G&D ControlCenter-IP 2.0

DE Installationsanleitung

EN Installation Guide

A9100357-1.60

Zu dieser Dokumentation

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

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

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

Gewährleistungsausschluss

G&D übernimmt keine Gewährleistung für Geräte, die

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

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

Warenzeichennachweis

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

Impressum

Version 1.60 – 04.03.2025
Firmware: 1.6.000

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

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

www.gdsys.com
sales@gdsys.com

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

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 nur eine aufrechte, horizontale Einbauweise 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.

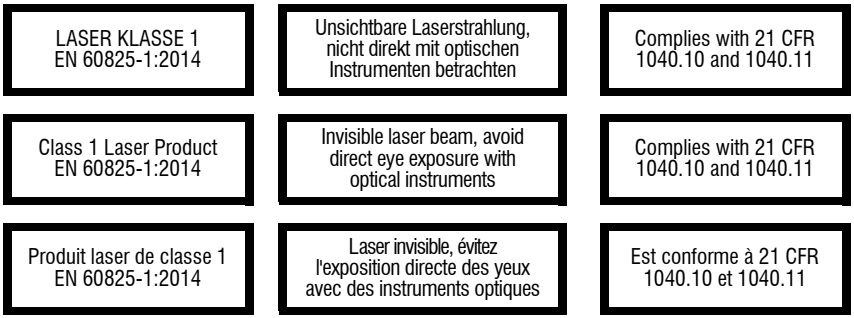
Mettre au rebut les batteries usagées conformêment aux instructions du fabricant et de manière écologique. Les batteries usagées ne doivent pas être jetées dans les ordures ménagères.

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

Besondere Hinweise zum Umgang mit Laser-Technologie

Einige G&D-Gerätevarianten (*Fiber*-Varianten) 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.

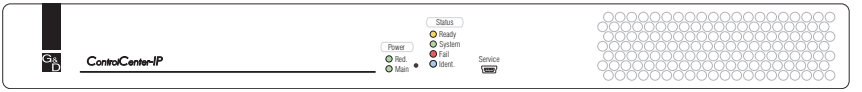
⚠ Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden

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.

Der IP-Matrixswitch »ControlCenter-IP«

Der IP-Matrixswitch *ControlCenter-IP* ist die zentrale Komponente des G&D IP-Matrixsystems.



Das IP-Matrixsystem ermöglicht die Aufschaltung eines IP-Arbeitsplatzmoduls (**CON**) auf ein IP-Rechnermodul (**CPU**). Durch die Aufschaltung wird das Videobild des am Rechnermodul angeschlossenen Computers auf dem Arbeitsplatz-Monitor angezeigt. Mit der Tastatur und Maus des Arbeitsplatzes bedienen Sie den aufgeschalteten Computer.

Sie können beliebige Geräte der **Vision-IP-** und **VisionXS-IP-** sowie der **RemoteAccess-IP-CPU**-Serie als Endgeräte der IP-Matrix einsetzen.

HINWEIS: Im Standard-Lieferumfang unterstützt der IP-Matrixswitch maximal 20 Endgeräte. Die Anzahl der Endgeräte kann durch den Kauf eines Feature-Keys erweitert werden.

Lieferumfang

- 1 × IP-Matrixswitch *ControlCenter-IP*
- 2 × Stromversorgungskabel (PowerCable-2 Standard)
- 1 × Rackmount-Set
- 1 × Sicherheitshinweise-Flyer

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.

