starten Sie das lokale OSD mit dem Hotkey **Alt**+**Num** (*Standard*).
2. Betätigen Sie die **Tabulator**-Taste zur Auswahl des **Sort.**-Feldes in der Kopfzeile.
3. Betätigen Sie die **F8**-Taste, um das gewünschte Sortierkriterium auszuwählen:

| | |
|---|---|
| **Alph+:** | Die Namen der Listeneinträge werden in alphabetisch *aufsteigender* Reihenfolge sortiert. |
| **Alph-:** | Die Namen der Listeneinträge werden in alphabetisch *absteigender* Reihenfolge sortiert. |

# Übersicht der Menüs des entfernten OSD

Sie können am Arbeitsplatz mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**) das entfernte OSD des Rechnermodus aufrufen und konfigurieren.

Auf den folgenden Seiten werden die Funktionen der Hauptmenüs des entfernten OSD aufgelistet.

## Konfigurationsmenü

Das Konfigurationsmenü des Rechnermoduls öffnet sich direkt nach dem Start des entfernten OSD.

In diesem Menü können folgende Einstellungen zur Konfiguration vorgenommen werden:

| | Funktion | Erläuterung |
|---|---|---|
| **Arbeitsplatzeinrichtung** | **Arbeitsplatztyp** | Seite 98 |
| | **Änderung des Namens des Arbeitsplatzmoduls** | Seite 99 |
| | **Persönliches Profil** | Seite 74 |
| | **Bildschirmschoner (min)** | Seite 115 |
| | **USB-Auto-Refresh** | Seite 114 |
| | **OSD-Tastatur-Layout** | Seite 116 |
| | **Freeze-Modus und Freeze-Visualisierung** | Seite 109 |
| | **DDC/CI-Unterstützung** | Seite 110 |
| **Rechnermodul-Einrichtung** | **Änderung des Namens des Rechnermoduls** | Seite 99 |
| | **USB-HID-Modus** | Seite 111 |
| | **EDID-Modus und EDID zuweisen** | Seite 107 |
| | **Farbtiefe** | Seite 108 |
| **System-Einrichtung** | **Passwort-Komplexität** | Seite 34 |
| | **Anmeldeoptionen** | Seite 36 |
| | **Nutzungsbedingungen-Konfig.** | Seite 38 |
| | **Hotkeys** | Seite 102 |
| | **Systemsicherheit** | Seite 54 |
| | **Werkseinstellungen wiederherstellen** | Seite 117 |

| | | |
|---|---|---|
| **Benutzereinrichtung** | **Neu** | Seite 82 |
| | **Löschen** | Seite 87 |
| | **Name** | Seite 83 |
| | **Aktivieren** | Seite 87 |
| | **Passwort** | Seite 84 |
| | **Persönliches Profil** | Seite 74 |
| | **Gruppenmitgliedschaft** | Seite 86 |
| | **Superuser-Recht** | Seite 92 |
| | **Konfig.-Rechte** | Seite 93 |
| | **Globale Geräterechte** | Seite 93 |
| | **Geräte-Rechte: Zugriff** | Seite 94 |
| | **Geräte-Rechte: USB-Zugriff** | Seite 95 |
| **Benutzergruppeneinrichtung** | **Neu** | Seite 88 |
| | **Löschen** | Seite 91 |
| | **Name** | Seite 89 |
| | **Aktivieren** | Seite 91 |
| | **Mitgliederverwaltung** | Seite 90 |
| | **Superuser-Recht** | Seite 92 |
| | **Konfig.-Rechte** | Seite 93 |
| | **Globale Geräterechte** | Seite 93 |
| | **Geräte-Rechte: Zugriff** | Seite 94 |
| | **Geräte-Rechte: USB-Zugriff** | Seite 95 |
| **Netzwerkeinrichtung** | **Schnittstellen Netzwerk** | Seite 59 |
| | **Schnittstellen KVM-over-IP** | Seite 42 |
| | **Link-Aggregation** | Seite 64 |
| | **Link-Status** | Seite 66 |
| | **Host pingen** | Seite 63 |
| | **Netzfilterkonfiguration zurücksetzen** | Seite 118 |
| **KVM-Verbindung** | **Control-Port, Communication-Port und Data-Port** | Seite 44 |
| | **Bandbreitenbeschränkung (Mb/s)** | Seite 51 |
| | **DiffServ Communication und DiffServ Data** | Seite 52 |
| | **Aktivierte Signale (Audio und RS232)** | Seite 53 |
| **Information** | **Hardware-, Firmware-, Hotkey- und Feature-Information** | Seite 75 |

## Persönliches Profile-Menü

Das *Persönliche Profil*-Menü kann nach dem Start des OSD mit der **F10**-Taste geöffnet werden. Die Einstellungen dieses Menüs gelten ausschließlich für den Benutzer, dessen Name rechts oben angezeigt wird.

In diesem Menü werden die Einstellungen aufgelistet, die für jeden Benutzer individuell festgelegt werden können:

| Funktion | Erläuterung |
|---|---|
| **Passwort ändern** | Seite 100 |
| **Sprache** | Seite 101 |
| **Einblendung (allgemein)** | Seite 120 |
| **OSD-Transparenz** | Seite 120 |
| **OSD-Farbe** | Seite 119 |
| **Timeout der OSD-Sitzung (s)** | Seite 121 |
| **Display-Position festlegen** | Seite 121 |
| **Menü-Position festlegen** | Seite 122 |

## Bedienung-Menü

Das Bedienung-Menü kann nach dem Start des OSD mit der **F9**-Taste geöffnet werden. Folgende Funktionen können vom Benutzer ausgeführt werden:

| Funktion | Erläuterung |
|---|---|
| **E – Benutzer abmelden** | Seite 39 |
| **T – Temporärer Login** | Seite 33 |

### Information-Menü

Das Information-Menü kann nach dem Start des OSD mit der F12-Taste geöffnet werden. In diesem Menü erhalten Sie folgende Informationen:

| Funktion | Erläuterung |
|---|---|
| **Hardware-Information** | Hier werden beispielsweise die Firmware-Version, die Seriennummer des Geräts und die MAC-Adressen der Netzwerkschnittstellen aufgelistet. |
| **Firmware-Information** | Hier werden die Firmware-Versionen des Arbeitsplatzmoduls und des aufgeschalteten Rechnermoduls angezeigt. |
| **Hotkey-Information** | Hier werden die aktiven Hotkeys angezeigt. |
| **Feature-Information** | Hier werden die aktivierten Features angezeigt. |

## Übersicht der Menüs des lokalen OSD

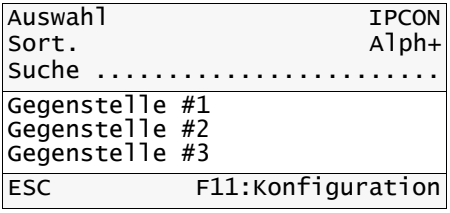
Sie können am Arbeitsplatz mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**) das lokale OSD des Arbeitsplatzmoduls aufrufen und konfigurieren.

Auf den folgenden Seiten werden die Funktionen der Hauptmenüs des lokalen OSD aufgelistet.

### Auswahl-Menü

Das Auswahl-Menü wird üblicherweise unmittelbar nach dem Aufruf des OSD angezeigt.

Hier werden die im Extendersystem bekannten Rechnermodule angezeigt (siehe *IP-MUX-Funktionalität* auf Seite 55).




Über die Such- und Sortierfunktion können Sie die Auswahl einschränken.

### Konfigurationsmenü

Das Konfigurationsmenü kann nach dem Start des OSD mit der **F11**-Taste geöffnet werden. Folgende Funktionen können vom Benutzer ausgeführt werden:

| | Funktion | Erläuterung |
|---|---|---|
| **Hotkey** | **Hotkey bearbeien** | Seite 102 |
| **Tastatur/Maus** | **USB-Auto-Refresh (Konfiguration über das entfernte OSD)** | Seite 114 |
| | **OSD-Tastatur-Layout** | Seite 116 |
| | **Generic USB** | Seite 113 |
| **Arbeitsplatz-Utility** | **Werkseinstellungen aktivieren** | Seite 117 |
| **Netzwerk** | **Schnittstellen** | Seite 59 |
| | **Link-Aggregation** | Seite 64 |
| | **Link-Status** | Seite 66 |
| | **Host pingen** | Seite 63 |
| | **Netzfilterkonfiguration zurücksetzen** | Seite 118 |
| **KVM-Verbindung** | **Passwortschutz** | Seite 48 |
| | **Control-Port, Communication-Port und Data-Port** | Seite 48 |
| | **IP-MUX** | Seite 49 |
| **Information** | **Hardware-, Firmware-, Hotkey- und Feature-Information** | Seite 75 |

# Freischaltung einer erworbenen Zusatzfunktion

**HINWEIS:** Die Freischaltung der Zusatzfunktionen erfolgt über die Webapplikation **Config Panel**.

Die erforderlichen Schritte sind im Handbuch der Webapplikation beschrieben.

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

# Webapplikation Config Panel

Die Webapplikation **Config Panel** bietet eine grafische Benutzeroberfläche zur Konfiguration und Überwachung des KVM-Extenders.

## Grundlegende Bedienung der Webapplikation

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

**HINWEIS:** Grundlegende Informationen zu den Systemvoraussetzungen, der erforderlichen Konfiguration der Netzwerkschnittstellen der **VisionXS-IP-F-TypeC-UHR**-Geräte und zum Einsatz der Webapplikation finden Sie im separaten Handbuch.

### Start der Webapplikation

**So starten Sie die Webapplikation Config Panel:**

1. Geben in der Adresszeile folgende URL ein:

   **https://[IP-Adresse des Rechner- oder Arbeitsplatzmoduls]**

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

| | |
|---|---|
| **(Nutzungs-) Bedingungen:** | Betätigen Sie die **Eingabtaste**, um die Nutzungsbedingungen angezeigt zu bekommen. |
| **Akzeptieren (der Nutzungs-bedingungen):** | Betätigen Sie die **F8**-Taste, um die Nutzungsbedingungen zu akzeptieren. |
| **Benutzername:** | Geben Sie Ihren Benutzernamen ein. |
| **Passwort:** | Geben Sie das Passwort Ihres Benutzerkontos ein. |
| **2-Factor Auth Code (TOTP):** | Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein. |

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

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

**HINWEIS:** Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde
(siehe *Anzeigen von Nutzungsbedingungen* auf Seite 38).

**HINWEIS:** Das Feld *2-Factor Auth Code (TOTP)* erscheint nur bei aktivierter 2-Faktor-Authentifizierung. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.

3. Klicken Sie auf **Login**.

## Sprache der Webapplikation auswählen

**So ändern Sie die Sprache der Webapplikation:**




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

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

## 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.

# Benutzer und Gruppen

## Effizienter Einsatz der Rechteverwaltung

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 Beutzer 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.

Das Individualrecht wird im OSD in gelber Farbe dargestellt. Das Effektivrecht wird in grüner Farbe dargestellt.

Mit der Tastenkombination **Strg+F12** rufen Sie das Fenster **Effektivrecht-Ursprung** auf.

Hier sehen Sie, aus welchen Gruppen das Effektivrecht resultiert.

**BEISPIEL:** Der Benutzer *Muster* ist Mitglied der Gruppen *Office* und *Rechnermodul-Konfig*.

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

| Recht | Benutzer *Muster* | Gruppe *Office* | Gruppe *Rechnermodul-Konfig* | Effektivrecht |
|---|---|---|---|---|
| **Rechnermodul-Konfig** | nein | ja | **ja** | **ja** |
| **Eigenes Passwort ändern** | nein | **ja** | nein | **ja** |
| **Geräte-Rechte: Zugriff** | **voll** | Ansicht | nein | **voll** |

Das Effektivrecht der Rechte *Rechnermodul-Konfig* und *Eigenes Passwort ändern* resultieren aus den Rechten der Benutzergruppen. Das Recht *Geräte-Rechte: Zugriff* wurde hingegen direkt im Benutzerkonto vergeben.

## 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 *Rechnermodul-Konfig* erhalten, bieten sich folgende Möglichkeiten an, dies mit Benutzergruppen zu realisieren:

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

In beiden Fällen erhält der Benutzer durch die Gruppen das Effektivrecht **ja** für das Recht *Rechnermodul-Konfig*.

**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

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 (siehe *Konfiguration der Passwort-Komplexität* auf Seite 34) vor der Anlage eines neuen Benutzerkontos vornehmen.

**So erstellen Sie ein neues Benutzerkonto:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Betätigen Sie die **F3**-Taste und erfassen Sie folgende Daten:

| | |
|---|---|
| **Name:** | Geben Sie den gewünschten Benutzernamen ein. |
| **Passwort:** | Geben Sie das Passwort des Benutzerkontos ein. |
| **Wiederholung:** | Wiederholen Sie das oben eingegebene Passwort. |

4. Betätigen Sie die **F2**-Taste zur Speicherung Ihrer Eingaben und Erstellung des Benutzerkontos.

**WICHTIG:** Das neu erstellte Benutzerkonto ist weder mit Konfigurations- noch mit Zugriffsrechten auf Rechnermodule ausgestattet.

Fügen Sie das Benutzerkonto vor dessen Verwendung einer bestehenden Benutzergruppe hinzu oder erteilen Sie dem Benutzerkonto individuelle Rechte (s. Seite 81).

## Änderung des Namens eines Benutzerkontos

**So ändern Sie den Namen eines Benutzerkontos:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto, dessen Namen Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Name** und betätigen Sie die **Eingabetaste**.
5. Geben Sie den gewünschten Namen ein und betätigen Sie die **Eingabetaste**.
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung des Passworts eines Benutzerkontos

**TIPP:** Die Änderung des eigenen Passworts kann alternativ über das *Pers. Profile-Menü* (s. Seite 74) erfolgen, falls das Benutzerkonto über das *Pers. Profile-* und das *Eigenes Passwort ändern*-Recht verfügt.

**HINWEIS:** Bei der Änderung des Passworts werden ggf. die festgelegten Passwort-Richtlinien (siehe *Konfiguration der Passwort-Komplexität* auf Seite 34) berücksichtigt.

**So ändern Sie das Passwort eines Benutzerkontos:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto, dessen Passwort Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Passwort** und betätigen Sie die **Eingabetaste**.
5. Geben Sie im Menü folgende Daten ein:

| | |
|---|---|
| **Aktuell:** | Geben Sie das bisherige Passwort ein.<br>**HINWEIS:** Bei Benutzern mit aktiviertem Superuser-Recht (s. Seite 92 ff.) ist in diesem Feld keine Eingabe notwendig. |
| **2-Factor Auth Code (TOTP):** | Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.<br>**HINWEIS:** Das Feld *2-Factor Auth Code (TOTP)* erscheint nur bei aktivierter 2-Faktor-Authentifizierung. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation. |
| **Neu:** | Geben Sie das neue Passwort ein. |
| **Wiederholung:** | Wiederholen Sie das neue Passwort. |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung der Rechte eines Benutzerkontos

Den verschiedenen Benutzerkonten können differenzierte Berechtigungen erteilt werden.

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

| Bezeichnung | Berechtigung | Seite |
|---|---|---|
| **Eigenes Passwort ändern** | Änderung des eigenen Passworts | Seite 94 |
| **Persönliches Profil** | Änderung der Einstellungen des persönlichen Profils eines Benuters | Seite 93 |
| **Superuser-Recht** | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 92 |
| **Geräte-Rechte: Zugriff** | Zugriff auf ein Rechnermodul | Seite 94 |
| **Rechnermodul-Konfig** | Konfiguration der Rechnermodule | Seite 94 |
| **Geräte-Rechte: USB-Zugriff** | USB-Zugriffsberechtigung für alle Module | Seite 95 |
| **WebIf-Login** | Login mit der Webapplikation **Config Panel** | Seite 93 |

## 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. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto, dessen Gruppenzugehörigkeit Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Gruppenmitgliedschaft** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie im Listenfeld die Benutzergruppe, welcher Sie das Benutzerkonto hinzufügen oder aus welcher Sie das Benutzerkonto entfernen möchten.

   **TIPP:** Verwenden Sie ggf. das *Suchfunktion* oder das *Sortierkriterium* (s. Seite 71) des Menüs, um die Auswahl der Listeneinträge einzugrenzen.

6. Betätigen Sie die **F8**-Taste, um das Benutzerkonto der ausgewählten Benutzergruppe hinzuzufügen oder aus dieser zu entfernen.

   **HINWEIS:** Benutzergruppen, welchen das Benutzerkonto zugeordnet ist, werden mit einer Pfeilmarkierung (▸) angezeigt.

7. Wiederholen Sie ggf. die Schritte 5. und 6., falls Sie die Gruppenzugehörigkeit weiterer Konten bearbeiten möchten.
8. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## 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. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto, das Sie (de)aktivieren möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Aktivieren** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Benutzerkonto aktiviert |
| **nein** | Benutzerkonto deaktiviert |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Löschen eines Benutzerkontos

**So löschen Sie ein Benutzerkonto:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzereinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das zu löschende Benutzerkonto und betätigen Sie die **F4**-Taste.
4. Wählen Sie den Eintrag **Ja** der Sicherheitsabfrage und betätigen Sie die **Eingabetaste**.

# Verwaltung von Benutzergruppen

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

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

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

## Anlegen einer neuen Benutzergruppe

Innerhalb des Systems können Sie bis zu 1.024 Benutzergruppen erstellen.

**So erstellen Sie eine neue Benutzergruppe:**

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Betätigen Sie die **F3**-Taste und erfassen Sie folgende Daten:

| | |
|---|---|
| **Name:** | Geben Sie den gewünschten Benutzergruppennamen ein. |

4. Betätigen Sie die **F2**-Taste zur Speicherung Ihrer Eingaben und Erstellung der Benutzergruppe.

**WICHTIG:** Die neu erstellte Benutzergruppe ist weder mit Konfigurations- noch mit Zugriffsrechten auf Rechnermodule ausgestattet
(siehe *Effizienter Einsatz der Benutzergruppen* auf Seite 81).

## Änderung des Namens einer Benutzergruppe

**So ändern Sie den Namen einer Benutzergruppe:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Benutzergruppe, deren Namen Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Name** und betätigen Sie die **Eingabetaste**.
5. Geben Sie den gewünschten Namen ein und betätigen Sie die **Eingabetaste**.
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung der Rechte einer Benutzergruppe

Den verschiedenen Benutzergruppen können differenzierte Berechtigungen erteilt werden.

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

| Bezeichnung | Berechtigung | Seite |
|---|---|---|
| **Eigenes Passwort ändern** | Änderung des eigenen Passworts | Seite 94 |
| **Persönliches Profil** | Änderung der Einstellungen des persönlichen Profils eines Benuters | Seite 93 |
| **Superuser-Recht** | Zugriff auf die Konfiguration des Systems uneingeschränkt möglich | Seite 92 |
| **Geräte-Rechte: Zugriff** | Zugriff auf ein Rechnermodul | Seite 94 |
| **Rechnermodul-Konfig** | Konfiguration der Rechnermodule | Seite 94 |
| **Geräte-Rechte: USB-Zugriff** | USB-Zugriffsberechtigung für alle Module | Seite 95 |
| **WebIf-Login** | Login mit der Webapplikation **Config Panel** | Seite 93 |

## Mitgliederverwaltung einer Benutzergruppe

**So verwalten Sie die Mitglieder einer Benutzergruppe:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Benutzergruppe, deren Mitglieder Sie verwalten möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Mitgliederverwaltung** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie im Listenfeld ein Benutzerkonto, das Sie der Benutzergruppe hinzufügen oder aus dieser entfernen möchten.

   **TIPP:** Verwenden Sie ggf. das *Suchfunktion* oder das *Sortierkriterium* (s. Seite 71) des Menüs, um die Auswahl der Listeneinträge einzugrenzen.

6. Betätigen Sie die **F8**-Taste, um das Benutzerkonto in die ausgewählte Benutzergruppe aufzunehmen oder aus dieser zu entfernen.

   **HINWEIS:** Benutzerkonten, die der Benutzergruppe zugeordnet sind, werden mit einer Pfeilmarkierung (▸) angezeigt.

7. Wiederholen Sie ggf. die Schritte 5. und 6., falls Sie die Gruppenzugehörigkeit weiterer Konten bearbeiten möchten.
8. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Aktivierung oder Deaktivierung einer Benutzergruppe

**So aktivieren oder deaktivieren Sie eine Benutzergruppe:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Benutzergruppe, die Sie (de)aktivieren möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Aktivieren** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Benutzergruppe aktiviert |
| **nein** | Benutzergruppe deaktiviert |

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

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Löschen einer Benutzergruppe

**So löschen Sie eine Benutzergruppe:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die zu löschende Benutzergruppe und betätigen Sie die **F4**-Taste.
4. Wählen Sie den Eintrag **Ja** der Sicherheitsabfrage und betätigen Sie die **Eingabetaste**.

# 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. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren *Superuser*-Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Superuser-Recht** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Uneingeschränkten Zugriff auf das KVM-System |
| **nein:** | Zugriffsberechtigung gemäß den Benutzer- und Gruppenrechten |

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Berechtigung zum Ändern der Einstellungen des »Persönliches Profil«-Menüs

**So ändern Sie die Berechtigung zum Ändern der Einstellungen des *Pers. Profil*-Menüs:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Globale Geräterechte** und betätigen Sie die **F8**-Taste.
5. Wählen Sie die Zeile **Persönliches Profil** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Einsehen und Editieren des eigenen Benutzerprofils erlaubt |
| **nein:** | Einsehen und Editieren des eigenen Benutzerprofils untersagt |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Berechtigung zum Login in die Webapplikation

**So ändern Sie die Berechtigung zum Login mit der Webapplikation:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Konfig.-Rechte** und betätigen Sie die **F8**-Taste.
5. Wählen Sie die Zeile **WebIf-Login** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Zugriff auf die Webapplikation erlaubt |
| **nein:** | Zugriff auf die Webapplikation untersagt |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Berechtigung zur Änderung des eigenen Passworts

**So ändern Sie die Berechtigung zur Änderung des eigenen Passworts:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Globale Geräterechte** und betätigen Sie die **F8**-Taste.
5. Wählen Sie die Zeile **Eigenes Passwort ändern** und betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Passwortänderung des eigenen Benutzerkontos erlaubt |
| **nein:** | Passwortänderung des eigenen Benutzerkontos untersagt |

6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Zugriffsrecht auf ein Rechnermodul

**So ändern Sie die Rechnermodul-Zugriffsrechte:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Geräte-Rechte: Zugriff** und betätigen Sie die **F8**-Taste.
5. Wählen Sie das Rechnermodul, für das Sie die Zugriffsrechte ändern möchten.
6. Betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **voll:** | Vollzugriff auf den am Rechnermodul angeschlossenen Computer erlaubt |
| **nein:** | Zugriff auf den am Rechnermodul angeschlossenen Computer untersagt |
| **Ansicht:** | Ansicht des Monitorbildes des am Rechnermodul angeschlossenen Computers erlaubt |

7. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Zugriffsrecht auf USB-Geräte

**So ändern Sie die Zugriffsrechte auf USB-Geräte:**

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Möchten Sie dieses Recht eines Benutzerkontos ändern, wählen Sie die Zeile **Benutzereinrichtung**. Möchten Sie dieses Recht einer Benutzergruppe ändern, wählen Sie die Zeile **Benutzergruppeneinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie das Benutzerkonto bzw. die Benutzergruppe, deren Recht Sie ändern möchten und betätigen Sie die **F5**-Taste.
4. Wählen Sie die Zeile **Geräte-Rechte: USB-Zugriff** und betätigen Sie die **F8**-Taste.
5. Wählen Sie das Rechnermodul, für das Sie die Zugriffsrechte ändern möchten.
6. Betätigen Sie die **F8**-Taste zur Auswahl einer der aufgelisteten Optionen:

| | |
|---|---|
| **ja:** | Zugriff auf die USB-Geräte erlaubt |
| **nein:** | Zugriff auf die USB-Geräte untersagt |

7. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

# Konfiguration

Die Konfiguration des KVM-Extenders kann wahlweise im On-Screen-Display (OSD) oder über die Webapplikation **Config Panel** durch den Anwender geändert werden:

- Das *OSD* wird auf dem Monitor des Arbeitsplatzes angezeigt. Die meisten Konfigurationseinstellungen können Sie im OSD direkt am Arbeitsplatz einstellen.
- Mit der Webapplikation **Config Panel** steht eine grafische Benutzeroberfläche zur Konfiguration und Überwachung des KVM-Extenders über einen Webbrowser zur Verfügung.

## Übersicht der Funktionen und Standardeinstellungen

In der folgenden Tabelle finden Sie eine Übersicht der konfigurierbaren Funktionen des KVM-Extenders. Zusätzlich werden die *Standardeinstellungen* und Verweise auf die ausführlichen Erläuterungen der Funktionen aufgeführt.

| Funktion | Standardeinstellung | Seite |
|---|---|---|
| Betriebsarten von Arbeitsplatzmodulen | OpenAccess (Standard bei Geräten mit aktiviertem *SecureCert Feature*) | 98 |
| Änderung des eigenen Passworts | | 100 |
| Sprache auswählen | deutsch | 101 |
| Änderung des Hotkeys | **Strg** | 102 |
| Änderung der OSD-Taste | **Num** | 103 |
| OSD mit doppeltem Tastendruck starten | ausgeschaltet | 104 |
| Kanalumschaltung bei Verwendung eines DH-Rechnermoduls | Pfeil links, rechts | 105 |
| Betriebsmodus der RS232-Schnittstelle einstellen | RS232 | 106 |
| Auswahl des EDID-Modus des KVM-Extenders | automatisch | 107 |
| Reduzierung der Farbtiefe der zu übertragenden Bilddaten | 24 bit | 108 |
| Verwendung des Freeze-Modus | deaktiviert | 109 |
| DDC/CI-Unterstützung (de)aktivieren | deaktiviert | 110 |
| USB-Tastaturmodus oder »Generic USB« de(aktivieren) | PC Multimedia | 111 |
| USB-Gerät für einen Neustart priorisieren | kein Gerät | 113 |
| Reinitialisierung von USB-Eingabegeräten | nur fehlerhafte Geräte | 114 |
| Wartezeit des Bildschirmschoners einstellen | deaktiviert | 115 |
| Automatische Abmeldung der Benutzer einstellen | deaktiviert | 115 |
| Tastaturlayout für Eingaben innerhalb des OSD auswählen | Deutsch | 116 |

| Funktion | Standardeinstellung | Seite |
|---|---|---|
| Wiederherstellung der Standardeinstellungen | | 117 |
| Reset der Netzfilterregeln | | 118 |
| Farbe der Informationseinblendung ändern | hellgrün | 119 |
| Anzeige der Informationseinblendung | temporär | 120 |
| Transparenz des OSD einstellen | mittleres Durchscheinen | 120 |
| Automatisches Schließen des OSD nach Inaktivität | deaktiviert | 121 |
| Position der Informationseinblendung ändern | links oben | 121 |
| Position des OSD ändern | zentriert | 122 |

Die grundlegende Bedienung des OSD wird ab Seite 67 beschrieben.