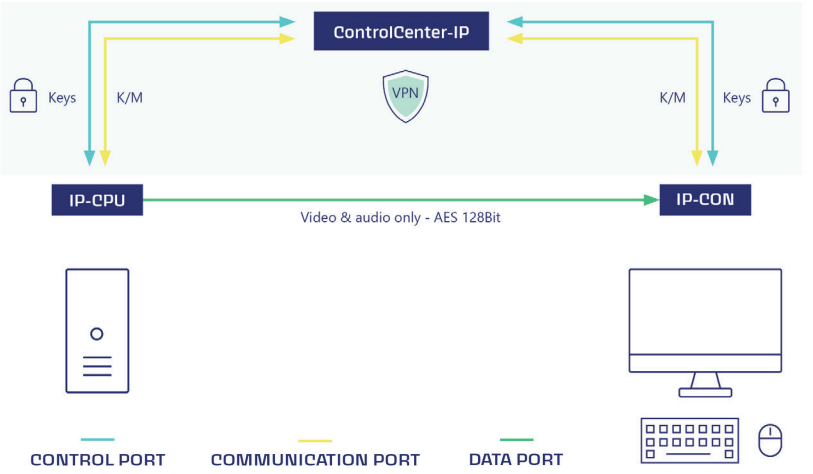
Bei KVM-over-IP-Systemen erfolgt die Übertragung IP-basiert über Ethernet-Netzwerke (OSI-Schichtenmodell Layer 3). Mit KVM-over-IP hat man aufgrund der Flexibilität und einfachen Erweiterbarkeit eine zukunftssichere Lösung. Jedoch steigt mit der IP-Übertragung auch das Sicherheitsrisiko. Es besteht hierbei 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 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 Matrix aufgebaut wird, ist der sogenannte Control-Port. Hier wird mittels eines selbstentwickelten Authentication-Plugins die Kommunikation der Endgeräte 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 von der KVM-over-IP-Matrix 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 Umschalterereignissen. Wenn sich ein Arbeitsplatzmodul mit einem Rechnermodul verbindet, wird ein Sicherheitsschlüssel für diese Verbindung generiert. Sobald sich 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 Matrix 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 dauerhaft und verschlüsselt in der Datenbank des ControlCenter-IP oder ControlCenter-IP-XS gespeichert. 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 Einschmuggeln 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 Temperaturüberschreitung, 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.

Optionale sicherheitsrelevante Zusatzfunktionen

Die Matrix kann mit den folgenden kostenpflichtigen Zusatzfunktionen erweitert werden.

2-Faktor-Authentifizierung (2FA)

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

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

MatrixGuard-Funktion

Die MatrixGuard-Funktion organisiert bei Nichterreichbarkeit des aktuellen Datenbank-Leaders die Weitergabe der Leader-Rolle an einen anderen, erreichbaren Matrixswitch des MatrixGuards.

Alle Matrixswitches eines MatrixGuard-Systems verwenden eine gemeinsame (virtuelle) Matrix-Guard-Adresse. Der MatrixGuard bestimmt anhand der Erreichbarkeit und der Priorität der Teilnehmer automatisch den Datenbank-Leader.

DirectRedundancyShield-Funktion (DRS)

Mittels DirectRedundancyShield (DRS) steht unmittelbar ein zweiter Matrixswitch bereit, sofern der erste nicht mehr erreichbar ist.

Sobald die DRS-Funktion konfiguriert ist, stellen jedes Arbeitsplatz- und jedes Computermodul zwei permanente Verbindungen zur aktiven und passiven KVM-over-IP über das Netzwerk her, wobei nur eine Übertragungsleitung verwendet wird. Wenn die primäre Verbindung unterbrochen wird, übernimmt die vorherige passive Verbindung automatisch und direkt. Das Umschalten erfolgt nahtlos (unter 1 Sekunde).

SecureCert

Mit dem SecureCert Feature können bei den Produktgruppen ControlCenter-IP, ControlCenter-IP-XS, VisionXS-IP, 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.

Anforderung an den Netzwerk-Switch

Die Rechnermodule (**IP-CPU**) versenden den Videostream in der Standardeinstellung per *Multicast* an die Arbeitsplatzmodule (**IP-CON**).

Die Multicast-Übertragung erlaubt Benutzern mit »Multi-Access-Targetzugriff«-Recht die Aufschaltung auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist.

WICHTIG: Die Multicast-Streams werden durch die Netzwerk-Switches gesteuert und ermöglichen die effiziente Verteilung der Streams an mehrere Empfänger zur gleichen Zeit.