**HINWEIS:** Weitere Informationen zum Einsatz der Webapplikation finden Sie im separaten Handbuch.

# Konfigurationseinstellungen

## Betriebsarten von Arbeitsplatzmodulen

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

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

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

**WICHTIG:** Bei Geräten mit aktiviertem *SecureCert Feature* ist *standardmäßig* die Standard-Betriebsart eingestellt.

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

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

- **Standard-Betriebsart:** Die Standard-Betriebsart erlaubt den Zugang zum KVM-Extender erst nach der Authentifizierung des Benutzers mit seinem Benutzernamen, seinem Passwort und ggf. der 2-Faktor-Authentifizierung.

**HINWEIS:** Diese Betriebsart ist bei der Verwendung des Extenders als **Matrixswitch-Modul** (siehe *Verwendung als Extender- oder Matrixswitch-Module* auf Seite 5) *standardmäßig* eingestellt.

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

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

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie in der Zeile **Betriebsmodus** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **OpenAccess** ‣ OpenAccess-Betriebsart (*Standard*)
   **Standard** ‣ Standard-Betriebsart (*Standard* bei Geräten mit aktiviertem *SecureCert Feature*)

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung des Namens des Arbeitsplatzmoduls

**So ändern Sie den Namen des Arbeitsplatzmoduls:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Name** und betätigen Sie die **Eingabetaste**.
4. Geben Sie den gewünschten Namen ein und betätigen Sie die **Eingabetaste**.
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung des Namens des Rechnermoduls

**So ändern Sie den Namen des Rechnermoduls:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Rechnermodul-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Name** und betätigen Sie die **Eingabetaste**.
4. Geben Sie den gewünschten Namen ein und betätigen Sie die **Eingabetaste**.
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung des eigenen Passworts

**WICHTIG:** *Standardmäßig* ist die OpenAccess-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart *nicht* durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

**WICHTIG:** Bei Geräten mit aktiviertem *SecureCert Feature* ist *standardmäßig* die Standard-Betriebsart eingestellt. Der Zugang zum KVM-Extender ist in dieser Betriebsart durch eine Authentifizierung geschützt. Informationen zu den Betriebsarten finden Sie unter *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98.

**So ändern Sie das Passwort des eigenen Benutzerkontos:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie die Zeile **Passwort ändern** und betätigen Sie die **Eingabetaste**.
4. Geben Sie im Menü *Eigenes Passwort ändern* folgende Daten ein:

   **Aktuell** ‣ Geben Sie das bisherige Passwort ein.
   **2-Factor Auth Code (TOTP)** ‣ Geben Sie den 2-Fakor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
   **Neu** ‣ Geben Sie das neue Passwort ein.
   **Wiederholung** ‣ Wiederholen Sie das neue Passwort.

   Bei Benutzern mit aktiviertem Superuser-Recht ist im Feld *Aktuell* **keine** Eingabe notwendig.

   Das Feld *2-Factor Auth Code (TOTP)* erscheint nur bei aktivierter 2-Faktor-Authentifizierung. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Sprache 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 Web-Applikation als auch für das OSD des Gerätes.

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

**So ändern Sie die Sprache:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie in der Zeile **Sprache** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **vom System** ‣ Verwendung der Systemsprache
   **[Auswahl]** ‣ Verwendung der ausgewählten Sprache
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung des Hotkeys

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

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

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

**So ändern Sie den aktuellen Hotkey:**

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**), falls Sie die Einstellungen für das entfernte OSD ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**), falls Sie die Einstellungen für das lokale OSD ändern möchten.

2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste (lokales OSD).

3. Wählen Sie die Zeile **Hotkeys** und betätigen Sie die **Eingabetaste**.

4. Wählen Sie im Abschnitt **Modifizierer** *mindestens* eine der aufgeführten Hotkey-Modifizierertasten durch Markierung des entsprechenden Kontrollkästchens mit den Pfeiltasten und anschließende Betätigung der **F8**-Taste aus:

   **Strg** ‣ *Strg*-Taste (*Standard* für das entfernte OSD)
   **Alt** ‣ *Alt*-Taste (*Standard* für das lokale OSD)
   **Alt Gr** ‣ *Alt Gr*-Taste
   **Win** ‣ *Windows*-Taste
   **Shift** ‣ Umschalttaste

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Änderung der OSD-Taste

Der Hotkey zum OSD-Aufruf besteht aus mindestens einer Hotkey-Modifiziertaste (siehe *Änderung des Hotkeys* auf Seite 102) und einer zusätzlichen OSD-Taste, die vom Anwender innerhalb eines vorgegebenen Rahmens frei gewählt werden kann.

Sowohl die Hotkey-Modifiziertaste als auch die OSD-Taste können von Ihnen verändert werden.

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

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**), falls Sie die Einstellungen für das entfernte OSD ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**), falls Sie die Einstellungen für das lokale OSD ändern möchten.

2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste (lokales OSD).

3. Wählen Sie die Zeile **Hotkeys** und betätigen Sie die **Eingabetaste**.

4. Wählen Sie in der Zeile **(OSD-Aktions)Taste** durch Betätigung der **F8**-Taste eine OSD-Taste aus, welche gemeinsam mit der bzw. den Hotkey-Modifiziertaste(n) den Aufruf des OSD bewirkt:

   **Num** ‣ *Num*-Taste (*Standard*)
   **Pause** ‣ *Pause*-Taste
   **Einfg** ‣ *Einfg*-Taste
   **Löschen** ‣ *Entf*-Taste
   **Pos1** ‣ *Pos 1*-Taste
   **Ende** ‣ *Ende*-Taste
   **Bild hoch** ‣ *Bild*↑-Taste
   **Bild runter** ‣ *Bild*↓-Taste
   **Leertaste** ‣ Leertaste

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## OSD mit doppeltem Tastendruck starten

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

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

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für das entfernte OSD ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für das lokale OSD ändern möchten.

2. Wählen Sie die Zeile **System-Einrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste (lokales OSD).

3. Wählen Sie die Zeile **Hotkeys** und betätigen Sie die **Eingabetaste**.

4. Wählen Sie in der Zeile **OSD via 2x Tastendruck** die gewünschte Option aus:

   **aus** ‣ OSD-Aufruf mit doppeltem Tastendruck deaktiviert (*Standard*)
   **Strg** ‣ OSD-Aufruf mit doppeltem Druck auf die *Strg*-Taste
   **Alt** ‣ OSD-Aufruf mit doppeltem Druck auf die *Alt*-Taste
   **Alt Gr** ‣ OSD-Aufruf mit doppeltem Druck auf die *Alt Gr*-Taste
   **Win** ‣ OSD-Aufruf mit doppeltem Druck auf die *Windows*-Taste
   **Shift** ‣ OSD-Aufruf mit doppeltem Druck auf die *Umschalt*-Taste
   **Drucken** ‣ OSD-Aufruf mit doppeltem Druck auf die *Druck*-Taste

5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Kanalumschaltung bei Verwendung eines DH-Rechnermoduls

Sie können ein Arbeitsplatzmodul der **VisionXS-IP**-Serie in Kombination mit einer DH-Variante eines Rechnermoduls der **VisionXS-IP**-Serie verwenden.

**HINWEIS:** Die DH-Varianten ermöglichen die Übertragung von zwei separaten Videosignalen über ein Übertragungskabel.

Um am Arbeitsplatz das Bild des zweiten Videoausgangs des Computers angezeigt zu bekommen, haben Sie die Möglichkeit zwischen den Videokanälen umzuschalten.

Die Tastenkombination für die Kanalumschaltung besteht aus mindestens einer Modifizierertaste (siehe *Betriebsarten von Arbeitsplatzmodulen* auf Seite 98) und zusätzlichen *Stream-Auswahl*-Tasten. Sowohl die Modifizierertaste als auch die *Stream-Auswahl*-Tasten können von Ihnen verändert werden.

**So ändern Sie die Stream-Auswahl-Tasten:**

OSD

1. Starten Sie das OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**).
2. Betätigen Sie die **F11**-Taste.
3. Wählen Sie die Zeile **Hotkeys** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie in der Zeile **Stream-Auswahl** die gewünschte Option aus:

   **Pfeil links, rechts** ‣ *Pfeil links*-Taste und *Pfeil rechts*-Taste (*Standard*)
   **Num+, Num-** ‣ *Num+*-Taste und *Num-*-Taste
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Betriebsmodus der RS232-Schnittstelle einstellen

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

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

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

**So stellen Sie den Betriebsmodus der RS232-Schnittstelle ein:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**, falls Sie die Einstellung für das Arbeitsplatzmodul vornehmen möchten.

   Wählen Sie die Zeile **Rechnermodul-Einrichtung** und betätigen Sie die **Eingabetaste**, falls Sie die Einstellung für das Rechnermodul vornehmen möchten.
3. Wählen Sie in der Zeile **RS232-Port-Modus** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **RS232** ‣ Der Datenstrom eines RS232-Gerätes wird vom Rechnermodul zum Arbeitsplatzmodul übertragen (*Standardeinstellung*).

   **RS422-Adapter** ‣ Der Datenstrom eines RS422-Gerätes wird über die separat erhältlichen **G&D RS232-422-Adapter** vom Rechnermodul zum Arbeitsplatzmodul übertragen.
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Auswahl des EDID-Modus des KVM-Extenders

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

**HINWEIS:** Beachten Sie bei der Erstinbetriebnahme sowie bei Anschluss eines anderen Monitors die auf Seite 31 empfohlene Einschaltreihenfolge.

Für bestimmte Auflösungen werden spezielle GUD-Profile mitgeliefert. Die Namen dieser Profile geben Auskunft über die bevorzugte Auflösung, die bei Anwendung des Profils an die Grafikkarte des Rechners übermittelt wird.

**WICHTIG:** Beachten Sie, dass das am Rechnermodul ausgewählte Profil auch vom Arbeitsplatzmodul und dem dort angeschlossenen Monitor unterstützt werden muss. Ansonsten erscheint eine Fehlermeldung, z. B. *Pixeltakt zu hoch* (Pixeltakt höher als vom aktuellen Arbeitsplatzmodul unterstützt).

Alternativ kann in der Webapplikation **Config Panel** das EDID-Profil eines Monitores eingelesen und durch den KVM-Extender an den angeschlossenen Rechner übermittelt werden. Ausführliche Informationen hierzu finden Sie im separaten Handbuch zur Webapplikation **Config Panel**.

**So wählen Sie den EDID-Modus des KVM-Extenders:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

   Wählen Sie die Zeile **Rechnermodul-Einrichtung** und betätigen Sie die **Eingabetaste**.

2. Wählen Sie in der Zeile **EDID-Modus** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **Auto** ‣ automatische Behandlung der EDID-Daten (*Standard*)
   **Benutzer** ‣ Verwendung eines G&D-Profils oder eines vom Benutzer in der Webapplikation eingelesenen Profils

3. Falls Sie die Option **Benutzer** gewählt haben, wählen Sie die Zeile **EDID zuweisen** und betätigen Sie die **Eingabetaste**.

   Wählen Sie mit den **Pfeiltasten** das zu aktivierende Profil und aktivieren Sie es mit der **F8**-Taste. Speichern Sie Ihre Auswahl mit der **F2**-Taste.

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Reduzierung der Farbtiefe der zu übertragenden Bilddaten

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

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

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

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

**So ändern Sie die Farbtiefe der zu übertragenden Bilddaten:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

   Wählen Sie die Zeile **Rechnermodul-Einrichtung** und betätigen Sie die **Eingabetaste**.

2. Wählen Sie in der Zeile **Farbtiefe** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

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

3. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Verwendung des Freeze-Modus

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

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

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

**So konfigurieren Sie den Freeze-Modus:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

   Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.

2. Wählen Sie in der Zeile **Freeze-Modus** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **aus** ‣ Freeze-Modus deaktiviert (*Standard*)
   **an** ‣ Freeze-Modus aktiviert

3. Falls der *Freeze*-Modus aktiviert ist, wählen Sie in der Zeile **Freeze-Visualisation** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **Rahmen** ‣ Anzeige eines farbigen Rahmens bei Verbindungsabbruch
   **OSD** ‣ Einblendung des Hinweises Eingefroren und der vergangenen Zeit seit dem Verbindungsabbruch
   **Rahmen+OSD** ‣ Anzeige des farbigen Rahmens (**frame**) und Einblendung des Hinweises *Eingefroren* (**OSD**)

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## DDC/CI-Unterstützung (de)aktivieren

Die vom **VisionXS-IP-F-TypeC-UHR**-System unterstützten Rechner- und Arbeitsplatzmodule wurden vorbereitet, um Monitore mit **DDC/CI**-Funktion zu unterstützen.

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

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

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

   Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.

2. Wählen Sie in der Zeile **DDC/CI-Unterstützung** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   | | |
   |---|---|
   | **aus** | ‣ Die Übertragung von DDC/CI-Signalen ist deaktiviert (*Standard*). |
   | **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. |

3. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

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

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

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

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

**WICHTIG:** Das Arbeitsplatzmodul erlaubt die gleichzeitige Nutzung von bis zu fünf Generic-USB-Geräten. Hierfür muss sowohl das eingesetzte Arbeitsplatzmodul als auch das eingesetzte Rechnermodul die Nutzung von bis zu fünf GenericUSB-Geräten unterstützen.

Es können nur bis zu drei HighSpeed-Geräte (z. B. USB-Flashdrive) und zwei FullSpeed-Devices verwendet werden. Werden darüber hinaus weitere High-Speed-Geräte verbunden, werden diese nicht akzeptiert.

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

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

Die folgende Tabelle listet die unterstützten USB-Tastaturen auf:

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

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

| EINGABEGERÄT | EINSTELLUNG |
|---|---|
| iiyama ProLite TF2415 | ‣ iiyama TF2415 |
| Wacom Intuos5 S | ‣ Wacom Intuos 5S |
| Wacom Intuos5 M | ‣ Wacom Intuos 5M |
| Wacom Intuos5 L | ‣ Wacom Intuos 5L |
| Wacom IntuosPro L | ‣ Wacom IntuosPro L |
| Wacom Cintiq Pro 24 Pen | ‣ Wacom CP24 Pen |
| Wacom Cintiq Pro 27 | ‣ Wacom CP27 Pen/Touch |
| Wacom Cintiq Pro 32 Pen | ‣ Wacom CP32 Pen |
| Wacom Cintiq Pro 32 Touch | ‣ Wacom CP32 Touch |
| Wacom DTK-2451 | ‣ Wacom DTK-2451 |

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

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

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

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

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

| EINGABEGERÄT | EINSTELLUNG |
|---|---|
| LK463-kompatible Tastatur | ‣ LK463 |

**So wählen Sie einen USB-HID-Modus:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Rechnermodul-Einrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **USB-HID-Modus** und betätigen Sie die **F8**-Taste zur Auswahl einer Option (s. oben).
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## USB-Gerät für einen Neustart priorisieren

Wenn im Generic-USB-Modus mehrere USB-Geräte angeschlossen und erkannt werden, wird im *Standard* nach einem Neustart des Arbeitsplatzmoduls das USB-Gerät verbunden, das zuerst erkannt wurde. Wenn sowohl das eingesetzte Arbeitsplatzmodul als auch das eingesetzte Rechnermodul die Nutzung von bis zu fünf Generic-USB-Geräte unterstützt, werden bis zu fünf USB-Geräte entsprechend der Reihenfolge der Erkennung wieder verbunden. Diese Geräte erscheinen im OSD gelb und mit einem Sternchen (✱) markiert.

Sie haben die Möglichkeit, ein USB-Gerät zu bestimmen, das nach einem Neustart priorisiert werden soll und auf jeden Fall wieder im Zugriff sein soll.

**So priorisieren Sie ein USB-Gerät für den Neustart:**

OSD

1. Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**).
2. Betätigen Sie die **F11**-Taste.
3. Wählen Sie die Zeile **Tastatur/Maus** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Generic USB** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie das USB-Gerät aus, das nach einem Neustart auf jeden Fall wieder im Zugriff sein soll und betätigen Sie die **Eingabetaste**.

   Dieses Gerät erscheint im OSD nun grün und mit einem Dreieck (▶) markiert.
6. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

**HINWEIS:** Die Priorisierung bleibt auch bestehen, wenn das USB-Gerät vom Arbeitsplatzmodul getrennt wird (erscheint im OSD dann rot) und anschließend wieder verbunden wird (erscheint im OSD dann wieder grün und mit einem Dreieck (▶) markiert).

## Reinitialisierung von USB-Eingabegeräten

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

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

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

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie in der Zeile **USB-Auto-Refresh** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **nur fehlerhafte** ‣ Der Status der USB-Geräte wird überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, wird dieses Gerät reinitialisiert (*Standard*).

   **alle** ‣ Der Status der USB-Geräte wird überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, werden alle angeschlossenen USB-Geräte reinitialisiert.

   **aus** ‣ Der Status der USB-Geräte wird **nicht** überwacht. Falls die Kommunikation zu einem USB-Gerät gestört ist, findet **keine** Reinitialisierung statt.
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Wartezeit des Bildschirmschoners einstellen

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

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

**So stellen Sie die Wartezeit des Bildschirmschoners ein:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).

   Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**, falls Sie den Bildschirmschoner des entfernten Arbeitsplatzes (am **CON**-Modul) einstellen möchten.

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

   *Der Wert 0 deaktiviert den Bildschirmschoner.*

3. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Automatische Abmeldung der Benutzer einstellen

Ein Arbeitsplatzmodul kann so konfiguriert werden, dass eine aktive Aufschaltung auf ein Rechnermodul nach einem bestimmten Zeitraum der Inaktivität des Benutzers automatisch getrennt und der Benutzer vom KVM-Matrixsystem abgemeldet wird.

**So stellen Sie die automatische Abmeldung der Benutzer ein:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Geben Sie in der Zeile **Auto-Logout (min)** den Zeitraum (1 bis 999 Minuten) bis zur automatischen Abmeldung ein.

   *Der Wert 0 deaktiviert die automatische Abmeldung der Benutzer am Arbeitsplatzmodul.*

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Tastaturlayout für Eingaben innerhalb des OSD auswählen

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

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

**So wählen Sie das Tastaturlayout der Tastatur des Arbeitsplatzmoduls aus:**

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg+Num**), falls Sie die Einstellungen für das entfernte OSD ändern möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt+Num**), falls Sie die Einstellungen für das lokale OSD ändern möchten.

2. Wählen Sie die Zeile **Arbeitsplatzeinrichtung** und betätigen Sie die **Eingabetaste** (entferntes OSD) bzw. betätigen Sie die **F11**-Taste, wählen die Zeile **Tastatur/Maus** und betätigen Sie die **Eingabetaste** (lokales OSD).

3. Wählen Sie in der Zeile **OSD-Tastatur-Layout** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   - **Deutsch** (*Standard*)
   - **US-Englisch**
   - **UK-Englisch**
   - **Französisch**
   - **Spanisch**
   - **Lat.-amerik.**
   - **Portugiesisch**
   - **Schwedisch**
   - **Schweiz-Französich**
   - **Dänisch**

4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Wiederherstellung der Standardeinstellungen

Mit dieser Funktion werden die *Standardeinstellungen* des KVM-Extenders wiederhergestellt. Nach dem Ausführen der Funktion sind die auf Seite 96 aufgeführten *Standardeinstellungen* des KVM-Extenders wieder aktiv.

**So stellen Sie die Standardeinstellungen wieder her:**

**HINWEIS:** Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **local hotkey** (*Standard*: **Alt**+**Num**), falls Sie statt den Einstellungen des Extender-Systems nur die **lokalen** Einstellungen des Arbeitsplatzmodul zurücksetzen möchten.

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**), falls Sie die Einstellungen des Extender-Systems zurücksetzen möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**), falls Sie nur die lokalen Einstellungen des Arbeitsplatzmodul zurücksetzen möchten.
2. Wählen Sie die Zeile **System-Einrichtung** (entferntes OSD) bzw. **Arbeitsplatz-Utility** (lokales OSD) und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Werkseinstellungen wiederherstellen** und betätigen Sie die **Eingabetaste**.
4. Bestätigen Sie die Sicherheitsabfrage oder brechen Sie den Vorgang ab.

## Reset der Netzfilterregeln

Im Auslieferungszustand des KVM-Extenders haben alle Netzwerk-Rechner Zugriff auf die IP-Adresse des Systems (offener Systemzugang).

Über die Webapplikation **Config Panel** können Sie Netzfilterregeln erstellen, um den Zugang gezielt zu kontrollieren. Sobald eine Netzfilterregel erstellt ist, wird der offene Systemzugang deaktiviert und alle eingehenden Datenpakete mit den Netzfilterregeln verglichen.

Mit dieser Funktion können die angelegten Netzfilterregeln vollständig gelöscht werden.

**So löschen Sie die eingerichteten Netzfilterregeln:**

OSD

1. Starten Sie das entfernte OSD des Rechnermoduls mit dem **Remote-Hotkey** (*Standard*: **Strg**+**Num**), falls Sie die Einstellungen des Extender-Systems zurücksetzen möchten.

   Öffnen Sie das lokale OSD des Arbeitsplatzmoduls mit dem **lokalen Hotkey** (*Standard*: **Alt**+**Num**), falls Sie nur die lokalen Einstellungen des Arbeitsplatzmodul zurücksetzen möchten.
2. Wählen Sie die Zeile **Netzwerkeinrichtung** und betätigen Sie die **Eingabetaste**.
3. Wählen Sie die Zeile **Netzfilterkonfiguration zurücksetzen** und betätigen Sie die **Eingabetaste**.
4. Bestätigen Sie die Sicherheitsabfrage oder brechen Sie den Vorgang ab.

## 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:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie in der Zeile **OSD-Farbe** durch Betätigung der **F8**-Taste die gewünschte Farbe.
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Anzeige der Informationseinblendung

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

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

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

**So ändern Sie die Einstellung der Informationseinblendung:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie in der Zeile **Einblendung (allgemein)** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **aus** ‣ Informationseinblendung ausschalten
   **temp** ‣ temporäre Informationseinblendung für 5 Sekunden (*Standard*)
   **perm** ‣ permanente Informationseinblendung
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## 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:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie in der Zeile **OSD-Transparenz** durch Betätigung der **F8**-Taste zwischen folgenden Optionen:

   **hoch** ‣ hohes Durchscheinen des Bildschirminhalts
   **mittel** ‣ mittleres Durchscheinen des Bildschirminhalts (*Standard*)
   **niedrig** ‣ leichtes Durchscheinen des Bildschirminhalts
   **aus** ‣ überdeckende Darstellung des OSD
4. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Automatisches Schließen des OSD nach Inaktivität

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

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

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

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

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie die Zeile **Timeout der OSD-Sitzung (s)** und betätigen Sie die **Eingabetaste**.
4. Geben Sie die gewünschte Zeitspanne im Bereich von **5** bis **99** Sekunden ein und betätigen Sie die **Eingabetaste**.
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen.

## Position der Informationseinblendung ändern

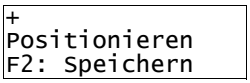
In der *Standardeinstellung* erfolgen die Informationseinblendungen links oben auf dem Bildschirm des Arbeitsplatzes. Die Position der Einblendung können Sie nach Ihren Wünschen anpassen.

**So ändern Sie die Position der Informationseinblendung:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie die Zeile **Display-Position festlegen** und betätigen Sie die **Eingabetaste**.

   An der aktuellen Position der Informationseinblendung erscheint das rechts abgebildete Menü.




4. Verwenden Sie die **Pfeiltasten** oder die Maus, um das Menü an die gewünschte Position zu verschieben oder betätigen Sie die Tastenkombination **Strg+D** zur Wiederherstellung der *Standardposition*.
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen oder die **Esc**-Taste zum Abbruch der Aktion.

## Position des OSD ändern

Das OSD wird in der *Standardeinstellung* zentriert auf dem Bildschirm des Arbeitsplatzes dargestellt. Die OSD-Position können Sie nach Ihren Wünschen anpassen.

**So ändern Sie die Position des OSD:**

OSD

1. Starten Sie das OSD mit dem Hotkey **Strg+Num** (*Standard*).
2. Betätigen Sie die **F10**-Taste zum Aufruf des **Persönlichen Profils**.
3. Wählen Sie die Zeile **Menü-Position festlegen** und betätigen Sie die **Eingabetaste**.
4. Verwenden Sie die **Pfeiltasten** oder die Maus, um das OSD an die gewünschte Position zu verschieben oder betätigen Sie die Tastenkombination **Strg+D** zur Wiederherstellung der *Standardposition.*
5. Betätigen Sie die **F2**-Taste zur Speicherung der durchgeführten Änderungen oder die **Esc**-Taste zum Abbruch der Aktion.

# Weiterführende Informationen

## DDC-Weiterleitung mit Cache-Funktion

Der KVM-Extender unterstützt *Enhanced-DDC* (Enhanced Display Data Channel), um die Eigenschaften des am Arbeitsplatzmoduls angeschlossenen Monitors auszulesen und an den Rechner weiterzuleiten. Diese Eigenschaften umfassen beispielsweise Informationen über die bevorzugte Auflösung und die unterstützten Frequenzen des Monitors.

Damit der am Rechnermodul (**VisionXS-IP-CPU**) angeschlossene Rechner schon während des Bootvorgangs Zugriff auf die Eigenschaften des entfernten Monitors hat, ist eine Cache-Funktion in den KVM-Extender integriert. Auch wenn das Rechner- oder das Arbeitsplatzmodul ausgeschaltet oder nicht miteinander verbunden sind, stehen entweder die Eigenschaften des zuletzt angeschlossenen Monitors oder die Werksvorgabe des KVM-Extenders zu Verfügung.

Üblicherweise werden die DDC-Informationen des Monitors unverändert an den Rechner weitergeleitet. Stellt der KVM-Extender aber fest, dass sich die Informationen des Monitors nicht vollständig auslesen lassen oder diese unzulässige Einträge enthalten, werden die Informationen (wenn möglich) vervollständigt oder korrigiert.

# Ermittlung der Netzwerkeinstellungen über den Service-Port

Falls Ihnen die IP-Adresse eines Arbeitsplatzmoduls oder Rechnermoduls unbekannt ist, können Sie diese über den Service-Port des Moduls anzeigen.

Verwenden Sie ein beliebiges Terminalemulationsprogramm (beispielsweise *Tera Term* oder *PuTTY*) um die Log-Meldungen der Module anzuzeigen.

## Installation des Gerätetreibers

Installieren Sie vor der Einrichtung der Verbindung im Terminalemulationsprogramm den Gerätetreiber **CP210x USB to UART Bridge VCP**.

**HINWEIS:** Der Treiber stellt die per Servicekabel verbundene *Service*-Buchse eines Arbeitsplatzmoduls oder Rechnermoduls als *virtuelle* serielle Schnittstelle (COM-Port) zur Verfügung. Die virtuelle Schnittstelle kann anschließend im Terminalemulationsprogramm zum Verbindungsaufbau ausgewählt werden.