Voraussetzungen der Netzwerk-Switches

Folgende Voraussetzungen gelten für das Netzwerk:

- Mindestens **Layer-2-Managed-Switch**, der neben den grundlegenden Switch-Funktionen über zusätzliche Steuer- und Überwachungsfunktionen verfügt, wie z. B. Priorisierung für Quality of Service (QoS) und VLAN-Support.
- **Gigabit Ethernet:** Die Arbeitsplatz- und die Rechnermodule werden mit 1 GBit-Netzwerkverbindungen (gemäß IEEE 802.3ab) an das Netzwerk angebunden.
- **Multicast:** Die Rechnermodule (**IP-CPU**) versenden den Videostream per Multicast. Es ist die Aufgabe des Switches, die Multicast-Gruppen zu verwalten und Multicast-Tabellen zu pflegen.
- **IGMP:** Das *Internet Group Management Protocol* (IGMP) wurde für die Organisation von Multicast-Gruppen konzipiert. Über das Protokoll (min. *IGMPv2*) teilen die Arbeitplatzmodule (**IP-CON**) dem Switch mit, welcher Multicast-Gruppe sie beitreten oder welche sie verlassen möchten.
- **IGMP Snooping:** Als *IGMP-Snooping* wird das Abhören des IGMP-Netzwerkverkehrs durch einen Netzwerk-Switch bezeichnet. Durch das Abhören der IGMP-Konversation können die Switches feststellen, welche ihrer *eigenen* Hosts einen Multicast-Stream angefordert haben. Nur diese Hosts werden mit dem geforderten Multicast-Stream versorgt.

WICHTIG: Ohne *IGMP-Snooping* flutet der Switch alle Ports mit dem Multicast-Stream, damit mögliche Interessenten den Stream empfangen können.

Da der Multicast-Stream eines einzelnen Rechnermoduls bereits das *vollständige* GBit ausnutzt, kommt es zu Paketverlusten, wenn mehr als ein Multicast-Stream gleichzeitig an einem Ports anliegt!

- **IGMP Snooping Querier:** Ein IGMP-Snooping-Querier (Funktion des Switches) fragt in regelmäßigen Abständen alle Abonnenten einer Multicast-Gruppe, ob sie diese noch empfangen möchten (IGMP-Query). Die Antworten (IGMP-Reports) werden von allen lokalen Switchen erkannt und ausgewertet.

  HINWEIS: Ports, die nicht in regelmäßigen Abständen ihr Abonnement zu den jeweiligen Multicast-Gruppen bestätigen, erhalten deren Pakete *nicht* mehr.

  Ist *kein* Querier vorhanden, schaltet ein Switch grundsätzlich den Port nach Ereichen des Timeouts eines Member-Ports für den Empfang von Multicast-Paketen ab.

- **Ausreichende Performance des Netzwerkswitches sicherstellen:** Prüfen Sie die Angaben zu *Forwarding-Bandbreite*, *Switching-Bandbreite* und *Forwarding-Performance* des Netzwerkswitches und berechnen Sie vorab die zu erwartenden Werte Ihrer IP-Matrixswitch-Installation.

  BEISPIEL: Typische Bandbreitenanforderungen bei KVM-over-IP:

  - 3840 × 2160 = 800-900 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung)
  - 2560 × 1440 = 600-500 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung)
  - 1920 × 1080 = 300-400 Mbit/s
    (Office-Anwendung bei ca. 40% Änderung)
  - Fenstermaximierung: 900 Mbit/s bei 3840 × 2160
  - Standbild: 20 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.

  Auch Parameter wie die Größe der *MAC-Adresstabelle* und des *Packet Buffer Memory* können die Performance stark beeinflussen.

- **Flaschenhals bei Verwendung mehrerer Netzwerkswitches vermeiden:** Werden die IP-Endgeräte über mehr als einen Switch verteilt, ist die Verbindung zwischen den Switches möglicherweise ein Engpass.

  Definieren Sie im Vorfeld die gleichzeitig benötigten Multicast-Streams und planen Sie die Netzwerk-Topologie entsprechend.

  WICHTIG: Zu beachten ist, dass die Rechnermodule (**IP-CPU**) möglichst an den Switch angeschlossen werden, auf dem der *IGMP Snooping Querier* läuft.

Empfohlene Einstellungen der Netzwerk-Switches

Nehmen Sie folgende Einstellungen in den Netzwerk-Switches vor, um einen reibungslosen Betrieb der IP-Matrix zu gewährleisten:

- **Aktivierung von »Fast Leave«/»Immediate Leave«:** Wenn eine Arbeitsplatzmodul (**IP-CON**) ein *IGMP-Leave-Paket* an den Switch sendet, wird die Multicast-Gruppe vom Switch noch für einen kurzen Moment weiterhin an den Port gesendet.

  Dies führt zu Bildstörungen, wenn von einer Multicast-Gruppe auf eine andere geschaltet wird, weil kurzzeitig *beide* Multicast-Streams an den Port gesendet werden.

  WICHTIG: Aktivieren Sie *Fast Leave/Immediate Leave*, um das *sofortige* Abschalten des Multicast-Streams zu erreichen.

- **Deaktivierung des »Spanning Tree TCN Flooding«:** Wenn mehrere Netzwerk-Switches im Einsatz sind, wird *Spanning Tree* verwendet, um sicherzustellen (Vermeidung von Loops), dass immer nur ein Datenpfad existiert.

  Wird ein neuer Datenpfad erkannt, aktiviert der Switch kurzzeitig das *TCN flooding* (*topology chance notification*). Hierbei werden Multicast-Gruppen an alle Ports geflutet. Dies führt zu Bildstörungen an den Arbeitsplatzmodulen (**IP-CON**), die gerade auf einen Multicast-Stream eines Rechnermoduls (**IP-CPU**) aufgeschaltet sind.

  WICHTIG: Deaktivieren Sie *Spanning Tree TCN flooding* für die Ports an denen IP-Matrix-Geräte angeschlossen sind.

- **QoS mit DiffServ-/DSCP-Support:** Der IP-KVM-Datenverkehr kann gegenüber anderem Netzwerkverkehr priorisiert werden. In Überlast-Situationen wird mit einer *Strict-Priority* der Verlust von KVM-Daten vermieden.

  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!

Sonderfall: Unicast-Übertragung

Falls Sie in Ihrem IP-Matrixsystem den Benutzern die Aufschaltung auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist, *nicht* gewähren möchten, kann der IP-Matrixswitch alternativ im *Unicast*-Modus betrieben werden (siehe *Festlegung der Art der Videoübertragung* ab Seite 27).

Im Unicast-Modus senden die Rechnermodule (**IP-CPU**) die Videostreams per *Unicast* an die Arbeitsplatzmodule (**IP-CON**). Die Aufschaltung eines Benutzers auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist, ist in diesem Modus *nicht* möglich (Meldung: **No multicast video**)!

HINWEIS: Bei Verzicht auf die *Multicast*-Übertragung werden deutlich weniger Anforderungen an den Netzwerkswitch gestellt.

Folgende der oben aufgelisteten Voraussetzungen und Einstellungen des Netzwerkswitches entfallen in diesem Fall:

Multicast, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* und *Spanning Tree TCN Flooding*.

Installation

Auf den folgenden Seiten wird die Installation der IP-Matrixswitches beschrieben.

HINWEIS: Stellen Sie bei der Standortwahl des Gerätes sicher, dass die zulässige Umgebungstemperatur (siehe *Technische Daten* auf Seite 35) in der unmittelbaren Nähe eingehalten und nicht durch andere Geräte beeinflusst wird.

Sorgen Sie für eine ausreichende Luftzirkulation.

Stromversorgung

Main Power: Schließen Sie ein mitgeliefertes Stromversorgungskabel an. Verbinden Sie das Stromversorgungskabel mit einer Netzsteckdose und schalten Sie den Netzschalter ein.

Red. Power: Schließen Sie ggf. ein mitgeliefertes Stromversorgungskabel zur Herstellung einer redundanten Stromversorgung an. Verbinden Sie das Stromversorgungskabel mit einer Netzsteckdose eines *anderen* Stromkreises und schalten Sie den Netzschalter ein.

Netzwerkschnittstellen

Network A: Stecken Sie ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5e (oder höher) ein.

Das andere Ende des Kabels ist mit einer Netzwerkschnittstelle eines lokalen Netzwerks zu verbinden.

Network B: Stecken Sie ggf. ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5e (oder höher) ein.

Das andere Ende des Kabels ist mit einer Netzwerkschnittstelle eines lokalen Netzwerks zu verbinden.

Service-Schnittstelle

Das Gerät besitzt an der Frontseite 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, 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 *ControlCenter-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 **Mehr von G&D > 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: 115.200
   - Datenbits: 8
   - Parität: Keine
   - Stoppbits: 1
   - Flusssteuerung: Keine

3. Verwenden Sie ein Datenkabel, um den Rechner mit der Service-Buchse an der Frontseite des *ControlCenter-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:
   - 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.