**So installieren Sie den Gerätetreiber zur Adressierung der Service-Buchse:**

1. Öffnen Sie im Webbrowser des Computer die Website **www.gdsys.com/de**.
2. Navigieren Sie in den Bereich **Service > Downloads > Tools & Treiber** der Website.
3. Downloaden Sie den Gerätetreiber für das Betriebssystem des Computers.
4. Führen Sie die Datei aus und folgen Sie den Hinweisen des Installationsassistenten.

## Einrichten einer Verbindung im Terminalemulationsprogramm

**So richten Sie die Verbindung im Terminalemulationsprogramm ein:**

1. Starten Sie ein beliebiges Terminalemulationsprogramm (beispielsweise *Tera Term* oder *PuTTY*).
2. Erstellen Sie eine neue Verbindung im Terminalemulationsprogramm und erfassen Sie folgende Verbindungseinstellungen:
   - Bits pro Sekunde: 115.200
   - Datenbits: 8
   - Parität: Keine
   - Stoppbits: 1
   - Flusssteuerung: Keine
3. Verwenden Sie das mitgelieferte USB-Servicekabel, um den Rechner mit der *Service*-Buchse an der Rückseite des Arbeitsplatzmodul bzw. Rechnermodul zu verbinden.

### Ermittlung der IP-Adresse

**So ermitteln Sie die IP-Adresse des Arbeitsplatzmoduls bzw. Rechnermoduls:**

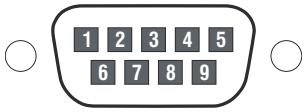
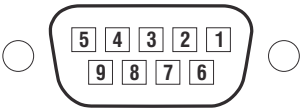
1. Starten Sie das Arbeitsplatzmodul bzw. Rechnermodul neu.

   Während des Bootvorgangs werden verschiedene Statusmeldungen im Terminalemulationsprogramm angezeigt.

2. Nach Abschluss der Boot-Vorgangs wird die IP-Adresse gemeinsam mit anderen **Systeminformationen** ausgegeben.

## Pin-Belegung der RS232-Schnittstelle

Die Pin-Belegungen des RS232-Steckers sowie der -Buchse (modellabhängig) zeigen die folgenden Abbildungen:

| Arbeitsplatzmodul | Rechnermodul |
|---|---|
|  |  |
| RS232-Stecker | RS232-Buchse |

Die Tabelle zeigt die Zuordnung der verschiedenen Leitungen der Datenverbindung zu den entsprechenden Pins auf:

| Pin-Nr. | Leitung | Arbeitsplatz-modul | Rechner-modul |
|---|---|---|---|
| 1 | *nicht belegt* | n/c | n/c |
| 2 | RxD (Receive Data) | Eingang | Ausgang |
| 3 | TxD (Transmit Data) | Ausgang | Eingang |
| 4 | *nicht belegt* | n/c | n/c |
| 5 | GND (Ground) | Ground | Ground |
| 6 | *nicht belegt* | n/c | n/c |
| 7 | RTS (Request to Send) | Ausgang | Eingang |
| 8 | CTS (Clear to Send) | Eingang | Ausgang |
| 9 | 5V | Power | Power |

# Statusanzeigen

Die LEDs an der Vorder- und Rückseite des Rechner- und des Arbeitsplatzmoduls geben Ihnen die Möglichkeit, den Betriebsstatus des KVM-Extenders jederzeit zu kontrollieren.

## LED an der Frontseite des Rechnermoduls




| LED | Farbe | Status | Bedeutung |
|---|---|---|---|
| | grün | an | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode und USB 2.0 zu liefern |
| | | blinkt | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode, USB 2.0 und Power Delivery (36W) zu liefern |
| | gelb | an | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode zu liefern, jedoch kein USB 2.0 |
| | | blinkt | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode und USB Power Delivery (36W) zu liefern, jedoch kein USB 2.0 |
| | rot | an | Quelle bietet USB Power (5V/0,5A), jedoch kein DP1.2 Alt-Mode |
| | | aus | keine Quelle erkannt |

# LED an der Vorderseite des Arbeitsplatzmoduls




| LED | Farbe | Status | Bedeutung |
|---|---|---|---|
| | grün | an | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode und USB 2.0 zu liefern |
| | | blinkt | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode, USB 2.0 und Power Delivery (36W) zu liefern |
| | gelb | an | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode zu liefern, jedoch kein USB 2.0 |
| | | blinkt | Quelle bietet USB Power (5V/0,5A) und ist bereit, DP1.2 Alt-Mode und USB Power Delivery (36W) zu liefern, jedoch kein USB 2.0 |
| | rot | an | Quelle bietet USB Power (5V/0,5A), jedoch kein DP1.2 Alt-Mode |
| | | aus | keine Quelle erkannt |

## LEDs an der Rückseite




| LED | Farbe | Status | Bedeutung |
|---|---|---|---|
| **Trans-mission** | grün | an | Eine G&D Gegenstelle ist aufgeschaltet. |
| | gelb | an | Kommunikation mit einer G&D-Gegenstelle aufgebaut. |
| | | blinkt | Verbindung zu einer Gegenstelle/einem Netzwerk-Switch hergestellt. |
| | | blinkt schnell | SFP-Modul nicht erkannt. |
| | | aus | Keine Verbindung zu einer Gegenstelle hergestellt.<br>Die **Transmission 2**-Schnittstelle muss vor der Verwendung zunächst mit dem kostenpflichtig erhältlichen **Transm. Redundancy**-Feature aktiviert werden. |
| **Network** | grün | an | Die Verbindung mit dem Netzwerk wurde erfolgreich aufgebaut. |
| | | aus | Es konnte keine Verbindung hergestellt werden. |
| **Pwr** | grün | an | Der KVM-Extender wird mit Spannung versorgt und die Gerätesoftware wurde erfolgreich gestartet. |
| | gelb | an | Der KVM-Extender wird mit Spannung versorgt. |
| | blau | an | Die Identification-Funktion wurde über die Webapplikation aktiviert. |
| | | aus | Der KVM-Extender wird nicht mit Spannung versorgt. |

# Verwendete Netzwerk-Ports und Protokolle

**HINWEIS:** Eine Übersicht über die Netzwerk-Ports und Protokolle, die bei KVM-over-IP von G&D verwendet werden können, finden Sie im separaten Handbuch zur Webapplikation.

# Technische Daten

## Allgemeine Eigenschaften der Serie

| VISIONXS-IP-F-TYPEC-UHR-SERIE | | |
|---|---|---|
| **Schnittstellen für Rechner** | USB-Type-C: | 1 × USB-Type-C-Buchse |
| | USB-Tastatur/Maus: | 1 × USB-B-Buchse<br>(USB-Tastatur/Maus alternativ auch über die USB-Type-C-Schnittstelle möglich) |
| | Audio:<br>‣ Varianten [A] und [AR] | 3,5-mm-Klinkenbuchse (Line In) |
| | RS232:<br>‣ Varianten [AR] | 1 × RS232-Buchse (Serial) |
| **Schnittstellen für entfernten Arbeitsplatz** | Videoausgang: | 1 × USB-Type-C-Buchse |
| | USB-Tastatur/Maus: | 2 × USB-A-Buchse |
| | USB-Devices: | 3 × USB-A-Buchse |
| | Audio:<br>‣ Varianten [A] und [AR] | 3,5-mm-Klinkenbuchse (Line Out) |
| | RS232:<br>‣ Varianten [AR] | 1 × RS232-Stecker (Serial) |
| **Übertragung zur G&D-Gegenstelle** | Übertragungsart: | KVM-over-IP™ |
| | Anzahl Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional]<br>‣ Der zweite Übertragungskanal kann mit einem optional käuflichen Feature-Key freigeschaltet werden. |
| **Sonstige Schnittstellen** | Network: | 1 × RJ45-Buchse (100 MBit/s) |
| | Service: | 1 × Micro-USB-Buchse (Typ B) |
| **Audio**<br>‣ Digital Embedded | Übertragungsart: | 2-Kanal-LPCM, Stereo, DTS, AC3 |
| | Auflösungen: | 16/20/24 bit |
| | Abtastraten: | bis 192 kHz (Rechnermodule)<br>bis 48 kHz (Arbeitsplatzmodule) |
| **Audio**<br>‣ Varianten [A] und [AR] | Übertragungsart: | transparent |
| | Auflösung: | 24 bit digital, Stereo |
| | Abtastrate | 96 kHz |
| | Bandbreite: | 22 kHz |
| **RS232**<br>‣ Varianten [AR] | Übertragungsart: | transparent |
| | Übertragungsrate: | max. 115.200 bit/s |
| | Übertragene Signale: | RxD, TxD, GND, RTS, CTS, 5V |

| VISIONXS-IP-F-TYPEC-UHR-SERIE | | |
|---|---|---|
| **Generic USB**<br>› Standard-CPU-Varianten unterstützen 1 Gerät, CPU-UG-Varianten unterstützen bis zu 5 Geräte | Spezifikation: | USB 2.0 |
| | USB-Klassen: | Human Interface Device (HID) |
| | | Massenspeicher (MSC/UMS) |
| | | SmartCard |
| | Übertragungsrate: | max. 25 Mbit/s |
| **Grafik** | Format: | DP1.2 Alt-Mode, LBR, HBR, HBR2, SingleStream-Transport (SST) |
| | Farbtiefe: | 24 bit |
| | Pixelkodierung: | RGB 4:4:4 mit 24bpp/8bpc |
| | Pixelrate: | ca. 25 MP/s bis ca. 600 MP/s |
| | max. Auflösung: | ▪ 5120 × 2160 @ 50 Hz<br>▪ 5120 × 1440 @ 60 Hz<br>▪ 4096 × 2160 @ 60 Hz (4K2K/60Hz)<br>▪ 2560 × 1440 @ 144 Hz<br>▪ 1920 × 1080 @ 240 Hz (Full HD/240Hz) |
| | Auflösungsbeispiele: | ▪ 3840 × 2160 @ 60 Hz (Ultra HD/60Hz)<br>▪ 2560 × 1600 @ 60Hz<br>▪ 2048 × 2048 @ 60Hz (2K × 2K)<br>▪ 1920 × 1200 @ 60Hz<br>▪ 1920 × 1080 @ 60Hz |
| | | › Weitere nach VESA und CTA standardisierte Auflösungen sind im Rahmen der unterstützten Videobandbreite/Pixelrate und Horizontal-/Vertikalfrequenz möglich. |
| | Vertikalfrequenz: | 24 Hz bis 240 Hz |
| | Horizontalfrequenz: | 25 kHz bis 295 kHz |
| **Hauptstromversorgung** | Typ: | externe Spannungsversorgung |
| | Anschluss: | miniDIN-4 Power-Buchse |
| | Spannung: | +12VDC |
| **redundante Stromversorgung**<br>› Varianten [DT] | Typ: | internes Netzteil |
| | Anschluss: | Kaltgerätestecker (IEC-320 C14) |
| | Spannung: | AC100-240V/60-50Hz |
| **alternative Stromversorgung**<br>› Zur Durchführung von Updates ist die alleinige Spannungsversorgung über USB Power Delivery nicht ausreichend. | Typ: | USB Power Delivery 3.0/3.1<br>(bis zu 30 Watt) |
| | Betriebsbereiche: | 12V/1,5-2A |
| | | 15V/1-2A |
| | | 20V/0,75-1,5A |
| **Einsatzumgebung**<br>› Sorgen Sie für eine ausreichende Luftzirkulation. | Temperatur: | +5 bis +45 °C |
| | Luftfeuchte: | 20 % bis 80 %, nicht kondensierend |

| VISIONXS-IP-F-TYPEC-UHR-SERIE | | |
|---|---|---|
| **Lagerumgebung** | Temperatur: | -20 °C bis +60 °C |
| | Luftfeuchte: | 15 % bis 85 %, nicht kondensierend |
| **Konformität** | | CE, UKCA, FCC Klasse B, TAA, EAC, RoHS, WEEE, REACH |

# Spezifische Eigenschaften der Geräte

| VISIONXS-IP-CPU-F-TYPEC-UHR | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Stromversorgung: | 12 VDC/1,6 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 109 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 0,9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-UG | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Stromversorgung: | 12 VDC/1,6 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 109 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 0,9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/1,8 A |
| | redundante Stromversorgung | 100-240 VAC/60-50Hz/0,5-0,3 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-UG-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/1,8 A |
| | redundante Stromversorgung | 100-240 VAC/60-50Hz/0,5-0,3 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-AR-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/1,8 A |
| | redundante Stromversorgung | 100-240 VAC/60-50Hz/0,5-0,3 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-AR-UG-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/1,8 A |
| | redundante Stromversorgung | 100-240 VAC/60-50Hz/0,5-0,3 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-A | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Stromversorgung: | 12 VDC/1,6 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 109 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 0,9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-A-UG | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Stromversorgung: | 12 VDC/1,6 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 109 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 0,9 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Stromversorgung: | 12 VDC/2,5 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 109 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 0,9 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/2,5 A |
| | redundante Stromversorgung: | 100-240 VAC/60-50Hz/0,65-0,35 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR-AR-DT | | |
|---|---|---|
| **Schnittstellen zur Gegenstelle** | Übertragungskanäle: | 1, inkl. Übertragunsmodul/ SFP-Transceiver [+1 optional] × LC-Duplex-Buchse (10 GBit/s) |
| **Stromaufnahme** | Hauptstromversorgung: | 12 VDC/2,5 A |
| | redundante Stromversorgung: | 100-240 VAC/60-50Hz/0,65-0,35 A |
| **Gehäuse** | Material: | Aluminium eloxiert |
| | Dimensionen (B × H × T): | ca. 170 × 40 × 184 mm |
| | IP-Schutzklasse: | IP20 |
| | Gewicht: | ca. 1,3 kg |

# Eigenschaften der Übertragungsmodule

| MULTIMODE-ÜBERTRAGUNGSMODUL | | |
|---|---|---|
| **Datenübertragung** | Art: | Lichtwellenleiter (2 Glasfasern) |
| | Schnittstellentyp: | LC-Duplex |
| **Kabellänge (max.)** | Multimode 50/125µm, Klasse OM4: | 400 Meter (Fasern mit 4700MHz*km) |
| | Multimode 50/125µm, Klasse OM3: | 300 Meter (Fasern mit 2000MHz*km) |
| | Multimode 50/125µm, Klasse OM2: | 82 Meter (Fasern mit 500MHz*km) |
| | Multimode 50/125µm: | 66 Meter (Fasern mit 400MHz*km) |
| | Multimode 62,5/125µm, Klasse OM1: | 33 Meter (Fasern mit 200MHz*km) |
| | Multimode 62,5/125µm, FDDI-Grade: | 26 Meter (Fasern mit 160MHz*km) |

| SINGLEMODE-ÜBERTRAGUNGSMODUL | | |
|---|---|---|
| **Datenübertragung** | Art: | Lichtwellenleiter (2 Glasfasern) |
| | Schnittstellentyp: | LC-Duplex |
| **Kabellänge (max.)** | Singlemode 9/125µm, Klasse OS1: | 10 Kilometer (Fasern mit 500MHz*km) |

# NOTIZEN

# NOTIZEN

## About this manual

This manual has been carefully compiled and examined to the state-of-the-art.

G&D neither explicitly nor implicitly takes guarantee or responsibility for the quality, efficiency and marketability of the product when used for a certain purpose that differs from the scope of service covered by this manual.

For damages which directly or indirectly result from the use of this manual as well as for incidental damages or consequential damages, G&D is liable only in cases of intent or gross negligence.

## Caveat Emptor

G&D will not provide warranty for devices that:

- Are not used as intended.
- Are repaired or modified by unauthorized personnel.
- Show severe external damages that was not reported on the receipt of goods.
- Have been damaged by non G&D accessories.

G&D will not be liable for any consequential damages that could occur from using the products.

## Proof of trademark

- USB Type-C® and USB-C® are registered trademarks of USB Implementers Forum.
- All other product and company names mentioned in this manual, and other documents you have received alongside your G&D product, are trademarks or registered trademarks of the holder of rights.

© Guntermann & Drunck GmbH 2026. All rights reserved.

**Version 1.32 – 24/07/2026**
Firmware: 1.8.000

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

Phone +49 271 23872-0
Fax +49 271 23872-120

www.gdsys.com
sales@gdsys.com

## FCC Statement

The devices named in this manual comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) the devices may not cause harmful interference, and (2) the devices must accept any interference received, including interference that may cause undesired operation.

**NOTE:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be deter-mined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

# Table of contents

**Safety instructions** ..... **1**

**The VisionXS-IP-F-TypeC-UHR series** ..... **5**
Use as extender or matrix switch modules ..... 5
Package contents ..... 6

**Secure KVM-over-IP solution** ..... **7**
Potential security vulnerabilitites, threats and dangers ..... 7
Protection of KVM systems from external or internal attacks ..... 7
Security requirements with KVM-over-IP ..... 7
The secure solution from G&D ..... 8
Trusted Computing Platform ..... 10
Monitoring, SNMP and Syslog ..... 10
Update and Backup/Restore ..... 10
Further security-relevant aspects ..... 11
2-factor authentication (2FA) ..... 11
Optional additional security-relevant functions ..... 12
SecureCert ..... 12

**Signal transmission and transmission length** ..... **13**

**Selecting a network switch** ..... **13**
Requirements of network switches ..... 13

**Installation** ..... **15**
Preparation ..... 15
Installing the computer module ..... 16
Installing console modules ..... 24

**Start-up** ..... **31**
Power-up ..... 31
Starting process ..... 31
Power-down ..... 31
Operation ..... 32
User login at the console module ..... 33
Configuring the password complexity ..... 34
Configuring the login options ..... 36
Showing terms of use ..... 38
User logout at the console module ..... 39

**Establishing a KVM-over-IP™ connection for the first time** ..... **40**
Default setting of the modules ..... 40
Configuring a KVM-over-IP connection of a computer module ..... 41
Configuring the network interface ..... 42
Configuring the global network settings ..... 43
Configuring a KVM-over-IP connection ..... 44

Configuring a KVM-over-IP connection of a console module ..... 45
Configuring the network interface ..... 45
Configuring the global network settings ..... 47
Configuring a KVM-over-IP connection ..... 48
Add, configuration and deletion of a counterpart ..... 49
Extended settings of KVM-over-IP connection ..... 51
Limiting the bandwidth ..... 51
Classifying IP packets (DiffServ) ..... 52
(De)Activating signals ..... 53
Restricting KVM-over-IP remote stations (UID locking) ..... 54

**IP-MUX functionality ..... 55**
Accessing a counterpart via OSD ..... 55
Accessing a counterpart via select keys ..... 56
Disconnecting a counterpart ..... 57

**Initial configuration of the network settings ..... 58**
Configuring the network interface ..... 59
Configuring global network settings ..... 61
Checking the availability of a host in the network (Ping) ..... 63
Link aggregation ..... 64
Reading out the status of the network interfaces ..... 66

**On-screen display ..... 67**
Basic operating of the on-screen display ..... 67
Showing the remote OSD ..... 68
Showing the local OSD ..... 68
Layout of the OSD ..... 68
Operating the OSD via keyboard or mouse ..... 69
OSD functions ..... 71
Search function ..... 71
Changing the sort criteria of the list entries ..... 71
Overview of the menus of the remote OSD ..... 72
Configuration menu ..... 72
Personal Profile menu ..... 74
Operation menu ..... 74
Information menu ..... 75
Overview of the menus of the local OSD ..... 75
Select menu ..... 75
Configuration menu ..... 76

**Activating a premium function ..... 76**

**Web application Config Panel ..... 77**
Basic operation of the web application ..... 77
Starting the web application ..... 77
Selecting the language of the web application ..... 79
Closing the web application ..... 79

**Users and groups** ..... **80**
Efficient rights administration ..... 80
The effective right ..... 80
Efficient user group administration ..... 81
Administrating user accounts ..... 82
Creating a new user account ..... 82
Renaming a user account ..... 83
Changing the password of a user account ..... 84
Changing the user account rights ..... 85
Changing a user account's membership ..... 86
Enabling or disabling a user account ..... 87
Deleting a user account ..... 87
Administrating user groups ..... 88
Creating a new user group ..... 88
Renaming a user group ..... 89
Changing the user group rights ..... 89
Administrating user group members ..... 90
(De)activating a user group ..... 91
Deleting a user group ..... 91
System rights ..... 92
Rights for unrestricted access to the system (Superuser) ..... 92
Changing settings in the »Personal Profile« menu ..... 93
Changing the login right to the web application ..... 93
Rights to change your own password ..... 94
Access rights to a computer module ..... 94
Access rights to USB devices ..... 95

**Configuration** ..... **96**
Overview of functions and default settings ..... 96
Configuration settings ..... 98
Operating modes of console modules ..... 98
Renaming a console module ..... 99
Renaming a computer module ..... 99
Changing your password ..... 100
Selecting the language ..... 101
Changing hotkeys ..... 102
Changing the OSD key ..... 103
Opening the OSD via double keypress ..... 104
Channel switching when using a DH computer module ..... 105
Adjusting the operating mode of the RS232 interface ..... 106
Selecting the EDID mode of the KVM extender ..... 107
Reducing the colour depth of the image data to be transmitted ..... 108
Freeze mode ..... 109
Enabling or disabling DDC/CI support ..... 110
(De)Activating an USB keyboard or the »Generic USB« mode ..... 111
Prioritizing a USB device for a reboot ..... 113
Reinitialising USB input devices ..... 114
Adjusting the waiting period of the screensaver ..... 115
Automatic user logout ..... 115

Configuration settings (*continued*)

Selecting a keyboard layout for inputs via OSD ..... 116
Resetting the default settings ..... 117
Resetting the netfilter rules ..... 118
Changing the colour of the information display ..... 119
Information display ..... 120
Adjusting the transparency of the OSD ..... 120
Automatic closing of the OSD after inactivity ..... 121
Changing the position of the information dispaly ..... 121
Changing the position of the OSD ..... 122

**Further information** ..... **123**
DDC transmission with cache function ..... 123
Determining network settings via service port ..... 124
Installing the device driver ..... 124
Establishing a connection by using a terminal emulator ..... 124
Determining the IP address ..... 125
Pin assignment of the RS232 interface ..... 125

**Status LEDs** ..... **126**
LED on the front panel of the computer module ..... 126
LED on the front panel of the console module ..... 127
LEDs on the back panel ..... 128

**Used network ports and protocols** ..... **128**

**Technical data** ..... **129**
General features of the series ..... 129
Specific features of devices ..... 132
Features of transmission modules ..... 136

English

# Safety instructions

Please read through the following safety guidelines before putting the G&D product into operation. The guidelines help to avoid damage to the product and prevent potential injuries.

Keep these safety guidelines ready to hand for all persons who use this product.

Observe all warnings and operating information given at the device or in this operating manual.



### ⚠ Disconnect all power sources

**CAUTION:** Shock hazard!

Before installation, ensure that the device has been disconnected from all power sources. Disconnect all power plugs and all power supplies of the device.

### ⚠ Débranchez toutes les sources d'alimentation

**ATTENTION:** Risque de choc électrique!

Avant l'installation, assurez-vous que l'appareil a été débranché de toutes les sources d'alimentation. Débranchez toutes les fiches d'alimentation et toutes les alimentations électrique de l'appareil.

### ⚠ Trennen Sie alle Spannungsversorgungen

**VORSICHT:** Risiko elektrischer Schläge!

Stellen Sie vor der Installation sicher, dass das Gerät von allen Stromquellen getrennt ist. Ziehen Sie alle Netzstecker und alle Spannungsversorgungen am Gerät ab.

### ⚠ Warning: electric shock

To avoid the risk of electric shock, you should not open the device or remove any covers. If service is required, please contact our technicians.

### ⚠ Ensure constant access to the devices' mains plugs

When installing the devices, ensure that the devices' mains plugs remain accessible at all time.

### ⚠ Do not cover the ventilation openings

For device variants with ventilation openings, it must always be ensured that the ventilation openings are not covered.

### ⚠ Ensure proper installation position for devices with vents

For reasons of electrical safety, only upright, horizontal installation is permitted for devices with ventilation openings. Vertical installation is only permitted with suitable equipment carriers from G&D.

### ⚠ Do not insert any objects through the device's openings

Objects should never be inserted through the device's openings. Dangerous voltage could be present. Conductive foreign bodies can cause a short circuit, which can lead to fires, electric shocks or damage to your devices.

### ⚠ Avoid tripping hazards

Avoid tripping hazards while laying cables.

### ⚠ Use earthed voltage source

Only operate this device with an earthed voltage source.

### ⚠ Use exclusively the G&D power pack

Only operate this device with the power packs included in delivery or listed in this operating manual.

### ⚠ Do not make any mechanical or electrical alternations to the device

Do not make any mechanical or electrical alternations to this device. Guntermann & Drunck GmbH is not responsible for compliance with regulations in the case of a modified device.

### ⚠ Do not remove device cover

The cover may only be removed by a G&D service technician. Unauthorised removal voids the guarantee. Failure to observe this precautionary measure can result in injuries and damage to the device.

### ⚠ Operate the device exclusively in the intended field of application

The devices are designed for indoor use. Avoid extreme cold, heat or humidity.

## Instructions on how to handle Lithium button cells

- This product contains a lithium button cell. It is not intended to be replaced by the user!

**CAUTION:** Risk of explosion if the battery is replaced by an incorrect battery type.

Dispose of used batteries in an environmentally friendly manner. Do not dispose of batteries in municipal waste.

Check local regulations for the disposal of electronic products.

- Ce produit contient une batterie au lithium. Il n'est pas prévu que l'utilisateur remplace cette batterie.

**ATTENTION:** Il y a danger d'explosion s'il y a remplacement incorrect de la batterie.

Mettre au rebut les batteries usagées conformêment aux instructions du fabricant et de manière écologique. Les batteries usagées ne doivent pas être jetées dans les ordures ménagères.

Respectez les prescriptions valables pour l'élimination des produits électroniques.

- Dieses Produkt enthält eine Lithium-Knopfzelle. Ein Austausch durch den Anwender ist nicht vorgesehen!

**VORSICHT:** Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Batterie-Typ ersetzt wird.

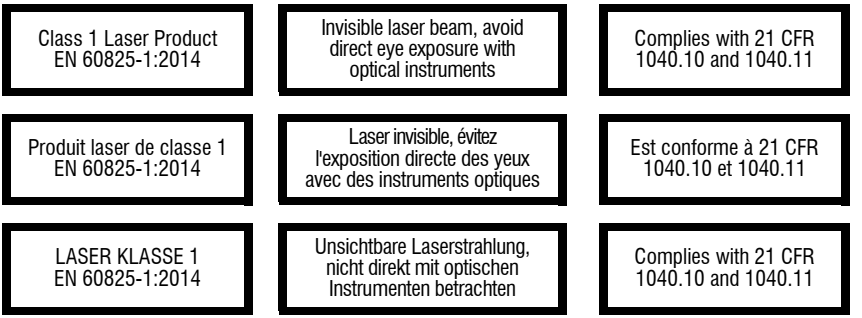
Entsorgen Sie gebrauchte Batterien umweltgerecht. Gebrauchte Batterien dürfen nicht in den Hausmüll geworfen werden.

Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

## Special advices for dealing with laser technology

The devices of the **VisionXS-IP-F-TypeC-UHR** series use components with laser technology which comply with laser class 1 or better.

They meet the requirements according to **EN 60825-1:2014** as well as **U.S. CFR 1040.10** and **1040.11**.




Mind the following advices when dealing with laser beams:

### ⚠ Avoid direct eye exposure to beam

Never stare directly into the beam when wearing optical instruments!

### ⚠ Always connect optical connections or cover them with protection caps

Always cover the optical connections of the *Transmission* socket and the cable plugs with a connector or a protection cap.

### ⚠ Only use G&D certified transmission modules

It is not permitted to use fibre optic modules, which do not meet the requirements of laser class 1 in accordance to **EN 60825-1:2014**. By using such modules, the compliance with regulations and advices for the safe handling of laser technology cannot be guaranteed.

The guarantee of complying with all relevant instructions can only be given by applying original components. Therefore, the devices have to be operated with G&D certified transmission modules only.

# The VisionXS-IP-F-TypeC-UHR series

**IMPORTANT:** Data transmission of devices of the **IP** series is *not* compatible to G&D devices of other series! The devices of the KVM-over-IP series are compatible with each other.



KVM extenders of the **VisionXS-IP-F-TypeC-UHR** series consist of a computer module and a console module.

Connect the computer to be operated to the computer module (**VisionXS-IP-CPU**). The remote console is connected to the console module (**VisionXS-IP-CON**).

Both the computer module and the console module are connected using two optical fibres.

**NOTE:** You can also use a cable to establish a *direct* connection between computer module and console module.

Signals of keyboard, mouse and video (DP1.2 alt mode) of the computer connected are transmitted using these fibres and enable you to operate the computer remotely.

## Use as extender or matrix switch modules

You can use the modules as either extender or matrix switch modules:

- **Extender modules:** Configure a KVM-over-IP connection between the computer and the console module. The configured connection between the modules is restored each time the modules are restarted.

**ADVICE:** Use the **IP-MUX** functionality (see page 55 ff.) to make up to 20 computers available in the OSD via separate computer modules.

- **Matrix switch modules:** In combination with the IP matrix switch **ControlCenter-IP** or **ControlCenter-IP-XS**, you can use the modules as end devices of the matrix switch.

In this case, configure a KVM-over-IP connection to the IP matrix switch for the modules.

In this configuration, the IP matrix switch enables the flexible connection of a console module to a computer module.

# Package contents

## Standard package contents computer modules

- 1 × computer module (**VisionXS-IP-CPU**), incl. transmission module/SFP transceiver
- 1 × TypeC connection cable (*TypeC-Cable-M/M-2*)
- 1 × USB device cable (*USB-AM/BM-2*)
- 1 × »Safety instructions« flyer
- 1 × »Correct power supply« flyer

## Additional package contents of expanded variants

The package contents of expanded variants of computer modules of the **VisionXS-IP-F-TypeC-UHR** series *additionally* contain the cables listed below.

| **DT VARIANTS** |
|---|
| 1 × power cable (PowerCable-2 Standard) |

| **A VARIANTS** |
|---|
| 1 × audio cable (Audio-M/M-2) |

| **AR VARIANTS** |
|---|
| 1 × audio cable (Audio-M/M-2) |
| 1 × serial connection cable (RS232-M/F-2) |

## Standard package contents console modules

- 1 × console module (**VisionXS-IP-CON**), incl. transmission module/SFP transceiver
- 1 × »Safety instructions« flyer
- 1 × »Correct power supply« flyer

## Additional package contents of expanded variants

The package contents of expanded variants of console modules of the **VisionXS-IP-F-TypeC-UHR** series *additionally* contain the cables listed below.

| **DT VARIANTS** |
|---|
| 1 × power cable (PowerCable-2 Standard) |

# Secure KVM-over-IP solution

## Potential security vulnerabilitites, threats and dangers

KVM solutions are the backbone of the IT infrastructure. Accordingly, it is crucial to protect the entire KVM installation. The security of KVM systems depends on two particular factors. First, the systems must be protected against attacks (from outside or inside). Second, the quality and reliability of the KVM products and KVM installations are important.



## Protection of KVM systems from external or internal attacks

Technical progress, the increased digitization of processes and the ever greater networking of IT systems are also creating new security vulnerabilities. On the one hand, work can be done more efficiently, but on the other hand, vulnerability to threats and attacks increases.

KVM matrix systems allow multiple workplaces to access multiple computers. This has great advantages: improved workflows, easier control and centralized administration. A first big and general security advantage of KVM solutions is the possibility of removing computers from work spaces and placing them in an access-protected equipment room. This makes it much more difficult for unauthorized persons to gain physical access to the computers.

## Security requirements with KVM-over-IP

Classic KVM systems use standard CAT-x copper cable or fiber optics to transmit signals. With such KVM systems, physical access is usually necessary to be able to manipulate anything, such as actively integrating additional unwanted devices.

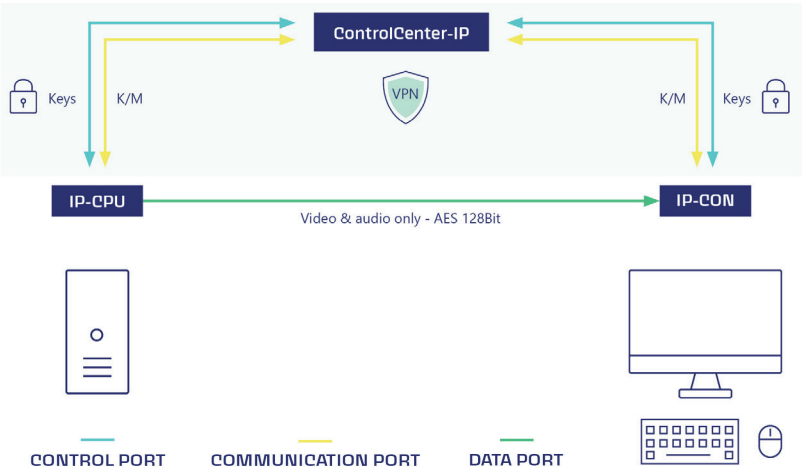
With KVM-over-IP systems, transmission is based on IP and runs on Gigabit Ethernet networks (OSI model layer 3). Using KVM-over-IP provides a future-proof solution due to its flexibility and easy expandability. However, IP transmission also increases security risks. There is an additional external risk, either via the internet or internally through easier network access.

Using appropriate software, it is possible to scan the entire internal network for security holes. In most cases, an attack is targeted at the weakest link in the chain. This can include, for example, man-in-the-middle attacks, where the entire network traffic is passed on to third parties. Therefore, separating and segmenting networks are important tools to protect an application from cyber attacks.

In KVM-over-IP systems, keyboard and mouse inputs as well as video, audio, USB and RS232 data must be encrypted to prevent unauthorized users from tapping data transmissions and thus gaining access to internal information, such as logins and passwords. Regularly exchanging the security keys is mandatory. The use of VPN, VLANs and secure encryption is also required to prevent unwanted access.

## The secure solution from G&D

G&D uses different ports for data transmission in the IP network. A VPN tunnel connects each end device (IP-CPU/IP-CON) to the respective counterpart or to the KVM-over-IP matrix Control-Center-IP or ControlCenter-IP-XS. An AES256 Galois/Counter Mode (GCM) encrypted IPSec VPN tunnel is used (GCM is based on Counter Mode CTR, but also offers integrated integrity protection). There is also downward compatibility for AES128-GCM.




The first port that is established from all KVM-over-IP end devices to the respective counterpart or to the matrix is the so-called control port. The communication between the end devices or with the matrix is negotiated through a self-developed authentication plug-in. This ensures that only G&D devices can establish a connection based on their UID, serial number and the Trusted Platform Module. The control port is also used to exchange the respective security keys the KVM-over-IP matrix generates within matrix operation or the computer module generates within extender operation for each end device.

The keyboard and mouse data are transmitted bidirectionally via the second port, the so-called communication port.

The key exchange for the highly security-relevant keyboard and mouse data as well as the control data is fully dynamic and occurs every 40 to 80 minutes.

Video data is transmitted directly from the computer module to the console module via UDP and MultiCast/UniCast (data port). For audio, GenericUSB and RS232 data as well as the video stream, which is converted to G&D's own proprietary protocol before being sent, AES128 Counter Mode (CTR) is used. A secret device key, which is required to unpack the video data, provides additional protection.

The proprietary protocol for dedicated connections is supplemented by fully dynamic encryption for KVM-over-IP. The key exchange for this high-speed data takes place every three to five hours or in the case of switching events. Each time a console module connects to a computer module, a security key is generated for that connection. Whenever another console module connects to this computer module within matrix operation, both console modules receive new security keys. In reverse, a new security key is also sent to the remaining console module when the other module is disconnected.

By separating control data (control port) and keyboard and mouse data (communication port) from video, audio, GenericUSB and RS232 data (data port), diverse attack scenarios, such as man-in-the-middle attacks, are prevented from the outset. If the target IP address or VPN tunnel is compromised, no new security keys are issued and the KVM end devices as well as the matrix system switch to security mode and stop the transmission of data.

## Trusted Computing Platform

The bootloader, the operating system and the firmware of the devices form a Trusted Computing Platform. Based on a core component complying with the FIPS140-2 security standard, an integrated Trusted Platform module secures all access and configuration data against third-party spying or manipulation. Here, an RSA encryption method with a key length of 2048 bits is used.

Sensitive data such as login information and passwords are stored permanently and encrypted in the database of the ControlCenter-IP or ControlCenter-IP-XS within matrix operation or in the database of the computer module within extender operation. This database is implemented in G&D's operating system, is TPM-protected and with the ControlCenter-IP additionally based on a hardware raid. Possible firmware modifications can be detected at an early stage, leading to an interruption of the boot process. Thus, any attempts at manipulation, such as smuggling in a keyboard sniffer, are prevented.

TPM ensures that a device is only booted with software that has been classified as trustworthy by the manufacturer.

## Monitoring, SNMP and Syslog

Monitoring and SNMP features enable system administrators to monitor the status of devices installed and peripherals connected. Any information is provided via the web interface of the respective devices. Permanent detection and reporting makes it possible to react at an early stage to critical conditions such as exceeding temperatures, loss of communication on the keyboard interface, or a compromised redundancy system. This preemptively prevents system failures, increases the system's availability and allows operators and system administrators to work more efficiently.

Syslog (System Logging Protocol) is used to generate various events in response to changing conditions. The events are logged locally and can be checked and analyzed by an administrator. The syslog messages can also be sent to a syslog server. Syslog can be used, for example, to log relevant system changes, logins and login failures.

## Update and Backup/Restore

Configuration settings can be saved using the backup function. With the auto backup function an automatic backup can be saved on a network drive at a defined interval. This means there ist no need to make a manual backup after a configuration option has been changed. Backed-up data can be restored using the restore function.

## Further security-relevant aspects

All G&D computer modules (CPUs) can be configured to automatically log off the computer‘s operating system when a user logs off the console module. This prevents unintentional open access to the computer and the possibility of another user accessing the computer without logging in.

The use of optional UID locking reliably restricts the end devices that can be used. Once activated, no further end devices can be added or replaced.

Optional USB 2.0 data connections can also be disabled via intelligent user management at hardware level.

Another important aspect is the security of the device on the user side. G&D KVM end devices do not store any information. It is therefore not possible to read out a stolen device to obtain cached login data.

The system wide password complexity (minimum password length, mimimum number of capitals/lowercases, minimum number of digits, minimum number of special characters, minimum number of characters that must be different compared with the previous password) can be configured to comply with individual password guidelines and to improve security.

To enhance security, further configuration options are available in the login options area. It is possible to specify how many failed attempts are accepted when entering a password and how long a user is locked out after exceeding the maximum number of failed attempts. In this area, it can also be determined how many simultaneous superuser sessions are permitted.

In addition, terms of use can be stored that a user must accept before each (new) device access.

## 2-factor authentication (2FA)

To provide a greater level of security, a second possession-based factor can be requested through the 2-factor authentication (2FA) option.

2FA makes use of a time-based one-time password (TOTP). Authenticator apps or hardware tokens can be used.

# Optional additional security-relevant functions

## SecureCert

The SecureCert feature can be used to activate certified security functions for the product groups ControlCenter-IP, ControlCenter-IP-XS, VisionXS-IP, VisionXS-IP 2.0, Vision-IP and RemoteAccess-IP-CPU. This functions are provided as part of the FIPS 140-3, DoDIN APL and CC EAL2+ certifications. Devices equipped with the feature meet the requirements of the mentioned standards and have been tested and certified in accordance with the relevant processes.

**IMPORTANT:** The SecureCert feature can only be ordered together with a device. After sales activation is **not** possible.

**ADVICE:** Additional functions are available for matrix operation. For detailed information, please refer to the manual of the matrix switch.

# Signal transmission and transmission length

G&D's **KVM-over-IP™** technology (see *The secure solution from G&D* on page 8) makes it possible to transmit signals between the computer and the console module compressed and encrypted using Gigabit Ethernet (Layer 3). Alternatively, the computer module and the console module can also be connected directly to each other. In this case, the transmission length is limited (see section *Features of transmission modules* in the chapter *Technical data*).

If the bandwidth of the Gigabit Ethernet is sufficient, the video signal is reproduced in a loss-free video quality and almost without any latency. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements (see *Limiting the bandwidth* on page 51).

When observing the max. length of sections between two *active* network components (see section *Features of transmission modules* in the chapter *Technical data*), the entire transmission length is unrestricted.

# Selecting a network switch

**NOTE:** No *multicast* transmission is provided within extender operation. This places significantly fewer requirements on the network switch than is the case within matrix operation.

**IMPORTANT:** If possible, the network switches should also meet the requirements for matrix operation (*Multicast*, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* and *Spanning Tree TCN Flooding*) with regard to system expansion. Further information on this can be found in the installation manual of the matrix switch.

## Requirements of network switches

The following requirements apply to the network:

- At least **Layer 2 managed switch**
- **VLAN support** to separate KVM-over-IP™ traffic from other network operations.

- **QoS with DiffServ/DSCP** support for performance enhancement and prioritization:
  Quality of Service (QoS) is a packet prioritization mechanism that ensures time-critical or important applications receive their data preferentially over the network.
  With DiffServ / DSCP support, data packets are marked and processed by the network according to the configuration. DSCP specifies how exactly a packet is handled.

> **NOTE:** Take into consideration that some network switches automatically assign the service class **Network Control** (DSCP name: **CS6**) for *all* data packets. In such environments, the **DSCP 48** option must not be selected!

- **Ensure adequate performance** of the network switch: check forwarding bandwidth, switching capacity, and forwarding performance.

> **EXAMPLE:** Typical bandwidth requirements for KVM-over-IP
>
> VisionXS-IP models are available in several variants: DVI-I, DP-HR and DP-HR-DH with 1 Gbit; DP-UHR and TypeC-UHR with multi-Gbit (1-10 Gbit). The bandwidth is unlimited by default but can optionally be restricted.
>
> - 1920 × 1080 = 300-400 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DVI-I)
> - 2560 × 1440 = 500-600 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-HR)
> - 2 × 2560 × 1440 = 800-900 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-HR-DH)
> - 3840 × 2160 = 2000-2500 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-UHR)
>   the maximum video bandwidth usage is 5 Gbit/s
> - Static image: 25 Mbit/s at 3840 × 2160

> **IMPORTANT:** Make sure that the uplink from access switch to core/main switch is sufficiently dimensioned for the number and operating mode of the connected end devices.

> **EXAMPLE:**
>
> - 30 × *VisionXS-IP-DP-HR-CPU* at 10Gbit uplink
> - uplink with 10 Gbit/s is a bottleneck, since 30 × 1Gbit/s would have to be ensured with the CPUs.

# Installation

**IMPORTANT:** The devices use components with laser technology which comply with laser class 1.

They meet the requirements in accordance to **EN 60825-1:2014** as well as **U.S. CFR 1040.10** and **1040.11**.

Consider the following safety guidelines regarding this matter:

- *Avoid direct eye exposure to beam* on page 4
- *Always connect optical connections or cover them with protection caps* on page 4



## Preparation

**IMPORTANT:** When choosing a location for the devices, please ensure to comply with the ambient temperature limit (see (see *Technical data* on page 129 ff.)) close to the device. The ambient temperature limit must not be influenced by other devices.

Ensure sufficient air circulation.

**IMPORTANT:** Do not cover the ventilation openings. For reasons of electric safety, only upright, horizontal installation is permitted for devices with ventilation openings. Vertical installation is only permitted with suitable device carriers from G&D.

Please refrain from using devices with ventilation openings in dusty environments. Dust in the housing can damage the electronics and may cause failures.

1. Ensure that the computer to be connected to the computer module is switched off. If the computer is provided with keyboard and mouse, unplug the cables of the input devices from the interfaces.
2. Place the computer module (**VisionXS-IP-CPU**) close to the computer.

   **NOTE:** Please mind the maximum cable length of *two* meters between the computer module and the computer to be connected.

3. Place the compatible console module close to the remote console.

   **NOTE:** Please mind the maximum cable length of *two* meters between the console module and the devices of the remote console.

4. Take the supplied cables and have them ready for the installation of the devices.

# Installing the computer module

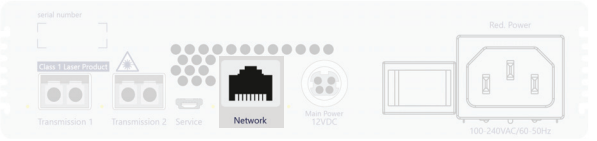
**NOTE:** All device variants of the **VisionXS-IP** series can be operated with an *external* power supply at the **Power** interface (for DT variants: **Main Power**).

The products support USB Power Delivery. They can only be used as a power receiver (sink, *Establishing the power supply* on page 20).

The illustrations in this chapter show the DT variant of the device series. This variant is additionally equipped with an *internal* power supply (**Red. Power**).

The computer, whose signals are transmitted to the remote console, is connected to the **VisionXS-IP-CPU** computer module.

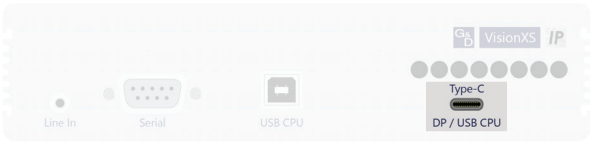
## Establishing a connection to a local management network




**NOTE:** If desired, connect this network interface to a local network. This enables you to access the **Config Panel** web application from this network and to send syslog messages to this network.

**Network:** Insert a category 5 twisted pair cable (or better), which is available as accessory. Connect the other end of the cable to the local network.

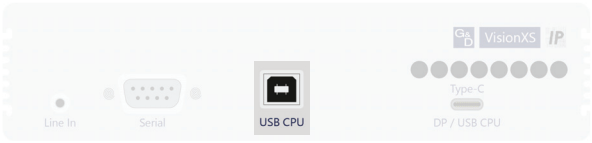
## Connecting the computer's keyboard and mouse signals




**Type-C DP/USB CPU:** Use the *TypeC-Cable-M/M-2* cable to connect one of the computer's USB interfaces to this interface.

> **NOTE:** The **Type-C DP/USB CPU** interface is primarily used to feed in video data. However, it also processes USB data. Thus, no separate USB connection has to be plugged in.

> **IMPORTANT:** If a separate USB connection is plugged in via the **USB CPU** interface, this is used with priority.




**USB CPU:** Use the *USB-AM/BM-2* cable to connect one of the computer's USB interfaces to this interface.

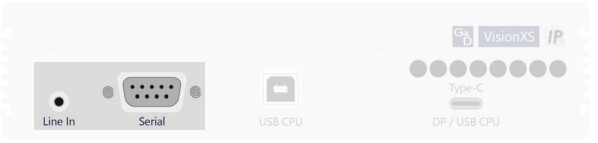
English

## Connecting the computer's video output




**Type-C/DP/USB CPU:** Use the TypeC-*Cable-M/M-2* cable to connect one of the computer's USB interfaces to this interface.

## Connecting audio and RS232 interfaces (depending on model)




**NOTE:** By default, the KVM extender transfers audio data. The transmission of RS232 data is deactivated.

You can enable the transmission of RS232 data and/or disable the transmission of audio data (see *(De)Activating signals* on page 53).

**Line In:** Use an *Audio-M/M-2* audio connection cable to connect the omputer's *Line-Out* interface to this interface

**Serial:** Use the *RS232-M/F-2* cable to connect one of the computer's 9-pin serial interfaces to this interface.

## Establishing a connection to the Gigabit Ethernet




**IMPORTANT:** The devices use components with laser technology which comply with laser class 1.

Never stare directly into the beam when wearing optical instruments!

**NOTE:** Remove the protection caps from the *Transmission* interfaces and from the cable plug.

**Transmission 1|Tx:** Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

**Transmission 1|Rx:** Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

**NOTE:** The activation of the **Transm. Redundancy** feature activates the **Transmission 2** interface.

To use the **Transmission 2** interface, you need an additional SFP transceiver. Choose the right **SFP transceiver** for your variant of the **VisionXS-IP-F-TypeC-UHR** series. The **Transm. Redundancy options** contain both, a corresponding **SFP transceiver** and the **Transm. Redundancy feature**.

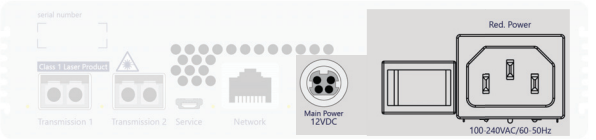
Use this interface to establish a redundant *transmission* connection (*link aggregation*) with the Gigabit network.

## Establishing the power supply

**NOTE:** All device variants of the **VisionXS-IP** series can be operated with an *external* power supply at the **Power** interface (for DT variants: **Main Power**).

The illustrations in this chapter show the DT variant of the device series. This variant is additionally equipped with an *internal* power supply (**Red. Power**).

**IMPORTANT:** Due to their hardware design, the DT variants preferentially draw power from the *external* power supply (**Main Power**). Should the *external* power supply fail or become temporarily unavailable, for example during replacement, the device will automatically be supplied with the required power by the *internal* power supply (**Red. Power**).




**Power/Main Power:** Connect an external power supply to this interface.

**Red Power:** .To provide a second, redundant power supply, insert an IEC cables here.

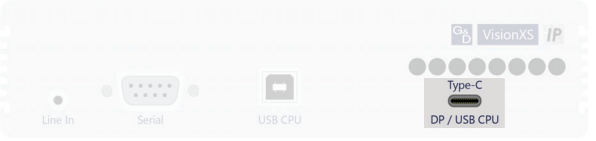
**IMPORTANT:** All G&D devices have information printed on them regarding their power consumption. Please ensure that the power pack you are using provides at least the required amount of power.

Our support will gladly assist you in ensuring that your device is supplied with power correctly.

If the device is not supplied with adequate power, it may not operate as expected and its function may be permanently impaired!

**NOTE:** The product supports USB Power Delivery. The product can only be used as a power receiver (sink).

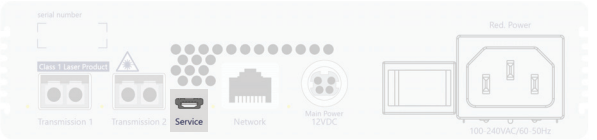
**IMPORTANT:** The sole power supply via USB Power Delivery is **not** sufficient to execute updates.



**Type-C DP/USB CPU:** Use the TypeC-*Cable-M/M-2* cable to connect one of the computer's USB interfaces to this interface.

## Service interface

The device has a service interface on the back panel. This interface has no relevant function for the user in normal operation.




Debug, error and status messages can be displayed in a terminal emulator (e.g. *HyperTerminal* or *PuTTY*). Via a service menu, technicians have the ability to retrieve information about the device, temporarily disable the network filter rules, reset the device to factory settings, or perform a restart.

The service menu can be operated via any terminal emulator. Use a service cable to connect the computer on which the terminal emulator is installed with the *Service* port of the device.

**How to establish a connection within the terminal emulator:**

**NOTE:** Before establishing a connection using the terminal emulator, install the device driver *CP210x USB to UART Bridge VCP*.

This driver provides the *Service* port of the **VisionXS-IP** system, which is connected via service cable, as virtual serial interface (COM port). Now, the virtual interface can be selected in the terminal emulator to establish the connection.

The driver is provided as download on the website **www.gdsys.com/en** under **Service > Downloads > Tools & drivers**.

1. Start any terminal emulator (e.g. *HyperTerminal* or *PuTTY*).

2. Establish a new connection in the terminal emulator and enter the following settings:
   - Bits per second: 460.800
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none
3. Use a data cable to connect the computer to the *Service* port at the back panel of the **VisionXS-IP**.

> **NOTE:** To log in into the service menu, enter the user name *service* and the password *service*. The service menü is freely accessible on devices with *SecureCert feature* activated.

4. In the service menu, you have the following options:
   - Quit (**not** visible on devices with *SecureCert feature* activated)
   - System information
   - Set system defaults: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Reboot: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Temporary deactivation of the network filter rules: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.

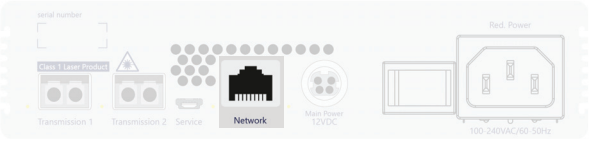
# Installing console modules

**NOTE:** All device variants of the **VisionXS-IP** series can be operated with an *external* power supply at the **Power** interface (for DT variants: **Main Power**).

The illustrations in this chapter show the DT variant of the device series. This variant is additionally equipped with an *internal* power supply (**Red. Power**).

The remote console is connected to the **VisionXS-IP-CON** console module. The computer connected to the computer module can be operated from this console.

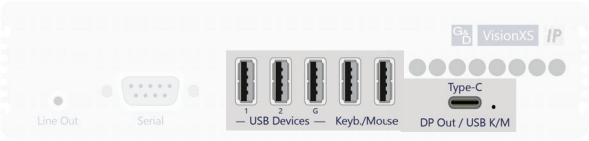
## Establishing a connection to a local management network




**NOTE:** If desired, connect this network interface to a local network. This enables you to access the **Config Panel** web application from this network and to send syslog messages to this network.

**Network:** Insert a category 5 twisted pair cable (or better), which is available as accessory. Connect the other end of the cable to the local network.

## Connecting keyboard and mouse of consoles and other devices




**Keyb./Mouse:** Connect the mouse and/or the keyboard of the console to this interface.

**USB Devices:** In the default settings, you can connect additional USB input devices,USB mass storage devices, and/or a supported display or tablet to this interfaces.

Activate the **generic USB** mode (see *(De)Activating an USB keyboard or the »Generic USB« mode* on page 111) if you want to connect another USB input device or USB mass storage device. In this mode, any data of the USB device is *not altered* when transmitted to the computer module.

**IMPORTANT:** If the **generic USB** mode is active, the OSD cannot be operated by a keyboard connected to the **USB Devices** sockets.

**IMPORTANT:** This product allows simultaneous use of up to five GenericUSB devices via a console module. For this, both the used console module and the used computer module must support the use of up to five GenericUSB devices.