Installation und Anschluss der Arbeitsplatzmodule

WICHTIG: Die **Fiber**-Varianten der Arbeitsplatzmodule 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
- *Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden* auf Seite 4

- Schließen Sie die Geräte des Arbeitsplatzes an die verschiedenen Arbeitsplatzmodule an.
  Die erforderlichen Schritte werden in den Handbüchern der Module beschrieben.

HINWEIS: Die Handbücher der Module stehen Ihnen auf unserer Website **www.gdsys.com/de/start** im Bereich *Mehr von G&D > Handbücher > Handbücher für KVM-over-IP-Extender-Systeme* zur Verfügung.

- Verbinden Sie die *Transmission*-Schnittstellen der einzelnen Arbeitsplatzmodule mit dem Gigabit-Ethernet.

Installation und Anschluss der Rechnermodule

WICHTIG: Die **Fiber**-Varianten der Rechnermodule 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
- *Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden* auf Seite 4

- Schließen Sie die Computer an die verschiedenen Rechnermodule an.
  Die erforderlichen Schritte werden in den Handbüchern der Module beschrieben.

HINWEIS: Die Handbücher der Module stehen Ihnen auf unserer Website **www.gdsys.com/de/start** im Bereich *Mehr von G&D > Handbücher > Handbücher für KVM-over-IP-Extender-Systeme* zur Verfügung.

- Verbinden Sie die *Transmission*-Schnittstellen der einzelnen Rechnermodule mit dem Gigabit-Ethernet.

Netzwerkeinstellungen

Erstkonfiguration der Netzwerkeinstellungen

Grundlegende Voraussetzung für den Zugriff auf die Webapplikation des IP-Matrixswitches ist die Konfiguration der Netzwerkeinstellungen des Gerätes.

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

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

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

1. Verbinden Sie die Netzwerkschnittstelle eines beliebigen Rechners mit der Schnittstelle *Network A* des IP-Matrixswitches.

   Verwenden Sie hierzu ein Twisted-Pair-Kabel der Kategorie 5 (oder höher).

2. Stellen Sie sicher, dass die IP-Adresse der Netzwerkschnittstelle des Rechners Teil des Subnetzes ist, welchem auch die IP-Adresse des IP-Matrixswitches angehört.

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

3. Schalten Sie den IP-Matrixswitch ein.

4. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile die URL **https://192.168.0.1** ein.

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

(Nutzungs-) Bedingungen:	Betätigen Sie die **Eingabtaste**, um die Nutzungsbedingungen angezeigt zu bekommen.
Akzeptieren (der Nutzungsbedingungen):	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: Das voreingestellte *Admin*-Passwort von Geräten mit Produktionsdatum vor Juni 2020 lautet **4658**.

HINWEIS: Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.

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.

6. Klicken Sie auf **Login**.
7. Klicken Sie auf **Config Panel 21**.
8. Klicken Sie im Menü auf **Matrixsysteme > [Name] > Matrix**.
9. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
10. Klicken Sie auf den Reiter **Netzwerk**.
11. Wählen Sie den Bereich **Schnittstellen**.
12. Erfassen Sie im Abschnitt **Schnittstelle A** und/oder **Schnittstelle B** folgende Daten:

Betriebsmodus: Wählen Sie den Betriebsmodus der **Schnittstelle A** bzw. **Schnittstelle B** aus:

- **Aus:** Netzwerkschnittstelle ausschalten.
- **Statisch:** Es wird eine statische IP-Adresse zugeteilt.
- **DHCP:** Bezug der IP-Adresse von einem DHCP-Server.

IP-Adresse: Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die IP-Adresse der Schnittstelle an.

WICHTIG: Die IP-Adresse *192.168.0.1* sollte am *ControlCenter-IP* **nicht** verwendet werden. Da diese IP-Adresse ebenfalls als Standard-IP-Adresse für die Netzwerkmanagement-Schnittstellen der KVM-over-IP-Endgeräte verwendet wird, kann es ansonsten zu Konflikten bei der Kommunikation kommen. Wählen Sie möglichst eine IP-Adresse in einem anderen Subnetz.

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

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

Netzmaske: Geben Sie – nur bei Auswahl des Betriebsmodus *Statisch* – die Netzmaske des Netzwerkes an.

13.Erfassen Sie folgende Daten im Bereich **Globale Netzwerkeinstellungen**:

Betriebsmodus:	Wählen Sie den gewünschten Betriebsmodus: ▪ **Statisch:** Verwendung von statischen Einstellungen. ▪ **DHCP:** Bezug der Einstellungen von einem DHCP-Server.
Host-Name:	Geben Sie den Host-Namen des Gerätes ein.
Domäne:	Geben Sie die Domäne an, welcher das Gerät angehören soll.
Gateway:	Geben Sie die IP-Adresse des Gateways an.
DNS-Server 1:	Geben Sie die IP-Adresse des DNS-Servers an.
DNS-Server 2:	Geben Sie optional die IP-Adresse eines weiteren DNS-Servers an.

14.Klicken Sie auf **Speichern**.

15.Klicken Sie auf das **Benutzersymbol** rechts oben und anschließend auf **Abmelden**.

16.Entfernen Sie die Twisted-Pair-Kabelverbindung zwischen dem Rechner und dem IP-Matrixswitch.

17.Integrieren Sie den IP-Matrixswitch in das lokale Netzwerk.

Reset der Netzfilterregeln

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

Über die Webapplikation können Sie Netzfilterregeln erstellen, um den Zugang zum Matrixsystem 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:

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Betätigen Sie die **F11**-Taste zum Aufruf des *Konfiguration*-Menüs.
3. Wählen Sie die Zeile **System** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie die Zeile **Netzfilterkonfiguration zurücksetzen** und betätigen Sie die **Eingabetaste**.
5. Wählen Sie den Eintrag **Ja** der Sicherheitsabfrage und betätigen Sie die **Eingabetaste**.

Grundkonfiguration der KVM-over-IP™-Verbindung

In diesem Abschnitt werden die für die Inbetriebnahme des IP-Matrixswitches erforderlichen Einstellungen erläutert.

HINWEIS: In der Dokumentation der Webapplikation des IP-Matrixswitches werden *alle* Einstellungen der KVM-over-IP™-Verbindung ausführlich beschrieben.

Aufnahme von Endgeräten

Kompatible Endgeräte können Sie automatisch vom IP-Matrixswitch suchen und hinzufügen lassen.

Die KVM-over-IP™-Verbindung des Endgerätes wird hierbei automatisch vom IP-Matrixswitch konfiguriert und ist danach sofort betriebsbereit.

HINWEIS: Alternativ können Sie die *Ersteinrichtung der KVM-over-IP™-Verbindung* jedes Endgerätes, wie in den Handbüchern der Endgeräte beschrieben, manuell durchführen.

So nehmen Sie (weitere) Endgeräte auf:

1. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile folgende URL ein:

   https://[IP-Adresse des Gerätes]

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

(Nutzungs-) Bedingungen:	Betätigen Sie die **Eingabtaste**, um die Nutzungsbedingungen angezeigt zu bekommen.
Akzeptieren (der Nutzungsbedingungen):	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.

HINWEIS: Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.

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**.
4. Klicken Sie auf **Config Panel 21**.
5. Klicken Sie im Menü auf **Matrixsysteme > [Name] > Matrix**.
6. Klicken Sie auf **Aufnahme von Endgeräten**.

   Die Tabelle *Device Detector* zeigt Ihnen folgende Informationen zu den gefundenen Geräten an:

Name:	Gerätename
IP-Transmission:	IP-Adresse der *Transmission*-Schnittstelle
IP-Management:	IP-Adresse der *Management*-Schnittstelle
MAC-Transmission:	MAC-Adresse der *Transmission*-Schnittstelle
MAC-Management:	MAC-Adresse der *Management*-Schnittstelle
UID:	physikalische ID des Geräts
Status:	Anzeige, ob das Gerät für die Aufnahme zu diesem Matrixswitch grundsätzlich **verfügbar** oder bereits **belegt** ist.

7. Aktivieren Sie den **Hinzufügen**-Schieberegler in der Zeile jedes Gerätes, das Sie dem IP-Matrixswitch hinzufügen möchten.

   TIPP: Um alle zulässigen Geräte *gleichzeitig* dem IP-Matrixswitch hinzuzufügen, aktivieren Sie das Kontrollkästchen im Spaltenkopf der **Hinzufügen**-Spalte.

   HINWEIS: Klicken Sie alternativ auf **Manuell hinzufügen**, um *manuell* den Host-Namen eines aufzunehmenden Endgerätes oder den IP-Adressbereich mehrerer aufzunehmender Endgeräte einzugeben.