Only up to three HighSpeed devices (e.g. USB flash drive) and two FullSpeed devices can be used. If additional HighSpeed devices are connected, they will not be accepted.

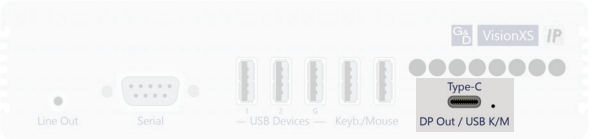
**NOTE:** There are *three* **Generic** interfaces on the console module. You need a USB hub or a USB composite device to connect *four* or *five* generic USB devices.

The two **Keyb./Mouse** interfaces *cannot* be used for **generic USB** mode.

**NOTE:** The USB Type-C interface, which is primarily used to output video data, also offers the option of accepting USB K/M data. This means that a USB keyboard and USB mouse can be connected to a USB hub on a monitor.

**Type-C/DP Out/USB K/M:** Connect the console monitor

## Connecting the console monitor




**Type-C/DP Out/USB K/M:** Connect the console monitor

## Connecting audio and RS232 interfaces (depending on model)

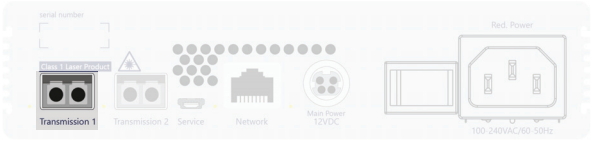



## Line Out

Connect the speakers or another audio output device.

**Serial:** Connect the serial end device to this interface.

## Establishing a connection to the Gigabit Ethernet




**IMPORTANT:** The device uses components with laser technology which comply with laser class 1.

Never stare directly into the beam when wearing optical instruments!

**NOTE:** Remove the protection caps from the *Transmission* interfaces and the cable plugs.

**Transmission 1|Tx:** Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

**Transmission 1|Rx:** Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

**NOTE:** The activation of the **Transm. Redundancy** feature activates the **Transmission 2** interface.

To use the **Transmission 2** interface, you need an additional SFP transceiver. Choose the right **SFP transceiver** for your variant of the **VisionXS-IP-F-TypeC-UHR** series. The **Transm. Redundancy options** contain both, a corresponding **SFP transceiver** and the **Transm. Redundancy feature**.

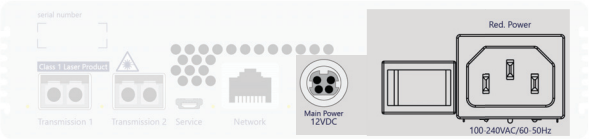
Use this interface to establish a redundant *transmission* connection (*link aggregation*) with the Gigabit network.

## Establishing the power supply

**NOTE:** All device variants of the **VisionXS-IP** series can be operated with an *external* power supply at the **Power** interface (for DT variants: **Main Power**).

The illustrations in this chapter show the DT variant of the device series. This variant is additionally equipped with an *internal* power supply (**Red. Power**).

**IMPORTANT:** Due to their hardware design, the DT variants preferentially draw power from the *external* power supply (**Main Power**). Should the *external* power supply fail or become temporarily unavailable, for example during replacement, the device will automatically be supplied with the required power by the *internal* power supply (**Red. Power**).




**Power/Main Power:** Connect an external power supply to this interface.

**Red Power:** .To provide a second, redundant power supply, insert an IEC cables here.

**IMPORTANT:** All G&D devices have information printed on them regarding their power consumption. Please ensure that the power pack you are using provides at least the required amount of power.

Our support will gladly assist you in ensuring that your device is supplied with power correctly.

If the device is not supplied with adequate power, it may not operate as expected and its function may be permanently impaired!

**NOTE:** The product supports USB Power Delivery. The product can only be used as a power receiver (sink).

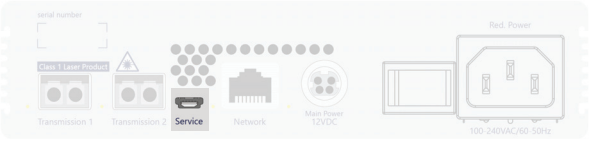
**IMPORTANT:** The sole power supply via USB Power Delivery is **not** sufficient to execute updates.




**Type-C/DP Out/USB K/M:** Connect the console monitor

## Service interface

The device has a service interface on the back panel. This interface has no relevant function for the user in normal operation.




Debug, error and status messages can be displayed in a terminal emulator (e.g. *HyperTerminal* or *PuTTY*). Via a service menu, technicians have the ability to retrieve information about the device, temporarily disable the network filter rules, reset the device to factory settings, or perform a restart.

The service menu can be operated via any terminal emulator. Use a service cable to connect the computer on which the terminal emulator is installed with the *Service* port of the device.

**How to establish a connection within the terminal emulator:**

**NOTE:** Before establishing a connection using the terminal emulator, install the device driver *CP210x USB to UART Bridge VCP*.

This driver provides the *Service* port of the **VisionXS-IP** system, which is connected via service cable, as virtual serial interface (COM port). Now, the virtual interface can be selected in the terminal emulator to establish the connection.

The driver is provided as download on the website **www.gdsys.com/en** under **Service > Downloads > Tools & drivers**.

1. Start any terminal emulator (e.g. *HyperTerminal* or *PuTTY*).

2. Establish a new connection in the terminal emulator and enter the following settings:
   - Bits per second: 460.800
   - Data bits: 8
   - Parity: none
   - Stop bits: 1
   - Flow control: none
3. Use a data cable to connect the computer to the *Service* port at the back panel of the **VisionXS-IP**.

**NOTE:** To log in into the service menu, enter the user name *service* and the password *service*. The service menü is freely accessible on devices with *SecureCert feature* activated.

4. In the service menu, you have the following options:
   - Quit (**not** visible on devices with *SecureCert feature* activated)
   - System information
   - Set system defaults: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Reboot: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Temporary deactivation of the network filter rules: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.

# Start-up

After the proper installation of the KVM extenders they can be immediately put into operation.

**IMPORTANT:** Due to their hardware design, the DT variants preferentially draw power from the *external* power supply (**Main Power**). Should the *external* power supply fail or become temporarily unavailable, for example during replacement, the device will automatically be supplied with the required power by the *internal* power supply (**Red. Power**).



## Power-up

Mind the following sequence when starting the modules:

1. Connect the *external* power supply to the **console module** *and/or* switch on the *internal* power supply (DT variants only).
2. Connect the *external* power supply to the **computer module** *and/or* switch on the *internal* power supply (DT variants only).
3. Turn on the **computer** that is connected to the computer module.

**NOTE:** The recommended activation sequence ensures that the KVM extenders are able to read out the features of the connected monitor and to transmit them to the computer (see *DDC transmission with cache function* on page 123).

## Starting process

After the Start-up, the LEDs show the module's operating status.

For further information about this topic, also see the chapter *Status LEDs* on page 126 ff.

## Power-down

Mind the following sequence when power-down the modules:

1. Disconnect the *external* power supply of the **computer module** *and/or* switch off the *internal* power supply (DT variant only).
2. Disconnect the *external* power supply of the **console module** *and/or* switch off the *internal* power supply (DT variant only).

## Operation

**IMPORTANT:** The OpenAccess operating mode is set by *default*. In this operating mode, access to the KVM extender is *not* protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

You can operate the computer connected to the computer module at the remote console of the console module.

**NOTE:** The connection between the computer module and the console module is established automatically after the modules are started.

**IMPORTANT:** The Standard operating mode is set by *default* for devices with *SecureCert feature* activated. In this operating mode, access to the KVM extender is protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

## User login at the console module

**IMPORTANT:** Before logging in at the console module, please ensure that the correct **keyboard layout** is selected. By *default*, the German keyboard layout is set. If you require a different layout, it must be manually adjusted before login to ensure that your input – especially passwords – is correctly recognized (see *Selecting a keyboard layout for inputs via OSD* on page 116).

Alternatively, the keyboard layout can also be changed via the ConfigPanel web application. Further information on this can be found in the separate manual for the web application.

**NOTE:** If the *standard* operating mode was set instead of the OpenAccess operating mode (*default* for extender operation, except for devices with *SecureCert feature* activated), the system asks you to log in, after the console module has been switched on.

**How to log in at the system:**

1. Enter the following data to the login box:

| | |
|---|---|
| **Terms (of use):** | Press **Enter** to display the terms of use. |
| **Accept (of terms of use):** | Press **F8** to accept the terms of use. |
| **Username:** | Enter your username. |
| **Password:** | Enter your user account password. |
| **2-Factor Auth Code (TOTP):** | Enter the 2-Factor Auth Code (TOTP) from two-factor authentication. |

2. Press **Enter** to log in and start the on-screen display.

**IMPORTANT:** The *Terms* field and the *Accept* field only appear if Showing terms of use is activated (see *Showing terms of use* on page 38).

**IMPORTANT:** The *2-Factor Auth Code (TOTP)* field only appears if 2-factor authentication is enabled. For detailed information, please refer to the separate manual of the web application.

## Configuring the password complexity

You can configure password complexity to comply with your individual password guidelines and improve security.

**IMPORTANT:** Changes in the section of password complexity have **no** effect on existing passwords, but are only taken into account when a password is changed (see *Changing the password of a user account* on page 84) and a new user account is created (see *Creating a new user account* on page 82). You should therefore configure the password complexity as early as possible.

**IMPORTANT:** Changes in the section of password complexity have **no** effect on user authentication with external directory services. The directory services have their own configuration options.

**How to configure the minimum password length:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the on-screen display (OSD).
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. length** line and press **Enter**.
5. Enter the desired minimum password lenght (*Default*: 3 or 15 with activated *SecureCert-Feature*)
6. Press **F2** to save your settings.

**How to configure the minimum number of capital letters within a password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. capital letters** line and press **Enter**.
5. Enter the desired minimum number of capital letters within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
6. Press **F2** to save your settings.

**How to configure the minimum number of lowercases within a password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. lowercase** line and press **Enter**.
5. Enter the desired minimum number of lowercases within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
6. Press **F2** to save your settings.

**How to configure the minimum number of digits within a password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. digits** line and press **Enter**.
5. Enter the desired minimum number of digits within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
6. Press **F2** to save your settings.

**How to configure the minimum number of special characters within a password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. special characters** line and press **Enter**.
5. Enter the desired minimum number of special characters within a password (*Default*: 0 or 1 with activated *SecureCert-Feature*)
6. Press **F2** to save your settings.

**How to configure the minimum number of characters that must be different compared with the previous password when changing the password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Password Complexity** line and press **Enter**.
4. Select the **Min. different** line and press **Enter**.
5. Enter the desired minimum number of characters that must be differnt compared with the previous password (*Default*: 0 or 8 with activated *SecureCert-Feature*)

> **NOTE:** The minimum number of different characters compared with the previous password must not be higher than the minimum password length.

6. Press **F2** to save your settings.

## Configuring the login options

To improve security, further configuration options are available in the login options area.

You can specify how many failed attempts are accepted when entering a password and how long a user is locked out after exceeding the maximum number of failed attempts.

In this area, you can also specify how many simultaneous superuser sessions are permitted.

**How to set the maximum number of failed password entry attempts:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Login options** line and press **Enter**.
4. Select the **Max. failed attempts** line and press **Enter**.
5. Enter the desired maximum number of failed attempts when entering the password (*Default*: 0 = off/unlimited number of failed attempts or 3 with activated *SecureCert-Feature*, max. 1,000)
6. Press **F2** to save your settings.

**How to set the locking time if the maximum number of failed password entry attempts is exceeded:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Login options** line and press **Enter**.
4. Select the **Locking time** line and press **Enter**.
5. Enter the desired locking time in minutes for which a user is locked after exceeding the maximum number of failed password entry attempts (*Default*: 1 (if max. failed attempts > 0) or 15 with activated *SecureCert-Feature*, max. 1,440 minutes)
6. Press **F2** to save your settings.

**How to set the maximum number of simultaneous superuser sessions:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Login options** line and press **Enter**.
4. Select the **Max. supueruser sessions** line and press **Enter**.
5. Enter the desired number of maximum simultaneous superuser sessions (*Default*: 0 = off/unlimited number of superuser sessions, max. 1,024)

> **NOTE:** The maximum number of simultaneous supueruser sessions is effectiv per interface (device/OSD and ConfigPanel).

6. Press **F2** to save your settings.

## Showing terms of use

If the terms of use are displayed, they must be accepted before each (new) device access.

**How to configure the display of terms of use:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **System setup** entry and press **Enter**.
3. Select the **Terms Of Use Config** line and press **Enter**.
4. Select the **Terms of use** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **off:** | *No* terms of use are displayed during log in (*default*). |
| **User:** | *Individual* terms of use are displayed during log in. |
| **DoD Notice:** | The terms of use of the *US Department of Defense* are used during log in (can only be selected if the optional *SecureCert feature* is activated). |

5. If you selected *User* in the previous step, the individual terms of use must be entered in the next step. Select the **Short text...** entry and press **Enter**.
6. Now enter the text that a user is shown before accepting the terms of use (**example**: *I have read the terms of use and hereby agree to them*). This text field is limited to 70 characters.
7. Press **F2** to save the text.
8. Press **Esc** to return to the previous screen.
9. Select the **Long text...** entry and press **Enter**.
10. Now enter the desired terms of use. This field is limited to 1,500 characters.
11. Press **F2** to save the text.
12. Press **Esc** and then **F2** to save your settings.

## User logout at the console module

Use the *User logout* function to log out of the system. If the *standard* operating mode was set and the logout was successful, the *Login* window opens.

**IMPORTANT:** Always use the *User logout* function of the system to protect the console module and system against unauthorised access.



**How to log out of the system:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the on-screen display.
2. Press **F9** to open the *Operation* menu.
3. Press **E** or select the **E - User logout** entry and press **Enter**.

**ADVICE:** After the on-screen display has been called up, you can use the *User logout* function by pressing **Ctrl+E**.

# Establishing a KVM-over-IP™ connection for the first time

**IMPORTANT:** If you use the KVM extender as a matrix module with the IP matrix switch **ControlCenter IP** or **ControlCenter-IP-XS**, you can conveniently set up the **KVM-over-IP™ connection** via the web application of the IP matrix switch (see instructions for the *web application of the IP matrix switch*).

Manual configuration as described in this chapter is *not* necessary in this case.

G&D's **KVM-over-IP™** technology makes it possible to transmit signals between the computer and the console module using a Gigabit Ethernet (layer 3).

The communication between two modules requires various settings. In the default settings, the modules are configured in a way that a computer and a console module can immediately establish a direct connection.

All computer modules are preconfigured with the IP address **172.17.0.10,** all console modules with the IP address **172.17.0.11**.

**IMPORTANT:** Change the default IP addresses before integrating several computer or console modules into the productive network.

**ADVICE:** If you do not know the IP address of an already configured console or computer module, it can be determined via the log messages of the device. For more information, see the section *Determining network settings via service port* on page 124.

## Default setting of the modules

The default setting of the modules allows users to quickly establish a direct connection between a computer and a console module. The OSD lets you adjust the configuration of both modules after their initial operation.

Both the IP addresses and the **KVM-over-IP** settings are preconfigured as follows:

| DEFAULT SETTING OF THE COMPUTER MODULE (CPU) | |
|---|---|
| **IP address:** | 172.17.0.10 |
| **Netmask** | 255.255.0.0 |
| **Control port:** | 18246 |
| **Communication port:** | 18245 |
| **Data port:** | 18244 |

| DEFAULT SETTING OF THE CONSOLE MODULE (CON) | |
|---|---|
| **IP address:** | 172.17.0.11 |
| **Netmask** | 255.255.0.0 |
| **Local control port:** | 18246 |
| **Local communication port:** | 18245 |
| **Local data port:** | 18244 |
| **Remote host:** | 172.17.0.10 |
| **Remote control port:** | 18246 |

**NOTE:** The **IP address** of the computer module (host) as well as the **control port** of the computer module must be specified to establish a **KVM-over-IP** connection through the console module.

The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

**IMPORTANT:** Configuration of **IPv6** should only be performed **by technically experienced users**. While IPv6 offers advanced features and a larger address space, it also introduces **more complex requirements regarding network structure, security, and compatibility**. Incorrect settings may lead to **connectivity issues or unexpected network behavior**. If you are **not familiar** with the IP addressing and network topology specific to IPv6, we recommend that you thoroughly **inform yourself about the implications** before enabling IPv6, or consult with your network administration.

## Configuring a KVM-over-IP connection of a computer module

You can carry out the required configuration settings directly on the console.

**NOTE:** Use the **local hotkey** (default: **Alt**+**Num**) to open the local OSD to configure the network interface of the console module, or use the **remote hotkey** (default: **Ctrl**+**Num**) to open the remote OSD to configure the network interface of the computer module.

The settings of both hotkeys are shown during the starting process of the console module (see *Starting process* on page 31).

**IMPORTANT:** The OSD of the computer module can be opened only if a **KVM-over-IP** connection to the computer module is established.

Therefore, you have to change the configuration of the computer module *first*.

## Configuring the network interface

**How to configure the network interface:**

1. Use the remote hotkey **Ctrl+Num** to open the OSD.
2. Select the entry **Network setup** and press **Enter**.
3. Select the entry **Interfaces** and press **Enter**.
4. Enter the following data under **Transmission**:

> **NOTE:** Each network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

| | |
|---|---|
| **Operational mode:** | Press **F8** to select the operational mode of the interface:<br>▪ **Off:** switches off network interface.<br>▪ **Static IPv4:** A static IPv4 address is assigned.<br>▪ **DHCPv4:** oObtain IPv4 address from a DHCP server. |
| **IP address:** | Enter the IPv4 address of the interface.<br>*This setting is auto obtained in the DHCPv4 operating mode.* |
| **Netmask:** | Enter the network netmask.<br>*This setting is auto obtained in the DHCP operating mode.* |
| **IPv6:** | Press **F8** to enable IPv6 (**enabled**). By default, IPv6 is **disabled**.<br>**NOTE:** When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user. |
| **Static IPv6 address:** | Enter the static IPv6 address of the interface. |
| **Prefix:** | Specify the prefix length (*default*: 64) for the interface according to the notation rules defined in RFC 5952. |

5. Press **F2** to save your settings.

## Configuring the global network settings

Even in complex networks global network settings ensure that the KVM extender is available from all partial networks.

**How to configure global network settings:**

1. Use the remote hotkey **Ctrl+Num** to open the OSD of computer module.
2. Select the entry **Network setup** and press **Enter**.
3. Select the entry **Interfaces** and press **Enter**.
4. Enter the following data under **Main Network**:

| | |
|---|---|
| **Global preferences** | Select the operating mode by pressing **F8**:<br>▪ **Static:** uses static settings.<br>▪ **Dynamic:** Partial automatic retrieval of the settings described below from a DHCP server (IPv4) or via SLAAC (IPv6). |
| **Hostname:** | Enter the matrix switch hostname. |
| **Domain:** | Enter the domain the matrix switch is to belong to. |
| **Gateway IPv4:** | Enter the IPv4 address of the gateway. |
| **Gateway IPv6:** | Enter the IPv6 address of the gateway. |
| **DNS Server 1:** | Enter the IP address of the DNS server..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **DNS Server 2:** | Enter the IP address of another DNS server (option)..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **Prioritize IPv6:** | Select **yes** by pressing **F8** if IPv6 should be preferred when a destination has both an IPv6 and an IPv4 address (*default*: **no**). |
| **Use SLAAC:** | Select **yes** (*default* if the *SecureCert feature* is not activated) by pressing **F8** if SLAAC should be used. Otherwise, select **no** (*default* if the *SecureCert feature* is activated). |
| **Send Mcast Echo Reply (IPv6):** | Select **yes** (*default*) by pressing **F8** if ICMPv6 Echo Requests should be answered. Otherwise, select **no**. |
| **Send DestUnreach (IPv6):** | Select **yes** (*default*) by pressing **F8** if an ICMPv6 error message should be sent to the sender when a packet cannot be delivered. Otherwise, select **no**. |

| | |
|---|---|
| **Process Redirects (IPv6):** | Select **yes** (*default*) by pressing **F8** if redirect messages should be accepted and processed. Otherwise, select **no**. |
| **Dupl. addr. detection (IPv6):** | Select **yes** (*default*) by pressing **F8** if a check for duplicate IPv6 addresses should be performed before an address is used. Otherwise, select **no**. |

5. Press **F2** to save your settings.

## Configuring a KVM-over-IP connection

The **IP address** of the console module (host) as well as the **control port** of the computer module must be specified to establish a **KVM-over-IP** connection through the computer module.

The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

**NOTE:** The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

**How to configure a KVM-over-IP connection:**

1. Use the remote hotkey **Ctrl+Num** to open the OSD of computer module.
2. Select the entry **KVM connection** and press **Enter**.
3. Enter the following data under **Network setting**:

| | |
|---|---|
| **Control port:** | Enter the number of the port you want to use. |
| **Communication port:** | Enter the number of the port you want to use. |
| **Data port:** | Enter the number of the port you want to use. |

4. Press **F2** to save your settings.

# Configuring a KVM-over-IP connection of a console module

You can carry out the required configuration settings directly on the console.

**NOTE:** Use the **local hotkey** (default: **Alt**+**Num**) to open the local OSD to configure the network interface of the console module, or use the **remote hotkey** (default: **Ctrl**+**Num**) to open the remote OSD to configure the network interface of the computer module.

The settings of both hotkeys are shown during the starting process of the console module (see *Starting process* on page 31).



## Configuring the network interface

**How to configure the network interface:**

1. Use the local hotkey **Alt**+**Num** to open the OSD of console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **Network setup** and press **Enter**.
4. Select the entry **Interfaces** and press **Enter**.

5. Enter the following data under **Transmission**:

> **NOTE:** Each network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

| | |
|---|---|
| **Operational mode:** | Press **F8** to select the operational mode of the interface:<br>▪ **Off:** switches off network interface.<br>▪ **Static IPv4:** A static IPv4 address is assigned.<br>▪ **DHCPv4:** oObtain IPv4 address from a DHCP server. |
| **IP address:** | Enter the IPv4 address of the interface.<br>*This setting is auto obtained in the DHCPv4 operating mode.* |
| **Netmask:** | Enter the network netmask.<br>*This setting is auto obtained in the DHCP operating mode.* |
| **IPv6:** | Press **F8** to enable IPv6 (**enabled**). By default, IPv6 is **disabled**.<br>**NOTE:** When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user. |
| **Static IPv6 address:** | Enter the static IPv6 address of the interface. |
| **Prefix:** | Specify the prefix length (*default*: 64) for the interface according to the notation rules defined in RFC 5952. |

6. Press **F2** to save your settings.

## Configuring the global network settings

Even in complex networks global network settings ensure that the KVM extender is available from all partial networks.

**How to configure global network settings:**

1. Use the local hotkey **Alt+Num** to open the OSD of the console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **Network setup** and press **Enter**.
4. Select the entry **Interfaces** and press **Enter**.
5. Enter the following data under **Main Network**:

| | |
|---|---|
| **Global preferences** | Select the operating mode by pressing **F8**:<br>▪ **Static:** uses static settings.<br>▪ **Dynamic:** Partial automatic retrieval of the settings described below from a DHCP server (IPv4) or via SLAAC (IPv6). |
| **Hostname:** | Enter the matrix switch hostname. |
| **Domain:** | Enter the domain the matrix switch is to belong to. |
| **Gateway IPv4:** | Enter the IPv4 address of the gateway. |
| **Gateway IPv6:** | Enter the IPv6 address of the gateway. |
| **DNS Server 1:** | Enter the IP address of the DNS server..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **DNS Server 2:** | Enter the IP address of another DNS server (option)..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **Prioritize IPv6:** | Select **yes** by pressing **F8** if IPv6 should be preferred when a destination has both an IPv6 and an IPv4 address (*default*: **no**). |
| **Use SLAAC:** | Select **yes** (*default* if the *SecureCert feature* is not activated) by pressing **F8** if SLAAC should be used. Otherwise, select **no** (*default* if the *SecureCert feature* is activated). |
| **Send Mcast Echo Reply (IPv6):** | Select **yes** (*default*) by pressing **F8** if ICMPv6 Echo Requests should be answered. Otherwise, select **no**. |

| | |
|---|---|
| **Send DestUnreach (IPv6):** | Select **yes** (*default*) by pressing **F8** if an ICMPv6 error message should be sent to the sender when a packet cannot be delivered. Otherwise, select **no**. |
| **Process Redirects (IPv6):** | Select **yes** (*default*) by pressing **F8** if redirect messages should be accepted and processed. Otherwise, select **no**. |
| **Dupl. addr. detection (IPv6):** | Select **yes** (*default*) by pressing **F8** if a check for duplicate IPv6 addresses should be performed before an address is used. Otherwise, select **no**. |

6. Press **F2** to save your settings.

## Configuring a KVM-over-IP connection

The **IP address** of the console module (host) as well as the **control port** of the computer module must be specified to establish a **KVM-over-IP** connection through the computer module.

The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

**NOTE:** The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

**How to configure the ports of the KVM-over-IP connection:**

1. Use the local hotkey **Alt+Num** to open the OSD of the console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **KVM Connection** and press **Enter**.

**IMPORTANT:** In order to protect the configuration of the KVM-over-IP connection from unwanted access, we recommend to activate the password protection. Select the **Password protection** entry, press **F8** (**on**) and then **F2** to save your settings.

4. Enter the following data under **Local**:

| | |
|---|---|
| **Control Port:** | Enter the number of the port you want to use. |
| **Communication Port:** | Enter the number of the port you want to use. |
| **Data Port:** | Enter the number of the port you want to use. |

5. Press **F2** to save your settings.

## Add, configuration and deletion of a counterpart

**How to add a new counterpart:**

1. Use the local hotkey **Alt+Num** to open the OSD of the console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **KVM Connection** and press **Enter**.
4. Select the entry **IP-MUX** and press **Enter**.
5. Press the **F3** key to create a new counterpart.
6. Enter the following data:

| | |
|---|---|
| **Name:** | Enter the name of the counterpart to be displayed in the *Select* menu. |
| **Hostname:** | Enter the IP address/host name of the counterpart. |

**NOTE:** In the **Hostname** field, you can use the key combination **Ctrl+F8** to open the **Detected devices** dialog. This dialog shows all unpaired G&D counterparts (computer modules and matrix switches).

Select the desired counterpart and press **Enter** to apply the IP address of the counterpart.

7. Press **F2** to save your settings.

**How to configure a counterpart:**

1. Use the local hotkey **Alt+Num** to open the OSD of the console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **KVM Connection** and press **Enter**.
4. Select the entry **IP-MUX** and press **Enter**.
5. Use the **arrow keys** to select the counterpart to be configured and press the **F5** key.
6. Enter/edit the following data:

| | |
|---|---|
| **Name:** | Enter the name of the counterpart to be displayed in the *Select* menu. |
| **Hostname:** | Enter the IP address/host name of the counterpart. |
| **Control port:** | Enter the number of the **Control port** configured in the counterpart. |
| **Select-Keys** | Enter the desired select key. |

**NOTE:** In the **Hostname** field, you can use the key combination **Ctrl+F8** to open the **Detected devices** dialog. This dialog shows all unpaired G&D conterparts (computer modules and matrix switches).