8. Klicken Sie auf **Speichern**.

Endgeräte entkoppeln

So entkoppeln Sie ein bereits hinzugefügtes Endgerät:

1. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile folgende URL ein:

   https://[IP-Adresse des Gerätes]

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

(Nutzungs-) Bedingungen:	Betätigen Sie die **Eingabtaste**, um die Nutzungsbedingungen angezeigt zu bekommen.
Akzeptieren (der Nutzungsbedingungen):	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.

HINWEIS: Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.

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**.
4. Klicken Sie auf **Config Panel 21**.
5. Klicken Sie im Menü auf **Matrixsysteme > [Name] > Arbeitsplatzmodule, Rechnermodule** oder **RemoteGateways**.
6. Markieren Sie das zu entkoppelnde Endgerät.

   TIPP: Die Mehrfachauswahl von Geräten ist möglich.

7. Klicken Sie auf **Endgerät entkoppeln**.
8. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Festlegung der Art der Videoübertragung

In der Standardeinstellung versenden die Rechnermodule (**IP-CPU**) die Videostreams per *Multicast* an die Arbeitsplatzmodule (**IP-CON**).

Diese Option erlaubt Benutzern mit »MultiAccess-Targetzugriff«-Recht die Aufschaltung auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist.

WICHTIG: Die Multicast-Streams werden durch die Netzwerk-Switches gesteuert und ermöglichen die effiziente Verteilung der Streams an mehrere Empfänger zur gleichen Zeit.

Beachten Sie die Anforderungen an den *Netzwerk-Switch* für das Versenden der Videostreams per Multicast. Detaillierte Informationen finden Sie in der Installationsanleitung.

Alternativ können Sie einstellen, dass die Rechnermodule (**IP-CPU**) die Videostreams per *Unicast* an die Arbeitsplatzmodule (**IP-CON**) senden.

Die Aufschaltung eines Benutzers auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist, ist in diesem Modus *nicht* möglich (Meldung: **No multicast video**)!

HINWEIS: Bei Verzicht auf die *Multicast*-Übertragung werden deutlich weniger Anforderungen an den Netzwerkswitch gestellt (s. Seite 12 ff.).

Folgende der oben aufgelisteten Voraussetzungen und Einstellungen des Netzwerkswitches entfallen in diesem Fall:

Multicast, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* und *Spanning Tree TCN Flooding*.

Sie können die Festlegung der Art der Videoübertragung systemweit festlegen. Die systemweite Einstellung wird standardmäßig von allen Rechnermodulen angewendet. Zusätzlich können Sie für jedes Rechnermodul die Art der Videoübertragung individuell festlegen.

So konfigurieren Sie die systemweite Einstellung der Multicast- bzw. Unicast-Videoübertragung:

1. Starten Sie das On-Screen-Display (OSD) mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Betätigen Sie die **F11**-Taste zum Aufruf des **Konfiguration**-Menüs.
3. Wählen Sie die Zeile **System** und betätigen Sie die **Eingabetaste**.

4. Markieren Sie die Zeile **Multicast-Video** wählen Sie mit der Taste **F8** zwischen folgenden Optionen:

an:	Die Rechnermodule (**IP-CPU**) versenden standardmäßig den Videostream per *Multicast* an die Arbeitsplatzmodule (**IP-CON**). Diese Option (*Standard*) erlaubt Benutzern mit »MultiAccess-Rechnermodulzugriff«-Recht die Aufschaltung auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist.
aus:	Die Rechnermodule (**IP-CPU**) versenden standardmäßig den Videostream per *Unicast* an die Arbeitsplatzmodule (**IP-CON**). Die Aufschaltung eines Benutzers auf einen Computer, auf den bereits ein *anderer* Benutzer aufgeschaltet ist, ist in diesem Modus *nicht* möglich (Meldung: **Multicast-Video nicht möglich**)!

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

WICHTIG: Die gewählte Einstellung wird erst beim Aufbau einer neuen Verbindung angewendet. Bereits bestehende Verbindungen werden unverändert beibehalten.