Select the desired counterpart and press **Enter** to apply the IP address of the counterpart.

7. Press **F2** to save your settings.

**How to delete a counterpart:**

1. Use the local hotkey **Alt+Num** to open the OSD of the console module.
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **KVM Connection** and press **Enter**.
4. Select the entry **IP-MUX** and press **Enter**.
5. Use the **arrow keys** to select the couunterpart you want to delete and press the **F4** key.
6. Confirm the safety prompt to delete the counterpart.

# Extended settings of KVM-over-IP connection

## Limiting the bandwidth

By default, the KVM extender uses the maximum available bandwidth of a Gigabit Ethernet. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

**How to set a limit for the bandwidth of a KVM-over-IP connection:**

1. Use the remote hotkey Ctrl+**Num** to open the OSD of the computer module.
2. Select the row **KVM connection** and press **Enter**.
3. Under **Bandwidth limit (Mb/s)** you can set the bandwidth limit of a KVM-over-IP connection in Mb/s.

   **NOTE:** Entering the value **0** deactivates the limit.

4. Press **F2** to save your settings.

## Classifying IP packets (DiffServ)

For QoS purposes (Quality of Service) you have the possibility to use **Differentiated Services Codepoints** (DSCP) to classify the IP packets.

Through this classification, you can prioritize the data packets, for example, through a switch.

You can define a DSCP for the IP packets of the keyboard, mouse and control data (**Communication** data packets), as well as the IP packets of the video, audio and RS232 data (**Data** data packets).

**How to configure the DSCPs of the IP data packets:**

1. Use the remote hotkey Ctrl+**Num** to open the OSD of the computer module.
2. Select the row **KVM connection** and press **Enter**.
3. Enter the following data under **Network control**:

| | |
|---|---|
| **DiffServ Communication:** | Define the **Differentiated Services Codepoint** (DSCP) to be used for the classification of the IP packets of the **Communication** data packets. |
| **DiffServ Data:** | Define the **Differentiated Services Codepoint** (DSCP) to be used for the classification of the IP packets of the **Data** data packets. |

**NOTE:** Take into consideration that some network switches automatically assign the service class **Network Control** (DSCP name: **CS6**) for *all* data packets.

In such environments, the **DSCP 48** option must not be selected!

4. Press **F2** to save your settings.

## (De)Activating signals

By default, not only keyboard, video and mouse data but also audio data are transmitted.

In addition, you can enable the transmission of RS232 data and, alternatively, disable the transmission of audio data.

**How to (de)activate the transmission of audio or RS232 signals:**

1. Use the remote hotkey Ctrl+**Num** to open the OSD.
2. Select the row **KVM connection** and press **Enter**.
3. Under **Activated signals** use the arrow keys to check the box of the signal you want to (de)activate and press **F8**.
4. Press **F2** to save your settings.

## Restricting KVM-over-IP remote stations (UID locking)

By default, *each* IP matrix and *each* console module is allowed to establish a KVM-over-IP connection to the computer module..

**ADVICE:** Activate the function **UID locking** if you want to *specify* which IP matrix switches or console modules should be able to connect to the computer module.

**How to enable/disable UID locking:**

1. Use the remote hotkey Ctrl+**Num** to open the OSD.
2. Select the row **System setup** and press **Enter**.
3. Select the row **System security** and press **Enter**.
4. Under **UID Locking** press **F8** to select one of the following options:

   **None** ‣ All remote stations may establish a KVM-over-IP connection (*default*).
   **UID** ‣ Only the remote stations specified in the list may establish a KVM-over-IP connection.

5. Select the row **Permit all connected devices** and press **Enter**, if UID Locking is activated and you want to enable a KVM-over-IP connection for all connected devices.
6. Select the row **Manage permitted devices** and press **Enter**, if you want to remove or add any devices.

   **F4: Delete** ‣ Mark the device, that you want to remove from the list, press **F4** and confirm you selection.
   **F3: Add** ‣ Press **F3**.
   ‣ Under Device type press F8 to select the device type you want to add.
   ‣ Enter the UID of the device under **Device UID**.

7. Press **F2** to save your settings.

# IP-MUX functionality

The modules of the **VisionXS-IP** series offer with the **IP-MUX** functionality the possibility to access different computer modules (one after the other).

> **IMPORTANT:** A console module can only be connected to one computer module at a time!

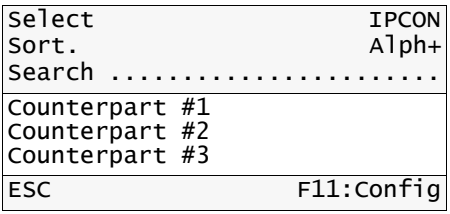
To use this function, you can connect a maximum of 20 computers to separate computer modules and configure these computer modules as counerparts (see page 49 ff.) in the console module.

The configured counterparts can be connected via the local OSD of the console module.

## Accessing a counterpart via OSD

**How to access a counterpart via OSD:**

1. Start the local OSD with the **Alt+Num** hotkey (*default*).




2. Use the **arrow keys** to select the counterpart to be accessed.
3. Press **Enter**.

## Accessing a counterpart via select keys

Calling the OSD is not required when accessing the counterparts using select keys. The counterparts can be accessed faster via select keys.

**How to change the select key modifier or the valid keys:**

1. Start the local OSD with the **Alt+Num** hotkey (*default*)
2. Press **F11** to open the *Configuration* menu.
3. Select the entry **Hotkey** and press **Enter**.
4. Use the arrow key to select *at least* one of the Target Select-Key modifier listed in the **Select-Key modifier** entry. Afterward, press **F8**.

| | |
|---|---|
| **Ctrl:** | *Ctrl* key |
| **Alt:** | *Alt* key |
| **Alt Gr:** | *Alt Gr* key |
| **Win:** | *Windows* key |
| **Shift:** | *Shift* key |

5. Select the **Valid target Select-Keys** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **Num:** | *only numerical keys* are interpreted as select keys when pressed in combination with the select key modifier |
| **Alph:** | *only alphabetic keys* are interpreted as select keys when pressed in combination with the select key modifier |
| **AlphNum:** | *alphabetical and numerical keys* are interpreted as select keys when pressed in combination with the select key modifier |

**IMPORTANT:** Both the selected valid keys and the select key modifier are no longer provided as key combinations to the operating system and the applications on the computer.

6. Press **F2** to save your settings.

**How to access a counterpart via select keys:**

1. Press the Target Select-Key modifier(s) that have been adjusted and the select key assigned to the counterpart (see *Add, configuration and deletion of a counterpart* on page 49 ff.).

> **EXAMPLE:**
>
> - Target Select-Key modifiers: **Alt Gr+Shift**
> - Target Select key for counterpart: **S**
>
> Press **Alt Gr+Shift** and then the select key **S**. As soon the keys are released, the switching to the counterpart takes place.



## Disconnecting a counterpart

**How to disconnect a counterpart:**

1. Start the local OSD with the **Alt+Num** hotkey (*default*).
2. Press the **Ctrl+D** key combination to disconnect the active connection to the counterpart.

# Initial configuration of the network settings

A basic requirement to access the web application of the KVM extender is the configuration of the network settings of the computer module and the console module.

**NOTE:** In the default settings the following settings are preselected:

- IP address of *Network Interface A*: **192.168.0.1**
- global network settings: obtain settings dynamically

The required configuration settings can be made directly at the console.

**IMPORTANT:** At the console, you can use the **local hotkey** (*default*: **Alt+Num**) to open and configure the local OSD of the console module and the **remote hotkey** (*default*: **Ctrl+Num**) to open and configure the remote OSD of the computer module.

During the starting process of the console module the settings of both hotkeys are shown (see *Starting process* on page 31).

## Configuring the network interface

**IMPORTANT:** Configuration of **IPv6** should only be performed **by technically experienced users**. While IPv6 offers advanced features and a larger address space, it also introduces **more complex requirements regarding network structure, security, and compatibility**. Incorrect settings may lead to **connectivity issues or unexpected network behavior**. If you are **not familiar** with the IP addressing and network topology specific to IPv6, we recommend that you thoroughly **inform yourself about the implications** before enabling IPv6, or consult with your network administration.



**How to configure the network interface:**

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl**+**Num**), if you want to change the configuration of the computer module.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt**+**Num**), if you want to change the configuration of the console module.

2. Select the entry **Network setup** and press **Enter**.

3. Select the entry **Interfaces** and press **Enter**.

4. Enter the following data under **Interface A**:

> **NOTE:** The network interface is assigned a unique **zone ID** in addition to its name, which specifies the interface number. This is required to uniquely identify the corresponding interface when using *IPv6 link-local addresses*.

| | |
|---|---|
| **Operational mode:** | Press **F8** to select the operational mode of the interface:<br>▪ **Off:** switch network interface off.<br>▪ **Static IPv4:** A static IPv4 address is assigned.<br>▪ **DHCPv4:** oObtain IPv4 address from a DHCP server. |
| **IP address:** | Enter the IPv4 address of the interface.<br>*This setting is auto obtained in the DHCPv4 operating mode.*<br>**NOTE:** The *Link Local* address space 169.254.0.0/16 is reserved for internal communication between devices in accordance with RFC 3330. It is not possible to assign an IP address of this address space. |
| **Netmask:** | Enter the network netmask.<br>*This setting is auto obtained in the DHCP operating mode.* |
| **IPv6:** | Press **F8** to enable IPv6 (**enabled**). By default, IPv6 is **disabled**.<br>**NOTE:** When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user. |
| **Static IPv6 address:** | Enter the static IPv6 address of the interface. |
| **Prefix:** | Specify the prefix length (*default*: 64) for the interface according to the notation rules defined in RFC 5952. |

5. Press **F2** to save your settings.

## Configuring global network settings

Even in complex networks global network settings ensure that the KVM extender is available from all partial networks.

**How to configure global network settings:**

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl+Num**), if you want to change the configuration of the computer module.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**), if you want to change the configuration of the console module.

2. Select the entry **Network setup** and press **Enter**.

3. Select the entry **Interfaces** and press **Enter**.

4. Enter the following data under **Main Network**:

| | |
|---|---|
| **Global preferences** | Select the operating mode by pressing **F8**:<br>▪ **Static:** uses static settings.<br>▪ **Dynamic:** Partial automatic retrieval of the settings described below from a DHCP server (IPv4) or via SLAAC (IPv6). |
| **Hostname:** | Enter the matrix switch hostname. |
| **Domain:** | Enter the domain the matrix switch is to belong to. |
| **Gateway IPv4:** | Enter the IPv4 address of the gateway. |
| **Gateway IPv6:** | Enter the IPv6 address of the gateway. |
| **DNS Server 1:** | Enter the IP address of the DNS server..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **DNS Server 2:** | Enter the IP address of another DNS server (option)..<br>**NOTE:** If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign **%**. |
| **Prioritize IPv6:** | Select **yes** by pressing **F8** if IPv6 should be preferred when a destination has both an IPv6 and an IPv4 address (*default*: **no**). |
| **Use SLAAC:** | Select **yes** (*default* if the *SecureCert feature* is not activated) by pressing **F8** if SLAAC should be used. Otherwise, select **no** (*default* if the *SecureCert feature* is activated). |
| **Send Mcast Echo Reply (IPv6):** | Select **yes** (*default*) by pressing **F8** if ICMPv6 Echo Requests should be answered. Otherwise, select **no**. |

| | |
|---|---|
| **Send DestUnreach (IPv6):** | Select **yes** (*default*) by pressing **F8** if an ICMPv6 error message should be sent to the sender when a packet cannot be delivered. Otherwise, select **no**. |
| **Process Redirects (IPv6):** | Select **yes** (*default*) by pressing **F8** if redirect messages should be accepted and processed. Otherwise, select **no**. |
| **Dupl. addr. detection (IPv6):** | Select **yes** (*default*) by pressing **F8** if a check for duplicate IPv6 addresses should be performed before an address is used. Otherwise, select **no**. |

5. Press **F2** to save your settings.

## Checking the availability of a host in the network (Ping)

The OSD can be used to test the availability of a particular host (e. g., a computer or a network device) in the network.

**How to check the availability of a host in the network:**

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl**+**Num**), if you want to change the configuration of the computer module.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt**+**Num**), if you want to change the configuration of the console module.

2. Select the entry **Network setup** and press **Enter**.
3. Select the entry **Ping host** and press **Enter**.
4. Use the **Host** entry to enter the IP address or the host name and press **Enter**.
5. The test results are displayed in the following table:

| | |
|---|---|
| **Transmitted:** | number of transmitted data packets |
| **Received:** | number of received data packets |
| **Lost:** | number of lost data packets |
| **Min. RTT:** | minimum round-trip-time |
| **Avg. RTT:** | average round-trip-time |
| **Max. RTT:** | maximum round-trip-time |

**NOTE:** A message informs the user if the host name cannot be resolved into an IP address.

6. Press **Esc** to leave the menu.

## Link aggregation

**IMPORTANT:** To increase reliability, you can enable the **Transmission 2** interface of the KVM extender with the **Transm. Redundancy** feature, which is available for a fee.

Both interfaces are combined into a group via *link aggregation*. Within a group, only one interface is active at a time. Another interface only becomes active if the active interface fails.

Two different modes are available for monitoring the interfaces:

- **MII mode:** The carrier status of the network interface is monitored via the *media independent interface* überwacht. In this mode, only the functionality of the network is tested.
- **ARP mode:** Using the *address resolution protocol*, requests are sent to an ARP target on the network. The response from the ARP target confirms both the functionality of the network interface and a proper network connection to the ARP target.

If the ARP target is connected to the network but temporarily offline, the requests cannot be answered. For this reason, you should determine several ARP targets in order to obtain a response from at least one target even if an ARP target fails.

**NOTE:** It is not possible to combine **MII** and **ARP mode**.

**How to configure the settings of grouped network interfaces:**

**NOTE:** The *Link Local* address space 169.254.0.0/16 is reserved for internal communication between devices in accordance with RFC 3330. It is not possible to assign an IP address of this address space.

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl**+**Num**), if you want to change the configuration of the computer module.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt**+**Num**), if you want to change the configuration of the console module.

2. Select the row **Network setup** and press **Enter** (remote OSD) or **F11**, select the row **Network** and press **Enter** (local OSD).

3. Select the row **Link aggregation** and press **Enter**.

4. Select between the following values under **Parameter**:

| | |
|---|---|
| **Primary follower:** | Press **F8** to select between the options.<br>Select whether data traffic should preferably be transmitted via the interface **Transmission 1** or the interface **Transmission 2**. As soon as the selected interface is available, this interface is used for data traffic.<br>If you select the option **None**, the data traffic is sent via any interface. A switch-over occurs only if the active interface fails. |
| **Link monitoring:** | Press **F8** to select between the options.<br>Select whether you want to use the **MII** or the **ARP** mode (see explanation above) to monitor the interface. |
| **MII down delay:** | Waiting period in milliseconds before a failed network interface is disabled.<br>The entered value must be a multiple of 100 ms (the MII link monitoring frequency). |
| **MII up delay:** | Waiting period in milliseconds before a reset network interface is activated.<br>The entered value must be a multiple of 100 ms (the MII link monitoring frequency). |
| **ARP interval:** | Enter the interval (100 to 10,000 milliseconds) after which the system checks for incoming ARP packets of the network interfaces. |
| **ARP validate:** | The validation ensures that the ARP packet for a particular network interface has been generated by one of the specified ARP targets.<br>Select whether or which of the incoming ARP packets should be validated. Press **F8** to select between the options.<br>▪ **None:** ARP packets are not validated (default).<br>▪ **Active:** Only the ARP packets of the active network interface are validated.<br>▪ **Backup:** Only the ARP packets of the inactive network interface are validated<br>▪ **All:** The ARP packets of all network interfaces of the group are validated. |
| **ARP target:** | The table contains a list of all configured ARP targets.<br>Use the buttons **F3: Add**, **F4: Delete** and **F5: Edit** to manage the ARP targets. |

5. Press **F2** to save your settings.

## Reading out the status of the network interfaces

The current status of both network interfaces can be read out in the OSD.

**How to detect the status of the network interfaces:**

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl+Num**), if you want to change the configuration of the computer module.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**), if you want to change the configuration of the console module.

2. Select the row **Network setup** and press **Enter** (remote OSD) or **F11**, select the row **Network** and press **Enter** (local OSD).

3. Select the row **Link status** and press **Enter**.

4. The paragraphs **Transmission** and **Interface A** include the following values:

| | |
|---|---|
| **Link detected:** | Connection to the network established (**yes**) or disconnected (**no**). |

5. Click on **ESC** to leave the menu.

# On-screen display

When starting the console module, information about the starting process as well as the firmware versions and IDs of the connected modules are displayed in the monitor of the console module.

Additionally, the **local hotkey** (*default*: **Alt**+**Num**) to open the local OSD of the console module and the remote OSD **remote hotkey** (default: **Ctrl**+**Num**) to open the remote OSD of the computer module are shown.

**ADVICE:** Press **Pause** to stop the process. Pressing **Space** continues the process.



## Basic operating of the on-screen display

The on-screen display (OSD) – just like the web application **Config Panel**, which is described on the following – can be used to change the configuration of the KVM extender.

**NOTE:** The actual configuration options by the user depend on the granted rights (see *Changing the user account rights* on page 85 ff.).

The OSD can be opened by pressing a configured hotkey at the console module. You can view and edit the settings of the KVM extender only in the *remote OSD* of the *computer module*.

**IMPORTANT:** The OpenAccess operating mode is set by default. In this operating mode, access to the KVM extender is *not* protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

**IMPORTANT:** The Standard operating mode is set by *default* for devices with *SecureCert feature* activated. In this operating mode, access to the KVM extender is protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

**NOTE:** Use the **remote hotkey** (*default*: **Ctrl**+**Num**) at the console to open and configure the remote OSD of the computer module and the **local hotkey** (*default*: **Alt**+**Num**) to open and configure the local OSD of the console module.

During the starting process of the console module, the settings of both hotkeys are shown (see *Starting process* on page 31).

## Showing the remote OSD

**How to open the remote OSD:**

1. Press **Ctrl+Num** (*default*) to open the OSD.

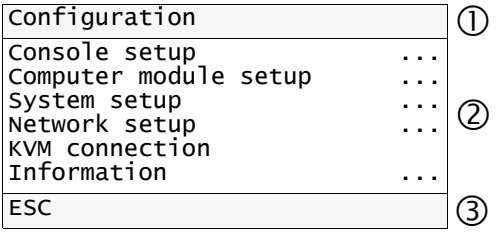
## Showing the local OSD

**How to open the local OSD:**

1. Press **Alt+Num** (*default*) to open the OSD.

## Layout of the OSD

After pressing the remote hotkeys, the OSD is displayed on the console monitor:




The OSD consists of three parts:

| | |
|---|---|
| **Header** ① | The header shows the title of the current menu. |
| **List field** ② | The list field shows the menu items of the selected menu.<br>there are two types of menu items:<br>▪ **Menu items *with* submenus:**<br>These items are displayed with three dots (…) in the right column. Select these items with the **arrow keys** and press **Enter** to open the submenu.<br>▪ **Menu items *without* submenus:**<br>The current setting is shown behind the menü item and can be changed directly. |
| **Footer** ③ | The footer shows the most important keys to operate the currently displayed menu and further information if available. |

## Operating the OSD via keyboard or mouse

### Keyboard operation

The OSD is mainly operated by keyboard. The table below shows a list of frequently used keys:

| | |
|---|---|
| **Arrow keys:** | Press the arrow keys **Up** and **Down** (in some menus also **Left** and **Right**) to move the cursor between the different menu items. |
| **Enter:** | Use this key to confirm inputs of open a submenu. |
| **Esc:** | This key closes the displayed menu and shows the superior menu.<br>A message is shown if entries are changed but not saved. |
| **Tab key:** | Use this key to move the cursor within the list field from one menu item to the next (or vice versa). |
| **F2:** | Press this key to save your settings.<br>The displayed menu closes after the settings are saved and the superior menu is displayed again. |
| **F8:** | Press this key to switch between the different options of a menu item. |
| **Ctrl+F8:** | Configuration settings with many options support this hotkey to open a clearly-arranged list containing all options. |

## Mouse operation

As an alternative to operating the OSD by keyboard, you can use the mouse to execute the following functions:

| | |
|---|---|
| **Mouse movement »Up«:** | This mouse movement moves the cursor *upwards* between the different menu entries in the list field. |
| **Mouse movement »Down«:** | This mouse movement moves the cursor *downwards* between the different menu entries in the list field. |
| **Left mouse key:** | This key is often used to confirm entries (e. g. in the login box) or call a submenu. |
| **Right mouse key:** | The currently displayed menu is closed after your settings are saved. Afterwards, the toplevel menu is shown.<br>A message informs you if you changed your entries but forgot to save them. |

# OSD functions

## Search function

Some menus provide a search function to enable the fast selection of the desired entry in the list field.

**How to search a particular entry with a known name:**

1. Start the local OSD with the **Alt+Num** hotkey (*default*).
2. If necessary, press the **Tab** key to select the list field.
3. Enter the name of the entry you want to search. You can also enter the first letters of the name to enable a clear allocation. The entered characters are displayed in the **Search** field.

> **NOTE:** After *every* entered character, the first entry this character does apply to is marked in the list field.
>
> Placeholders are not supported.

## Changing the sort criteria of the list entries

In the default settings, the list entries are sorted alphabetically in ascending order (*default*: **Alph+**).

**How to change the sort criteria and/or sort order:**

1. Start the local OSD with the **Alt+Num** hotkey (*default*).
2. Press the **Tab** key to select the **Sort** field in the header.
3. Press **F8** to select the desired sort criterion:

| | |
|---|---|
| **Alph+:** | The names of the list entries are sorted alphabetically in *ascending* order. |
| **Alph-:** | The names of the list entries are sorted alphabetically in *descending* order. |

# Overview of the menus of the remote OSD

Use the **remote hotkey** (*default*: **Ctrl+Num**) at the console to open and configure the remote OSD of the computer module.

The following pages show the main menus of the OSD.

## Configuration menu

After you called the remote OSD of the computer module, the Configuration menu opens.

This menu enables you to configure the folloging settings:

| | Function | Description |
|---|---|---|
| **Console setup** | **Console type** | page 98 |
| | **Renaming the console module** | page 99 |
| | **Personal Profile** | page 74 |
| | **Screensaver (min)** | page 115 |
| | **USB auto refresh** | page 114 |
| | **OSD keyb. layout** | page 116 |
| | **Freeze mode and Freeze visualization** | page 109 |
| | **DDC/CI support** | page 110 |
| **Computer module setup** | **Renaming the computer module** | page 99 |
| | **USB HID mode** | page 111 |
| | **EDID mode and Assign EDID** | page 107 |
| | **Color depth** | page 108 |
| **System setup** | **Password complexity** | page 34 |
| | **Login options** | page 36 |
| | **Terms Of Use Config** | page 38 |
| | **Hotkeys** | page 102 |
| | **System security** | page 54 |
| | **Set system defaults** | page 117 |

| | | |
|---|---|---|
| **User setup** | **Add** | page 82 |
| | **Delete** | page 87 |
| | **Name** | page 83 |
| | **Enable** | page 87 |
| | **Password** | page 84 |
| | **Personal profile** | page 74 |
| | **Group membership** | page 86 |
| | **Superuser right** | page 92 |
| | **Config rights** | page 93 |
| | **Global device rights** | page 93 |
| | **Device rights: Access** | page 94 |
| | **Device rights: USB access** | page 95 |
| **User group setup** | **Add** | page 88 |
| | **Delete** | page 91 |
| | **Name** | page 89 |
| | **Enable** | page 91 |
| | **Member management** | page 90 |
| | **Superuser right** | page 92 |
| | **Config rights** | page 93 |
| | **Global device rights** | page 93 |
| | **Device rights: Access** | page 94 |
| | **Device rights: USB access** | page 95 |
| **Network setup** | **Interfaces Network** | page 59 |
| | **Interfaces KVM-over-IP** | page 42 |
| | **Link aggregation** | page 64 |
| | **Link status** | page 66 |
| | **Ping host** | page 63 |
| | **Reset netfilter configuration** | page 118 |
| **KVM connection** | **Control port, Communication port and Data port** | page 44 |
| | **Bandwidth limit (Mb/s)** | page 51 |
| | **DiffServ Communication and DiffServ Data** | page 52 |
| | **Activated signals (Audio and RS232)** | page 53 |
| **Information** | **Hardware, Firmware, Hotkey and Feature information** | page 75 |

## Personal Profile menu

After you called the OSD, press **F10** to open the *Personal Profile* menu. The menu settings only apply for the user whose name is displayed in the right corner.

This menu lists the settings, which can be individually defined for every user:

| Function | Description |
|---|---|
| **Change password** | page 100 |
| **Language** | page 101 |
| **Display** | page 120 |
| **OSD transparency** | page 120 |
| **OSD color** | page 119 |
| **Close OSD when inactive for (s)** | page 121 |
| **Set display position** | page 121 |
| **Set menu position** | page 122 |

## Operation menu

After you called the OSD, press **F9** to open the Operation menu. The following functions can be carried out directly by the user:

| Function | Description |
|---|---|
| **E – User logout** | page 39 |
| **T – Temporary login** | page 33 |

### Information menu

After you called the OSD, press **F12** to open the Information menu. This menu provides the following information:

| Function | Description |
|---|---|
| **Hardware information** | This menu lists e. g., the firmware version, the device´s serial number, and the MAC addresses of the network ports. |
| **Firmware information** | This menu displays the firmware of the console module, and the accessing computer module. |
| **Hotkey information** | This menu displays the active hotkeys. |
| **Feature information** | This menu displays the activated features. |

## Overview of the menus of the local OSD

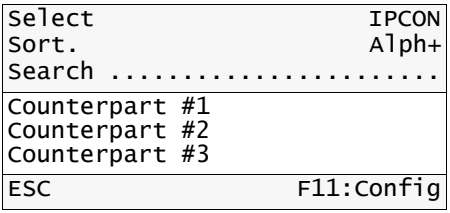
Use the **local hotkey** (*default*: **Alt+Num**) to open and configure the local OSD of the console module.

The following pages show the main menus of the OSD.

### Select menu

The Select menu is usually displayed after the OSD has been called.

The computer modules of the extender system are displayed in this menu (see *IP-MUX functionality* on page 55):




Both the Search and Sort function can be used to limit the displayed computer modules.

### Configuration menu

After you called the OSD, press **F11** to open the Configuration menu. This menu provides the following information:

| | Function | Description |
|---|---|---|
| **Hotkey** | **Edit Hotkey** | page 102 |
| **Keyboard/Mouse** | **USB auto refresh (configuration via remote OSD)** | page 114 |
| | **OSD keyb. layout** | page 116 |
| | **Generic USB** | page 113 |
| **Console utility** | **Set system defaults** | page 117 |
| **Network** | **Interfaces** | page 59 |
| | **Link aggregation** | page 64 |
| | **Link status** | page 66 |
| | **Ping host** | page 63 |
| | **Reset netfilter configuration** | page 118 |
| **KVM connection** | **Password protection** | page 48 |
| | **Control port, Communication port and Data port** | page 48 |
| | **IP-MUX** | page 49 |
| **Information** | **Hardware, Firmware, Hotkey and Feature information** | page 75 |

# Activating a premium function

**NOTE:** The premium functions can be activated in the *Config Panel* web application.

The necessary steps are described in the manual of the web application.

**IMPORTANT:** The *SecureCert feature* is only available with the order of new devices. After sales implementation is **not** possible!

# Web application Config Panel

The **Config Panel** web application provides a graphical user interface to configure and monitor the KVM extender.

## Basic operation of the web application

The web application can be used in the entire network independently from the locations of the devices and consoles connected to the KVM system.

**NOTE:** The separate manual provides information about system requirements, the required configuration of the network interfaces at the **VisionXS-IP-F-TypeC-UHR** devices and the operation of the web application.

### Starting the web application

**How to start the Config Panel web application:**

1. Enter the following URL in the address bar:

   **https://[IP address of the console or computer module]**

2. Enter the following data in the login mask:

| | |
|---|---|
| **Terms (of use):** | Press **Enter** to display the terms of use. |
| **Accept (of terms of use):** | Press **F8** to accept the terms of use. |
| **Username:** | Enter your username. |
| **Password:** | Enter your user account password. |
| **2-Factor Auth Code (TOTP):** | Enter the 2-Factor Auth Code (TOTP) from two-factor authentication. |

**IMPORTANT:** Change the administrator account's default password.

The *default* access data is:

- **Username:** Admin
- **Password:** see *login* information on the label on the bottom of the device

**NOTE:** The *Terms* field and the *Accept* field only appear if Showing terms of use is activated (see *Showing terms of use* on page 38).

**NOTE:** The *2-Factor Auth Code (TOTP)* field only appears if 2-factor-authentication is enabled. For detailed information, please refer to the separate manual of the web application.

3. Click on **Login**.

## Selecting the language of the web application

**How to change the language of the web application:**




1. Click the language identifier of the current language in the upper right corner.
2. Switch the language to be used by clicking on the desired language.

**NOTE:** The selected language is saved in the user settings of the active user. The next time this user logs on, the previously selected language setting is applied.



## Closing the web application

Use the *Close* button to end the active session of the web application.

**IMPORTANT:** To protect the web application against unauthorised access, always use the *Logout* function after finishing your work with the web application.

**How to close the web application:**



1. Click on the **user icon** at the top right.
2. Click on **Logout** to exit the active session.

# Users and groups

## Efficient rights administration

User accounts and user groups can be provided with different rights to operate the system.

**ADVICE:** Rights administration can be carried out almost completely through user groups. Therefore, user groups and the assigned rights have to be planned and implemented beforehand.

This way, user rights can be changed quickly and efficiently.

### The effective right

The effective right determines the right for a particular operation.

**IMPORTANT:** The effective right is the maximum right, which consists of the user account's individual right and the rights of the assigned group(s).

In the OSD, the individual right is highlighted in yellow. The effective right is highlighted in green.

Press **Ctrl+F12** to open the **Right Source** window. Here you can see the groups the effective right results from.

**EXAMPLE:** The user *JDoe* is member of the groups *Office* and *Computer module config*.

The following table shows the user account rights, the rights of the assigned groups and the resulting effective right:

| Right | User *JDoe* | Group *Office* | Group *Computer module config.* | Effective right |
|---|---|---|---|---|
| **Computer module config** | no | no | **yes** | **yes** |
| **Change own password** | no | **yes** | no | **yes** |
| **Device rights: Access** | **full** | view | no | **full** |

The settings of the *Computer module config* and *Change own password* rights result from the rights assigned to the user groups. The right *Device rights: Access* is given directly in the user account.

## Efficient user group administration

User groups let you create a shared right profile for multiple users with identical rights. Furthermore, any user accounts included in the member list can be grouped and therefore no longer have to be individually configured. This facilitates the rights administration within the system.

If the rights administration takes place within user groups, the user profile only stores general data and user-related settings (key combinations, language settings, …).

When initiating the system, it is recommended to create different groups for users with different rights (e. g. »*Office*« and »*IT*«) and assign the respective user accounts to these groups.

**EXAMPLE:** Create more groups if you want to divide the user rights even further. If, for example, you want to provide some users of the »*Office*« group with the *Computer module config* right, you can create a user group for these users:

- Create a user group (e. g., »*computer module admin*«) with identical settings for the »*Office*« group. The *Computer module config* right is set to **Yes**. Assign the respective user accounts to this group.
- Create a user group (e. g., »*computer module admin*«) and set only the *Computer module config* right to **Yes**. In addition to the »*Office*« group, also assign the respective user accounts to this group.

In both cases, the user is provided with the **Yes** effective right for *Computer module config*.

**ADVICE:** The user profile lets you provide extended rights to a group member.

# Administrating user accounts

User accounts let you define individual rights for every user. The personal profile also provides the possibility to define several user-related settings.

**IMPORTANT:** The administrator and any user assigned with the *Superuser* right are permitted to create and delete user accounts and edit rights and user-related settings.

## Creating a new user account

Each user account has individual login data, rights and user-specific settings for the KVM system.

**IMPORTANT:** If an individual password policy is to be taken into account, you must configure the password complexity
(see *Configuring the password complexity* on page 34) before creating a new user account.

**How to create a new user account:**

1. Press the **Ctrl+Num** (default) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Press **F3** and enter the following data:

| | |
|---|---|
| **Name:** | Enter the username. |
| **Password:** | Enter the user account password. |
| **Repeat:** | Repeat the password. |

4. Press **F2** to save your inputs and create an user account.

**IMPORTANT:** The recently created user account can neither configure nor access the computer modules.

Before the account can be used, it has to be added to an existing user group or provided with individual rights (see page 81).

## Renaming a user account

**How to change the name of a user account:**

1. Press the **Ctrl**+**Num** (*default*) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Select the user account you want to rename and press **F5**.
4. Select the **Name** entry and press **Enter**.
5. Enter the new name and press **Enter**.
6. Press **F2** to save your settings.

## Changing the password of a user account

**ADVICE:** The personal password can be changed in the *Personal Profile* menu (see page 74) if the user account is provided with the *Personal Profile* or the *Change own password* right.

**NOTE:** When changing the password, any defined password policies (see *Configuring the password complexity* on page 34) are taken into account.

**How to change the password of a user account:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Select the user account whose password you want to change and press **F5**.
4. Select the **Password** entry and press **Enter**.
5. Enter the following data into the *Change Password* menu:

| | |
|---|---|
| **Current:** | Enter the current password.<br>**NOTE:** No entry is required in this field for users with activated superuser rights (see page 92 ff.). |
| **2-Factor Auth Code (TOTP):** | Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.<br>**NOTE:** The *2-Factor Auth Code (TOTP)* field only appears if 2-factor-authentication is enabled. For detailed information, please refer to the separate manual of the web application. |
| **New:** | Enter your new password. |
| **Repeat:** | Repeat your new password. |

6. Press **F2** to save your settings.

## Changing the user account rights

Any user account can be assigned with different rights.

The following table lists the different user rights. Further information on the rights can be found on the indicated pages.

| Name | Right | Page |
|---|---|---|
| **Change own password** | Change own password | page 94 |
| **Personal profile** | Change personal user settings | page 93 |
| **Superuser right** | Unrestricted access to the configuration of the system | page 92 |
| **Device rights: Access** | Access rights to a computer module | page 94 |
| **Computer module config** | Configuration of computer modules | page 94 |
| **Device rights: USB access** | Access USB devices for all modules | page 95 |
| **WebIf login** | Login to the **Config Panel** web application | page 93 |

## Changing a user account's membership

**NOTE:** Any user within the system can be a member of up to 20 user groups.

**How to change a user account's group membership:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Select the user account whose group membership you want to change and press **F5**.
4. Select the **Group membership** entry and press **Enter**.
5. Select the user group to which you want to add a user account or from which you want to delete a user account.

   **ADVICE:** Use the menu's *search function* or the *sort criteria* (see page 71) to limit the selection of list entries.

6. Press **F8** to add the user account to or delete it from the selected user group

   **NOTE:** User groups to which the user account is assigned to are marked with an arrow (▸).

7. Repeat steps 5 and 6 to edit the group membership for further accounts.
8. Press **F2** to save your settings.

## Enabling or disabling a user account

**IMPORTANT:** If a user account is disabled, the user has no access to the KVM system.

**How to enable or disable a user account:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Select the user account you want to (de)activate and press **F5**.
4. Select the **Enable** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **yes:** | user account activated |
| **no:** | user account deactivated |

5. Press **F2** to save your settings.

## Deleting a user account

**How to delete a user account:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User setup** entry and press **Enter**.
3. Select the user account you want to delete and press **F4**.
4. Select **Yes** and press **Enter** to respond to the prompt for confirmation.

# Administrating user groups

*User groups* enable the user to create a common rights profile for several users with the same rights and to add user accounts as members of this group.

This way, the rights of these user accounts do not have to be individually configured, which facilitates the rights administration within the KVM system.

**NOTE:** The administrator and any user with the *Superuser* right are authorised to create and delete user groups as well as edit the rights and the member list.

## Creating a new user group

The user can create up to 1,024 user groups within the system.

**How to create a new user group:**

1. Press the **Ctrl+Num** (default) hotkey to open the OSD.
2. Select the **User group setup** entry and press **Enter**.
3. Press **F3** and enter the following data:

| | |
|---|---|
| **Name:** | Enter the name of the user group. |

4. Press **F2** to save your inputs and create an user account.

**IMPORTANT:** The recently created user group can neither configure nor access the computer modules
(see *Efficient user group administration* on page 81).

## Renaming a user group

**How to rename a user group:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User group setup** entry and press **Enter**.
3. Select the user group you want to rename and press **F5**.
4. Select the **Name** entry and press **Enter**.
5. Enter the new name and press **Enter**.
6. Press **F2** to save your settings.

## Changing the user group rights

The various user groups can be assigned with different rights.

The following table lists the different user rights. Further information on the rights can be found on the indicated pages.

| Name | Right | Page |
|---|---|---|
| **Change own password** | Change own password | page 94 |
| **Personal profile** | Change personal user settings | page 93 |
| **Superuser right** | Unrestricted access to the configuration of the system | page 92 |
| **Device rights: Access** | Access rights to a computer module | page 94 |
| **Computer module config** | Configuration of computer modules | page 94 |
| **Device rights: USB access** | Access USB devices for all modules | page 95 |
| **WebIf login** | Login to the **Config Panel** web application | page 93 |

## Administrating user group members

**How to administrate user group members:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User group setup** entry and press **Enter**.
3. Select the user group whose member you want to administrate and press **F5**.
4. Select the **Member management** entry and press **Enter**.
5. Select the user account you want to add to or delete from the user group..

> **ADVICE:** Use the menu's *search function* or the *sort criteria* (see page 71) to limit the selection of list entries.

6. Press **F8** to add the user account to the selected user group or to delete it from this group

> **NOTE:** User accounts that are assigned to the user group are marked with an arrow (▸).

7. Repeat steps 5 and 6 to change the group membership for further accounts.
8. Press **F2** to save your settings.

## (De)activating a user group

**How to (de)activate a user group:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User group setup** entry and press **Enter**.
3. Select the user group you want to (de)activate and press **F5**.
4. Select the **Enable** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **yes:** | user group activated |
| **no:** | user group deactivated |

> **IMPORTANT:** If the user group is deactivated, the group rights do *not* apply to the assigned members.

5. Press **F2** to save your settings.

## Deleting a user group

**How to delete a user group:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Select the **User group setup** entry and press **Enter**.
3. Select the user group you want to delete and press **F4**.
4. Select **Yes** and press **Enter** to respond to the prompt for confirmation.

# System rights

## Rights for unrestricted access to the system (Superuser)

The *Superuser* right allows a user unrestricted access to the configuration of the KVM system.

**NOTE:** The information about the user's previously assigned rights remains stored when the *Superuser* right is activated and is reactivated when the right is revoked.

**How to assign a user account with unrestricted access to the system:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose *Superuser* rights you want to change and press **F5**.
4. Select the **Superuser right** entry and press F8 to select one of the following options:

| | |
|---|---|
| **yes:** | full access to the KVM system |
| **no:** | access authorisation according to user and group rights |

5. Press **F2** to save your settings.

## Changing settings in the »Personal Profile« menu

**How to change a user account's operating rights:**

1. Press the **Ctrl**+**Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose rights you want to change and press **F5**.
4. Select the **Global device rights** entry and press **F8**.
5. Select the **Personal profile** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **yes:** | Allows to view and edit the personal profile |
| **no:** | Denies to view and edit the personal profile |

6. Press **F2** to save your settings.

## Changing the login right to the web application

**How to change the login right to the web application:**

1. Press the **Ctrl**+**Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose rights you want to change and press **F5**.
4. Select the **Config rights** entry and press **F8**.
5. Select the **WebIf login** entry and press F8 to select one of the following options:

| | |
|---|---|
| **yes:** | Allow access to web application |
| **no:** | Deny access to web application |

6. Press **F2** to save your settings.

## Rights to change your own password

**How to change the right to change your own password:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose rights you want to change and press **F5**.
4. Select the **Global device rights** entry and press **F8**.
5. Select the **Change own password** entry and press **F8** to select one of the following options:

| | |
|---|---|
| **yes:** | Allow users to change their own password |
| **no:** | Deny users the right to change their own password |

6. Press **F2** to save your settings.

## Access rights to a computer module

**How to change the access rights to a computer module:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose rights you want to change and press **F5**.
4. Select the **Device rights: Access** entry and press **F8**.
5. Select the computer module for which you want to change the access rights.
6. Press F8 to select one of the following options:

| | |
|---|---|
| **full:** | Full access to the computer connected to the computer module allowed |
| **no:** | Access to the computer connected to the computer module denied |
| **view:** | Screen contents of the computer connected to the computer module can be viewed |

7. Press **F2** to save your settings.

## Access rights to USB devices

**How to change the access rights to USB devices:**

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. If you want to change this right for a user account, select the **User setup** entry. For changing this right for a user group, select the **User group setup** entry. Press **Enter**.
3. Select the user account or the user group whose rights you want to change and press **F5**.
4. Select the **Device rights: USB access** entry and press **F8**.
5. Select the computer module for which you want to change the access rights.
6. Press F8 to select one of the following options:

| | |
|---|---|
| **yes:** | Access to USB devices allowed |
| **no:** | Access to USB devices denied |

7. Press **F2** to save your settings.

# Configuration

The configuration of the KVM extender can be changed either using the on-screen display (OSD) or the web application **Config Panel**:

- The *OSD* is shown on the console monitor. Most configuration settings can be changed directly on the OSD of the console.
- The web application **Config Panel** provides a graphical user interface to configure and monitor the KVM extender via web browser.

## Overview of functions and default settings

The following table provides an overview of the configurable functions of the KVM extender. It additionally lists the *default* settings and references to detailed descriptions of the functions.

| Function | Default setting | Page |
|---|---|---|
| Operating modes of console modules | OpenAccess (Standard for devices with *SecureCert feature* activated) | 98 |
| Changing your password | | 100 |
| Selecting the language | German | 101 |
| Changing hotkeys | **Ctrl** | 102 |
| Changing the OSD key | **Num** | 103 |
| Opening the OSD via double keypress | turned off | 104 |
| Channel switching when using a DH computer module | Cursor left, right | 105 |
| Adjusting the operating mode of the RS232 interface | RS232 | 106 |
| Selecting the EDID mode of the KVM extender | auto | 107 |
| Reducing the colour depth of the image data to be transmitted | 24 bit | 108 |
| Freeze mode | disabled | 109 |
| Enabling or disabling DDC/CI support | disabled | 110 |
| (De)Activating an USB keyboard or the »Generic USB« mode | PC Multimedia | 111 |
| Prioritizing a USB device for a reboot | none device | 113 |
| Reinitialising USB input devices | only faulty devices | 114 |
| Adjusting the waiting period of the screensaver | disabled | 115 |
| Automatic user logout | disabled | 115 |
| Selecting a keyboard layout for inputs via OSD | German | 116 |
| Resetting the default settings | | 117 |
| Resetting the netfilter rules | | 118 |

| Function | Default setting | Page |
|---|---|---|
| Changing the colour of the information display | light green | 119 |
| Information display | temporary | 120 |
| Adjusting the transparency of the OSD | average transparency | 120 |
| Automatic closing of the OSD after inactivity | disabled | 121 |
| Changing the position of the information dispaly | left upper corner | 121 |
| Changing the position of the OSD | centred | 122 |

The basic operation of the OSD is described on page 67.

**NOTE:** The separate manual provides more information about the operation of the web application.

# Configuration settings

## Operating modes of console modules

Depending on the application of the KVM extender, you can select one of the following operating modes:

- **OpenAccess mode:** In this mode, access to the KVM extender is *not* protected by authentication.

**NOTE:** This operating mode is set by *default*.

**IMPORTANT:** The Standard operating mode is set by *default* for devices with *SecureCert feature* activated.

You can configure the same access rights for both a KVM extender and a user account.

**IMPORTANT:** The configured access rights apply to all users working with this KVM extender.

- **Standard mode:** The *Standard* mode allows access to the KVM extender only after users are authenticated with their username, password, and 2-factor authentication if set up.

**NOTE:** This operating mode is set by *default*, if you use the extender as a **matrix switch module** (see *Use as extender or matrix switch modules* on page 5).

User rights can be configured in the individual user account.

**How to select the operating mode of the KVM extender:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Console setup** and press **Enter**.
3. Under **Operating mode**, select one of the following options:

   **OpenAccess** ‣ OpenAccess mode (*default*)
   **Standard** ‣ Standard mode (*default* for devices with *SecureCert feature* activated)

4. Press **F2** to save your settings.

## Renaming a console module

**How to rename a console module:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the **Console setup** entry and press **Enter**.
3. Select the **Name** entry and press **Enter**.
4. Enter the new name and press **Enter**.
5. Press **F2** to save your settings.

## Renaming a computer module

**How to rename a computer module:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the **Computer module setup** entry and press **Enter**.
3. Select the **Name** entry and press **Enter**.
4. Enter the new name and press **Enter**.
5. Press **F2** to save your settings.

## Changing your password

**IMPORTANT:** The OpenAccess operating mode is set by *default*. In this operating mode, access to the KVM extender is *not* protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

**IMPORTANT:** The Standard operating mode is set by *default* for devices with *SecureCert feature* activated. In this operating mode, access to the KVM extender is protected by authentication. Information on the operating modes can be found in chapter *Operating modes of console modules* on page 98 ff.

**How to change the password of you user account:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Select the *Change password* entry and press **Enter**.
4. Enter the new password into the *Change own password* menu:

   | | |
   |---|---|
   | **Current** | ‣ Enter the current password. |
   | **2-Factor Auth Code (TOTP)** | ‣ Enter the 2-Factor Auth Code (TOTP) from two-factor authentication. |
   | **New** | ‣ Enter your new password. |
   | **Repeat** | ‣ Repeat your new password. |

   **No** entry is required in the *Current* field for users with activated superuser rights.

   The *2-Factor Auth Code (TOTP)* field only appears if 2-factor-authentication is enabled. For detailed information, please refer to the separate manual of the web application.
5. Press **F2** to save your settings.

## Selecting the language

The specified *system language* is assigned to all user accounts by *default*. If required, you can permanently assign a (different) language to each user account.

**NOTE:** All language settings apply to both the web application and the OSD of the device.

If the OSD does not support the selected language, the OSD will be displayed in English.

**How to set the language:**

OSD

1. Press **Ctrl**+**Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Under **Language** press **F8** to choose between the following options:

   **from system**‣Use the system language
   **[Selection]** ‣ Use the selected language
4. Press **F2** to save your settings.

## Changing hotkeys

If many applications that use hotkeys are running on a computer, or if different KVM devices are used in a cascade, the number of available hotkeys may be limited.

If an application or another device in the cascade uses the same hotkey, the hotkey can be changed.

**NOTE:** Select your desired key or key combination from the keys *Ctrl*, *Alt*, *Alt Gr*, *Win* or *Shift*.

**How to change the current hotkey:**

OSD

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl+Num**), if you want to change the hotkey for the remote OSD.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**), if you want to change the hotkey for the local OSD.
2. Select the row **System setup** and press **Enter** (remote OSD) or **F11** (local OSD).
3. Select the row **Hotkey** and press **Enter**.
4. Under **Modifier**, select *at least* one of the listed hotkey modifiers by selecting the box with the arrow keys. Press **F8** to confirm your selection:

   **Ctrl** ‣ *Ctrl* key (*default* for remote hotkey)
   **Alt** ‣ *Alt* key (*default* for local hotkey)
   **Alt Gr** ‣ *Alt Gr* key
   **Win** ‣ *Windows* key
   **Shift** ‣ *Shift* key
5. Press **F2** to save your settings.

## Changing the OSD key

The hotkey to open the OSD consists of at least one hotkey modifier (see *Changing hotkeys* on page 102) and an additional OSD key. You can freely select these keys from a number of selectable keys.

You can change both the hotkey modifier and the OSD key.

**How to change the current OSD key:**

OSD

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl**+**Num**), if you want to change the hotkey for the remote OSD.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt**+**Num**), if you want to change the hotkey for the local OSD.
2. Select the row **System setup** and press **Enter** (remote OSD) or **F11** (local OSD).
3. Select the row **Hotkey** and press **Enter**.
4. Under **(OSD action)key**, press **F8** to select an OSD key. Now you can open the OSD when pressing the OSD key together with the hotkey modifier(s):

   **Num** ‣ *Num* key (*default*)
   **Pause** ‣ *Pause* key
   **Insert** ‣ *Insert* key
   **Delete** ‣ *Delete* key
   **Home** ‣ *Home* key
   **End** ‣ *End* key
   **PgUp** ‣ *Page Up* key
   **PgDn** ‣ *Pace Down* key
   **Space** ‣ *Space* key
5. Press **F2** to save your settings.

English

## Opening the OSD via double keypress

As an alternative to opening the OSD with the hotkey **Hotkey+ OSD key** or **Double hotkey+ OSD key** you can also open the OSD by pressing a configured key twice.

**How to enable/disable the activation of the OSD via double keypress:**

OSD

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl+Num**), if you want to change the hotkey for the remote OSD.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**), if you want to change the hotkey for the local OSD.
2. Select the row **System setup** and press **Enter** (remote OSD) or **F11** (local OSD).
3. Select the row **Hotkey** and press **Enter**.
4. Under **OSD via 2x keypress** select one of the following options:

   **Off** ‣ OSD cannot be opened via double keypress (*default*)
   **Ctrl** ‣ OSD is opened by pressing the *Ctrl* key twice
   **Alt** ‣ OSD is opened by pressing the *Alt* key twice
   **Alt Gr** ‣ OSD is opened by pressing the *Alt Gr* key twice
   **Win** ‣ OSD is opened by pressing the *Windows* key twice
   **Shift** ‣ OSD is opened by pressing the *Shift* key twice
   **Print** ‣ OSD is opened by pressing the *Print* key twice
5. Press **F2** to save your settings.

## Channel switching when using a DH computer module

You can use a console module of the **VisionXS-IP** series in combination with a DH variant of a computer module of the **VisionXS-IP** series.

**NOTE:** The DH variants allow the transmission of two separate video signals via one transmission cable.

To display the image of the second video output of the computer at the console, you have the possiblity to switch between the video channels.

The key combination for channel switching consists of at least one modifier key (see *Operating modes of console modules* on page 98) and additional *Select stream* keys. Both the modifier key and the *Select stream* keys can be changed.

**How to change the Select stream keys:**

OSD

1. Press **Alt+Num** (*default*) to open the OSD of the console module.
2. Press **F11**.
3. Select the row **Hotkeys** and press **Enter**.
4. Under **Select stream** select one of the following options:

   **Cursor left, right** ‣ *Cursor left key and Cursor right key (Standard)*
   **Num+, Num-** ‣ *Num+-key and Num- key*

5. Press **F2** to save your settings.

## Adjusting the operating mode of the RS232 interface

By *default*, the extender allows you to connect any RS232-compatible device to the *optional* RS232 port on the console module. The RS232 data stream is transmitted to the computer module unchanged.

For transmitting RS422 signals, you can use two **G&D RS232-422 adapters**. Each of the adapters converts the RS232 interface of the console module and the computer module into **RS422** interfaces.

**IMPORTANT:** If you want to transmit **RS422** signals, in addition to using adapters, you also need to change the operating mode of the *RS232* interfaces of both the console *and* the computer module.

**How to set the operating mode of the RS232 interface:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Console setup** and press **Enter** if you want to adjust the operating mode of the RS232 interface of the console module (**CON**).

   Select the row **Computer module setup** and press **Enter** if you want to adjust the operating mode of the RS232 interface of the computer module (**CPU**).
3. Under **RS232 port mode** press **F8** to select one of the following options:

   **RS232** ‣ The data stream of an RS232 device is transmitted from the computer module to the console module (*default setting*).

   **RS422** ‣ The data stream of an RS422 device is transmitted from the computer module to the console module via separately available **G&D RS232-422 adapters**.
4. Press **F2** to save your settings.

## Selecting the EDID mode of the KVM extender

EDID information (*Extended Display Identification Data*) of a monitor informs the graphics card of a connected computer about different technical device features. The information is usually transmitted via Enhanced-DDC (*Enhanced Display Data Channel*) and without any alteration between KVM extender and computer.

**NOTE:** For initial operation and when connecting another monitor, please follow the activation sequence recommended on page 31.

Special GUD profiles are available for some resolutions. The names of these profiles contain information about the preferred resolution that is sent to the computer's video card when the profile is used.

**IMPORTANT:** Please note that the profile selected on the computer module must also be supported by the console module and its connected monitor. Otherwise, an error message is displayed, e.g. *Pixel clock too high* (Pixel clock higher than supported by the current console module).

As an alternative, you can use the web application **Config Panel** web application to read the EDID profile of a monitor. The KVM extender will then transmit it to the connected computer. For detailed information on this topic, refer to the separate manual of the **Config Panel** web application.

**How to select the EDID mode of KVM extenders:**

OSD

1. Press **Ctrl**+**Num** (*default*) to open the OSD.

   Select the row **Computer module setup** and press **Enter**.

2. Under **EDID mode** press **F8** to select one of the following options:

   **auto** ‣ automatic treatment of EDID data (*default*)
   **user** ‣ use of a G&D profile or a profile that has been read out via web application

3. If the option **user** has been selected, select the row **Assign EDID** and press **Enter**.

   Use the **arrow keys** to select the profile you want the activate and press **F8**. Save your selection by pressing **F2**.

4. Press **F2** to save your settings.

## Reducing the colour depth of the image data to be transmitted

By *default*, the KVM Extender transmits image information to the console module at a maximum color depth of 24 bits.

When using a high resolution and displaying moving images, the console module may "skip" several images.

In such cases, reduce the color depth of the image data to 18 bits. This will reduce the amount of data to be transmitted.

**NOTE:** Depending on the image contents, reducing the colour depth may result in slight colour grades.

**How to change the colour depth of the image data to be transmitted:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.

   Select the row **Computer module setup** and press **Enter**.

2. Under **Color depth** press **F8** to select one of the following options:

   **24 Bit:** ‣ transmits the image data with a maximum colour depth of 24 bits (*default*)
   **18 Bit:** ‣ reduces the colour depth of image data to 18 bits

3. Press **F2** to save your settings.

## Freeze mode

If the cable between the computer module and the console module is disconnected during operation, the KVM extender will not display an image on the remote console.

Enable the *Freeze* mode if you want the last image that has been displayed at the console module to be available until the connection is re-established.

To highlight an interrupted connection, the last available image can be displayed with either a coloured frame and/or a **Frozen** popup and the time passed since the connection has been interrupted.

**How to configure the Freeze mode:**

OSD

1. Press **Ctrl**+**Num** (*default*) to open the OSD.

   Select the row **Console setup** and press **Enter**.

2. Under **Freeze mode** press **F8** to select one of the following options:

   **off** ‣ Freeze mode is disabled (*default*)
   **on** ‣ Freeze mode is enabled

3. If the *Freeze* mode is active, press **F8** to select one of the options available under **Freeze visualization**:

   **frame** ‣ shows a coloured frame when disconnected
   **OSD** ‣ shows *Frozen* and the time passed since disconnection
   **frame**+**OSD** ‣ shows a coloured frame (**frame**) and *Frozen* (**OSD**)

4. Press **F2** to save your settings.

## Enabling or disabling DDC/CI support

The computer and console modules supported by the **VisionXS-IP-F-TypeC-UHR** system are ready to support monitors with **DDC/CI** functionality.

After the function is enabled, the DDC/CI information is *transparently* forwarded to the monitor in order to support as many monitors as possible. However, we *cannot* guarantee the support for all monitors.

**How to configure the DDC/CI support of a console module:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.

   Select the row **Console setup** and press **Enter**.

2. Under **DDC/CI support** press **F8** to select one of the following options:

   | | |
   |---|---|
   | **disabled** | The transmission of DDC/CI signals is disabled (*default*). |
   | **CPU > monitor** | The transmission of DDC/CI signals is carried out exclusively from the CPU to the monitor. |
   | **bidirectional** | The transmission of DDC/CI signals is carried out bidirectionally. |

3. Press **F2** to save your settings.

## (De)Activating an USB keyboard or the »Generic USB« mode

The KVM extender supports various USB input devices. You can use the special features of a particular USB input device after selecting the specific USB keyboard mode.

As an alternative to the specific USB keyboard modes, you can also use the **generic USB** mode. In this mode, data of the USB devices is transmitted to the computer module without being altered.

**IMPORTANT:** The **generic USB** mode supports USB mass storage devices and many available USB devices (including FIDO security keys and some SmartCard readers, for example). However, being able to operate particular USB device in generic USB mode can not be guaranteed.

**IMPORTANT:** This console module allows up to five Generic USB devices to be used simultaneously. Both the console module and the computer module must support the use of up to five Generic USB devices.

Only up to three HighSpeed devices (e.g. USB flash drive) and two FullSpeed devices can be used. If additional HighSpeed devices are connected, they will not be accepted.

- **USB keyboards:** The *default* USB keyboard mode **Multimedia** supports the keys of the *default* keyboard layout.

When using an *Apple keyboard* a special keyboard mode allows you to use the special keys of these keyboards.

The following table lists the supported USB keyboards:

| INPUT DEVICE | SETTING |
|---|---|
| PC keyboard with additional multimedia keys | ‣ Multimedia |
| PC keyboard with default keyboard layout | ‣ PC default |
| Apple keyboard with numeric keypad (A1243) | ‣ Apple A1243 |

▪ **Displays and Tablets:** You can operated the computer connected to the KVM extender via a supported *display* or *tablet*:

| INPUT DEVICE | SETTING |
|---|---|
| iiyama ProLite TF2415 | ‣ iiyama TF2415 |
| Wacom Intuos5 S | ‣ Wacom Intuos 5S |
| Wacom Intuos5 M | ‣ Wacom Intuos 5M |
| Wacom Intuos5 L | ‣ Wacom Intuos 5L |
| Wacom IntuosPro L | ‣ Wacom IntuosPro L |
| Wacom Cintiq Pro 24 Pen | ‣ Wacom CP24 Pen |
| Wacom Cintiq Pro 27 | ‣ Wacom CP27 Pen/Touch |
| Wacom Cintiq Pro 32 Pen | ‣ Wacom CP32 Pen |
| Wacom Cintiq Pro 32 Touch | ‣ Wacom CP32 Touch |
| Wacom DTK-2451 | ‣ Wacom DTK-2451 |

▪ **Generic-USB mode:** In this mode, data of the USB devices is transmitted to the computer module without being altered.

| INPUT DEVICE | SETTING |
|---|---|
| any USB mass storage or USB HID device | ‣ Generic USB |

**IMPORTANT:** The **generic USB** mode supports many available USB mass storage devices and HID devices. However, being able to operate particular device in generic USB mode can not be guaranteed.

▪ **LK463 compatible keyboard:** You can connect an LK463 compatible keyboard to the console modules. The order of the 108 keys of these keyboards corresponds to the OpenVMS keyboard layout.

A special USB keyboard mode ensures that whenever a special key on this keyboard is pressed, the action is transmitted to the connected computer:

| INPUT DEVICE | SETTING |
|---|---|
| LK463 compatible keyboard | ‣ LK463 |

**How to select a USB-HID mode:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Computer module setup** and press **Enter**.
3. Select the row **USB HID mode** and press **F8** key to select an option (see above).
4. Press **F2** to save your settings.



## Prioritizing a USB device for a reboot

If multiple USB devices are connected and detected in Generic USB mode, the first detected USB device will be connected *by default* after the console module is rebooted. If both the console module and the computer module support the use of up to five Generic USB devices, up to five USB devices will be reconnected in the order they are detected. These devices appear in yellow on the OSD and are marked with an asterisk (✱).

You can specify a USB device that should be prioritized after a reboot and should be accessible in any case.

**How to prioritize a USB device for a reboot:**

OSD

1. Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**).
2. Press **F11**.
3. Select the **Keyboard/mouse** line and press **Enter**.
4. Select the **Generic USB** line and press **Enter**.
5. Select the USB device you want to access in any case after the reboot and press **Enter**.

   This device will now be highlighted in green with a triangle (▸) on the OSD.
6. Press **F2** to save your settings.

**NOTE:** The prioritization remains even if the USB device is disconnected from the console module (then appears in red on the OSD) and is subsequently reconnected (then reappears in green on the OSD and marked with a triangle (▸)).

## Reinitialising USB input devices

When you connect a USB keyboard or mouse to the KVM extender, the input device is initialized and ready for use.

Some USB input devices require the USB connection to be re-initialized after a period of time. Enable automatic re-initialization of USB input devices if a USB keyboard or mouse stops responding to your input during operation.

**How to enable/disable reinitialisation of USB input devices:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Console setup** and press **Enter**.
3. Under **USB auto refresh** press **F8** to select one of the following options:

   **only faulty** ‣ The status of the USB devices is monitored.
   If communication to a USB device is interrupted, this device is reinitialised (*default*).

   **all** ‣ The status of the USB devices is monitored.
   If communication to one USB device is interrupted, all devices are reinitialised.

   **off** ‣ The status of the USB devices is **not** monitored.
   If communication to a USB device is interrupted, the device is **not** reinitialised.

4. Press **F2** to save your settings.

## Adjusting the waiting period of the screensaver

The screensaver turns off the display of the console after the user has been inactive for a defined period of time.

**NOTE:** This setting does not affect the screensaver settings of the computer connected to the computer module.

**How to adjust the waiting period of the screensaver:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.

   Select the row **Console setup** and press **Enter** if you want to adjust the screensaver of the remote console (at the **CON** module).

2. Under **Screensaver (min)** enter a waiting period (1 to 999 minutes) for the screensaver.

   *Entering the value 0 disables the screensaver.*

3. Press **F2** to save your settings.

## Automatic user logout

A console module can be configured in a way that the access to the computer module is automatically disconnected after a user has been inactive for a certain amount of time. This way, the inactive user is automatically logged out of the KVM matrix system.

**How to set the automatic user logout:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Console setup** and press **Enter**.
3. Under **Auto logout (min)**, you can set the time (between 1 to 999 minutes) for the automatic logout.

   *Entering the value 0 disables the automatic user logout.*

4. Press **F2** to save your settings.

## Selecting a keyboard layout for inputs via OSD

If the OSD displays characters other than those typed on the console keyboard, the keyboard layout must be adjusted.

Find out which keyboard layout is used by the connected keyboard and configure it in the console module settings.

**How to change the keyboard layout of the keyboard of the console module:**

OSD

1. Open the remote OSD of the computer module by pressing the **remote hotkey** (*default*: **Ctrl+Num**), if you want to change the hotkey for the remote OSD.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**), if you want to change the hotkey for the local OSD.

2. Select the row **Console setup** and press **Enter** (remote OSD) or **F11**, select the row **Keyboard/Mouse** and press **Enter** (local OSD).

3. Under **OSD key. layout** press **F8** to select one of the following options:

   - **german**
   - **english US**
   - **english UK**
   - **french**
   - **spanish**
   - **lat. americ.**
   - **portuguese**
   - **swedish**
   - **swiss-french**
   - **danish**

4. Press **F2** to save your settings.

## Resetting the default settings

This function is used to reset the *default* settings of the KVM extender. By performing this function, the *default* settings mentioned on page 96 are reactivated.

**How to reset the default settings:**

**NOTE:** Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**) if you want to reset the **local** settings of the console module only instead of the settings of the extender system.

OSD

1. Open the remote OSD of the computer module by pressing **remote hotkey** (*default*: **Ctrl+Num**) if you want to reset the settings of the extender system.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt+Num**) if you want to reset the local settings of the console module.

2. Select the row **System setup** (remote OSD) or **Console utility** (local OSD) and press **Enter**.
3. Select the row **Set system defaults** and press **Enter**.
4. Confirm the security prompt or cancel the process.

## Resetting the netfilter rules

In the *default* settings, all network computers can access the system's IP address (open system access).

With the *Config Panel* web application, you can create netfilter rules to control the access. After a netfilter rule has been created, the open system access is deactivated and all incoming data packets are compared to the netfilter rules.

The created netfilter rules can also be deleted with this function.

**How to delete the created netfilter rules:**

OSD

1. Open the remote OSD of the computer module by pressing **remote hotkey** (*default*: **Ctrl**+**Num**) if you want to reset the settings of the extender system.

   Open the local OSD of the console module by pressing the **local hotkey** (*default*: **Alt**+**Num**) if you want to reset the local settings of the console module.
2. Select the row **Network** and press **Enter**.
3. Select the row **Reset netfilter configuration** and press **Enter**.
4. Confirm the security prompt or cancel the process.

## Changing the colour of the information display

By *default*, information display are shown in light green. You can adjust the colour of the information display in your personal profile.

The following colours are supported:

| | |
|---|---|
| **black** | **dark red** |
| **green** | **dark yellow** |
| **dark blue** | **purple** |
| **dark turquoise** | **silver** |
| **light green** | **yellow** |
| **blue** | **fuchsia** |
| **light turquoise** | **white** |

**How to change the setting of the information display:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Under **Display color** press **F8** to select the desired colour.
4. Press **F2** to save your settings.

## Information display

Information displays are shown temporarily (5 seconds) in the upper left corner.

**ADVICE:** If the temporary information display is active, you can press the hotkey **Ctrl+Caps Lock** to repeat the caption.

The information display can also be shown permanently or it can be disabled

**How to change the setting of the information display:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Under **Display** press **F8** to select between the following options:

   **off** ‣ information display is turned off
   **temp** ‣ information display is shown temporarily for 5 seconds (*default*)
   **permt** ‣ permanent information display
4. Press **F2** to save your settings.

## Adjusting the transparency of the OSD

In the *default* settings of the KVM switch, the OSD covers parts of the screen content. However, the parts of the screen contents covered by the OSD are still visible.

You can adjust the transparency level or turn the transparency off.

**How to adjust the transparency of the OSD:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Under **OSD transparency** press **F8** to select one of the following options:

   **high** ‣ high transparency of the screen content
   **average** ‣ average transparency of the screen content (*default*)
   **low** ‣ low transparency of the screen content
   **off** ‣ screen content is covered
4. Press **F2** to save your settings.

## Automatic closing of the OSD after inactivity

If desired, you can set the OSD to close automatically after a period of inactivity.

The period of inactivity can be defined by entering a value between **5** and **99** seconds.

**NOTE:** To disable the function, enter the value **0**.

**How to change the period of inactivity after which the OSD closes:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Select the row **Close OSD when inactive for [s]** and press **Enter**.
4. Enter the desired time range from **5** to **99** seconds and press **Enter**.
5. Press **F2** to save your settings.

## Changing the position of the information dispaly

In the *default* configuration, the information display is shown at the left upper corner of the console monitor. However, you can adjust the position to your liking.

**How to change the position of the information display:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Press **F10** to open the **Personal Profile** menu.
3. Select the row **Set display position** and press **Enter**.

   The message on the right is shown at the current position of the information display.

   ```
   +
   Display position
   F2: Save
   ```

4. Use the **arrow keys** or the mouse to move the menu to the desired position or press **Ctrl+D** to reset the *default* position..
5. Press **F2** to save your settings or **Esc** to cancel the process.

## Changing the position of the OSD

By *default*, the OSD is shown at the centre of the console monitor. You can adjust the position to your liking.

**How to change the position of the OSD:**

OSD

1. Press **Ctrl+Num** (*default*) to open the OSD.
2. Select the row **Console setup** and press **Enter**.
3. Select the row **Personal Profile** and press **Enter**.
4. Select the row **Set menu position** and press **Enter**.
5. Use the **arrow keys** or the mouse to move the OSD to the desired position or press **Ctrl+D** to reset the *default* position.
6. Press **F2** to save your settings or **Esc** to cancel the process.

# Further information

## DDC transmission with cache function

The KVM extender supports *Enhanced-DDC* (Enhanced Display Data Channel) to read out the data from the monitor that is connected to the console module and transmit them to the computer. This data includes information regarding the preferred resolution and the supported monitor frequencies.

To make sure that the computer connected to the computer module (**VisionXS-IP-CPU**) can already access the features of the remote monitor during booting, the KVM extender contains a cache function. Even when the computer module or the console module are switched off or the devices are not interconnected, the properties of the most recently connected monitor or a default data block are provided in the KVM extender.

The monitor's DDC information is usually transmitted one-to-one to the computer. Should the KVM extender determine that the display cannot be read without errors or that the entries are invalid, the information is completed or corrected (if possible).

# Determining network settings via service port

If you do not know the IP address of an already configured console module or computer module, you can use the service port of the module to find out the address.

Use any terminal emulator (e.g. *Tera Term* or *PuTTY*) to show the log messages of the modules.

## Installing the device driver

Before establishing a connection using the terminal emulator, install the device driver **CP210x USB to UART Bridge VCP**.

> **NOTE:** When connected to a service cable, the driver provides the *Service* port of a console module or a computer module as a virtual serial interface (COM port). The virtual interface can then be selected to establish a connection using the terminal emulator.

**How to install the device driver to address the service port:**

1. Use any web browser to open the website **www.gdsys.com/en**.
2. Go to **Service > Downloads > Tools & Driver**.
3. Download the device driver for the operating system installed on the computer.
4. Execute the file and follow the instructions of the installation wizard.

## Establishing a connection by using a terminal emulator

**How to establish a connection using a terminal emulator:**

1. Start any terminal emulator (e.g. *Tera Term* oder *PuTTY*).
2. Establish a new connection via terminal emulator and enter the follwoing settings:
   - Bits per second: 115.200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
3. Use the supplied USB service cable to connect the computer to the *Service* port on the back panel of the console or computer module.

### Determining the IP address

**How to determine the IP address of a console module or computer module:**

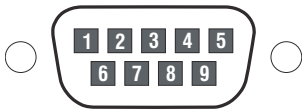
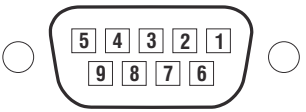
1. Restart the console module or computer module.

   During the boot process, the terminal emulator shows various status messages.

2. After the boot process, the IP address and other **system information** are displayed.

## Pin assignment of the RS232 interface

The following figures show the pin assignments of the RS232 plug as well as the RS 232 socket (depending on model):

| Console module | Computer module |
|---|---|
|  |  |
| RS232 plug | RS232 socket |

The table shows how the different lines of the data connection are assigned to the according pins:

| Pin no. | Line | Console module | Computer module |
|---|---|---|---|
| 1 | *not occupied* | n/c | n/c |
| 2 | RxD (Receive Data) | Input | Output |
| 3 | TxD (Transmit Data) | Output | Input |
| 4 | *not occupied* | n/c | n/c |
| 5 | GND (Ground) | Ground | Ground |
| 6 | *not occupied* | n/c | n/c |
| 7 | RTS (Request to Send) | Output | Input |
| 8 | CTS (Clear to Send) | Input | Output |
| 9 | 5V | Power | Power |

# Status LEDs

The LEDs on the front and back panel of the computer module and the console module let you control the operational status of the KVM extender at any time.

## LED on the front panel of the computer module




| Area | Color | Status | Meaning |
|---|---|---|---|
| | green | on | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode and USB 2.0 |
| | | blinking | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode, USB 2.0 and Power Delivery (36W) |
| | yellow | on | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode, but not USB 2.0 |
| | | blinking | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode and USB Power Delivery (36W), but not USB 2.0 |
| | red | on | source offers USB Power (5V/0.5A), but not DP1.2 Alt-Mode |
| | | off | no source detected |

# LED on the front panel of the console module




| Area | Color | Status | Meaning |
|---|---|---|---|
| | green | on | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode and USB 2.0 |
| | | blinking | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode, USB 2.0 and Power Delivery (36W) |
| | yellow | on | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode, but not USB 2.0 |
| | | blinking | source offers USB Power (5V/0.5A) and is ready to deliver DP1.2 Alt-Mode and USB Power Delivery (36W), but not USB 2.0 |
| | red | on | source offers USB Power (5V/0.5A), but not DP1.2 Alt-Mode |
| | | off | no source detected |

## LEDs on the back panel




| Area | Color | Status | Meaning |
|---|---|---|---|
| **Transmission** | green | on | Logged on at G&D remote station. |
| | yellow | on | Communication with a G&D remote station has been established. |
| | | blinking | Connection to a remote station/network switch established. |
| | | fast blinking | SFP module not detected. |
| | | off | Connection to remote station has not been established.<br>Before use, the **Transmission 2** interface must first be activated using the **Transm. Redundancy** feature, which is available for a fee. |
| **Network** | green | on | The connection to the network has been successfully established. |
| | | off | A connection could not be established. |
| **Pwr** | green | on | The KVM extender is supplied with voltage and the device software has been started successfully. |
| | yellow | on | The KVM extender is supplied with voltage. |
| | blue | on | On as soon as the LED has been activated via web application. |
| | | off | The KVM extender is not supplied with voltage. |

# Used network ports and protocols

**IMPORTANT:** You can find a list of the network ports and protocols that can be used by G&D KVM-over-IP in the separate manual of the web application.

# Technical data

## General features of the series

| VISIONXS-IP-F-TYPEC-UHR SERIES | | |
|---|---|---|
| **Interfaces for computers** | USB Type-C: | 1 × USB Type-C socket |
| | USB keyboard/mouse: | 1 × USB-B socket<br>(USB keyboard/mouse alternatively also possible via the USB Type-C interface) |
| | Audio:<br>‣ Variants [A] and [AR] | 3.5-mm jack plug (Line In) |
| | RS232:<br>‣ Variants [AR] | 1 × RS232 socket (Serial) |
| **Interfaces for remote console** | Video output: | 1 × USB Type-C socket |
| | USB keyboard/mouse: | 2 × USB-A socket |
| | USB devices: | 3 × USB-A socket |
| | Audio:<br>‣ Variants [A] and [AR] | 3.5-mm jack plug (Line Out) |
| | RS232:<br>‣ Variants [AR] | 1 × RS232 plug (Serial) |
| **Transmission to counterpart** | Transmission type: | KVM-over-IP™ |
| | Number of transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional]<br>‣ The second transmission channel can be unlocked with an optionally purchasable feature key. |
| **Other interfaces** | Network: | 1 × RJ 45 socket (100 MBit/s) |
| | Service: | 1 × Micro-USB socket (type B) |
| **Audio**<br>‣ Digital Embedded | Transmission type: | 2 channel LPCM, stereo, DTS, AC3 |
| | Resolutions: | 16/20/24 bit |
| | Sampling rates: | up to 192 kHz (computer modules)<br>up to 48 kHz (console modules) |
| **Audio**<br>‣ Variants [A] and [AR] | Transmission type: | transparent |
| | Resolution: | 24 bit digital, Stereo |
| | Sampling rate: | 96 kHz |
| | Bandwidth: | 22 kHz |
| **RS232**<br>‣ Variants [AR] | Transmission type: | transparent |
| | Transmission rate: | max. 115.200 bit/s |
| | Supported signals: | RxD, TxD, GND, RTS, CTS, 5V |

| VISIONXS-IP-F-TYPEC-UHR SERIES | | |
|---|---|---|
| **Generic USB**<br>› Standard CPU variants support 1 device, CPU-UG variants support up to 5 devices | Specification: | USB 2.0 |
| | USB classes: | Human Interface Device (HID) |
| | | Mass Storage (MSC / UMS) |
| | | SmartCard |
| | Transmission rate: | max. 25 Mbit/s |
| **Graphics** | Format: | DP1.2 Alt-Mode, LBR, HBR, HBR2, SingleStream-Transport (SST) |
| | Colour depth: | 24 bit |
| | Pixel encoding: | RGB 4:4:4 with24bpp/8bpc |
| | Pixel rate: | approx. 25 MP/s to approx. 600 MP/s |
| | Max. resolution: | ▪ 5120 × 2160 @ 50 Hz<br>▪ 5120 × 1440 @ 60 Hz<br>▪ 4096 × 2160 @ 60 Hz (4K2K/60Hz)<br>▪ 2560 × 1440 @ 144 Hz<br>▪ 1920 × 1080 @ 240 Hz (Full HD/240Hz) |
| | Examplary resolutions: | ▪ 3840 × 2160 @ 60 Hz (Ultra HD/60Hz)<br>▪ 2560 × 1600 @ 60Hz<br>▪ 2048 × 2048 @ 60Hz (2K × 2K)<br>▪ 1920 × 1200 @ 60Hz<br>▪ 1920 × 1080 @ 60Hz |
| | | › Further resolutions standardized according to VESA and CTA are possible within the supported video bandwidth/pixel rate and horizontal/vertical frequency. |
| | Vertical frequency: | 24 Hz to 240 Hz |
| | Horizontal frequency: | 25 kHz to 295 kHz |
| **Main power supply** | Type: | external power pack |
| | Connector: | miniDIN-4 Power socket |
| | Voltage: | +12VDC |
| **Redundant power suppply**<br>› Variants [DT] | Type: | internal power pack |
| | Connector: | IEC plug (IEC-320 C14) |
| | Voltage: | AC100-240V/60-50Hz |
| **Alternative power supply**<br>› The sole power supply via USB Power Delivery is not sufficient to execute updates. | Type: | USB Power Delivery 3.0/3.1 (up to 30 Watt) |
| | Operation: | 12V/1,5-2A |
| | | 15V/1-2A |
| | | 20V/0,75-1,5A |
| **Operating environment**<br>› Ensure sufficient air circulation. | Temperature: | +5 to +45 °C |
| | Air humidity: | 20 % to 80 %, non-condensing |

| VISIONXS-IP-F-TYPEC-UHR SERIES | | |
|---|---|---|
| **Storage environment** | Temperature: | -20 °C to +60 °C |
| | Air humidity: | 15 % to 85 %, non-condensing |
| **Conformity** | | CE, UKCA, FCC class B, TAA, EAC, RoHS, WEEE, REACH |

# Specific features of devices

| VISIONXS-IP-CPU-F-TYPEC-UHR | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Power supply: | 12 VDC/1.6 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 109 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 0.9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-UG | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Power supply: | 12 VDC/1.6 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 109 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 0.9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/1.8 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.5-0.3 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 1.3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-UG-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/1.8 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.5-0.3 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 1.3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-AR-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/1.8 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.5-0.3 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 1.3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-AR-UG-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/1.8 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.5-0.3 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 1.3 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-A | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Power supply: | 12 VDC/1.6 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 109 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 0.9 kg |

| VISIONXS-IP-CPU-F-TYPEC-UHR-A-UG | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Power supply: | 12 VDC/1.6 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | approx. 109 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 0.9 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Power supply: | 12 VDC/2.5 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | ca. 109 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 0.9 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/2.5 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.65-0.35 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | ca. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx 1.3 kg |

| VISIONXS-IP-CON-F-TYPEC-UHR-AR-DT | | |
|---|---|---|
| **Interfaces to counterpart** | Transmission channels: | 1, incl. transmission module/ SFP transceiver [+1 optional] × LC duplex socket (10 GBit/s) |
| **Current consumption** | Main power supply: | 12 VDC/2.5 A |
| | Redundant power suppply: | 100-240 VAC/60-50Hz/0.65-0.35 A |
| **Housing** | Material: | anodised aluminium |
| | Dimensions (W × H × D): | ca. 170 × 40 × 184 mm |
| | IP protection class: | IP20 |
| | Weight: | approx. 1.3 kg |

# Features of transmission modules

| MULTIMODE TRANSMISSION MODULE | | |
|---|---|---|
| **Data transmission** | Type: | fibre optics (2 glass fibres) |
| | Interface type: | LC duplex |
| **Cable length (max.)** | Multimode 50/125µm, Class OM4: | 400 metres (fibres with 4700MHz*km) |
| | Multimode 50/125µm, Class OM3: | 300 metres (fibres with 2000MHz*km) |
| | Multimode 50/125µm, Class OM2: | 82 metres (fibres with 500MHz*km) |
| | Multimode 50/125µm: | 66 metres (fibres with 400MHz*km) |
| | Multimode 62,5/125µm, Class OM1: | 33 metres (fibres with 200MHz*km) |
| | Multimode 62,5/125µm, FDDI grade: | 26 metres (fibres with 160MHz*km) |

| SINGLEMODE TRANSMISSION MODULE | | |
|---|---|---|
| **Data transmission** | Type: | fibre optics (2 glass fibres) |
| | Interface type: | LC duplex |
| **Cable length (max.)** | Singlemode 9/125µm, Class OS1: | 10 kilometres (fibres with 500MHz*km) |

# NOTES

# NOTES

# NOTES

# NOTES

## G&D. Control what you see.

**Headquarters | Hauptsitz**

**Guntermann & Drunck GmbH Systementwicklung**

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

**US Office**

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

**Middle East Office**

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

**APAC Office**

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