So konfigurieren Sie die individuelle Einstellung der Multicast- bzw. Unicast-Videoübertragung eines Rechnermoduls:

1. Starten Sie das OSD mit dem Hotkey **Strg**+**Num** (*Standard*).
2. Betätigen Sie die **F11**-Taste zum Aufruf des **Konfiguration**-Menüs.
3. Wählen Sie die Zeile **Target** und betätigen Sie die **Eingabetaste**.
4. Wählen Sie das zu konfigurierende Rechnermodul und betätigen Sie die **F5**-Taste.

TIPP: Verwenden Sie die *Suchfunktion* oder das *Sortierkriterium* des Menüs, um die Auswahl der Listeneinträge einzugrenzen.

5. Markieren Sie die Zeile **Multicast-Video** wählen Sie mit der Taste **F8** zwischen folgenden Optionen:

System:	Systemweite Einstellung (s. oben) anwenden.
an:	Dieses Rechnermodul (**IP-CPU**) versendet den Videostream per *Multicast* an andere Arbeitsplatzmodule (**IP-CON**). Diese Option erlaubt Benutzern mit »MultiAccess-Rechnermodulzugriff«-Recht die Aufschaltung auf diesen Computer, auch falls bereits ein *anderer* Benutzer aufgeschaltet ist.
aus:	Dieses Rechnermodul (**IP-CPU**) versendet den Videostream per *Unicast* an andere Arbeitsplatzmodule (**IP-CON**). Die Aufschaltung eines Benutzers auf diesen Computer ist nicht möglich, falls bereits ein *anderer* Benutzer aufgeschaltet ist (Meldung: **Multicast-Video nicht möglich**).

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

WICHTIG: Die gewählte Einstellung wird erst beim Aufbau einer neuen Verbindung angewendet. Bereits bestehende Verbindungen werden unverändert beibehalten.

Beschränkung der KVM-over-IP-Gegenstellen (UID-Locking)

In der Standardeinstellung eines Matrixswitches darf *jede* IP-Matrix, *jedes* Arbeitsplatzmodul und *jedes* Rechnermodul eine KVM-over-IP-Verbindung zum Matrixswitch aufbauen.

TIPP: Aktivieren Sie die Funktion **UID-Locking**, falls Sie den Verbindungsaufbau nur *bestimmten* Gegenstellen erlauben möchten.

So (de)aktivieren Sie das UID-Locking:

1. Klicken Sie im Menü auf **Matrixsysteme > [Name] > Matrix**.
2. Klicken Sie auf das zu konfigurierende Gerät und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **KVM-Verbindung**.
4. Tätigen Sie im Abschnitt **UID-Locking** die gewünschten Einstellungen:

UID-Locking:	Nur die in der Liste angegebenen Gegenstellen dürfen eine KVM-over-IP-Verbindung herstellen (**Aktiviert**) oder alle Gegenstellen dürfen eine Verbindung aufbauen (**Deaktiviert**).
Verbundene Geräte-UIDs:	Aktivieren Sie bei eingeschaltetem UID-Locking den **Erlaubt**-Schieberegler in der Zeile jedes Gerätes, das eine Verbindung zum Matrixswitch aufbauen darf.
Rechnermodul hinzufügen:	Klicken Sie auf diese Schaltfläche und geben Sie die UID des Rechnermoduls ein, das eine Verbindung mit diesem Matrixswitch herstellen darf. Klicken Sie abschließend auf **Speichern**.
Arbeitsplatzmodul hinzufügen:	Klicken Sie auf diese Schaltfläche und geben Sie die UID des Arbeitsplatzmoduls ein, das eine Verbindung mit diesem Matrixswitch herstellen darf. Klicken Sie abschließend auf **Speichern**.
RemoteAccess-IP-CPU hinzufügen:	Klicken Sie auf diese Schaltfläche und geben Sie die UID des Rechnermoduls ein, das eine Verbindung mit diesem Matrixswitch herstellen darf. Klicken Sie abschließend auf **Speichern**.
IP-Matrix hinzufügen:	Klicken Sie auf diese Schaltfläche und geben Sie die UID der IP-Matrix ein, die eine Verbindung mit diesem Matrixswitch herstellen darf. Klicken Sie abschließend auf **Speichern**.
Entfernen:	Klicken Sie auf eine erlaubte Gegenstelle und anschließend auf **Entfernen**, um die Erlaubnis zu widerrufen.

5. Klicken Sie auf **Speichern.**

Verwendung des Reset-Tasters

An der Frontseite des IP-Matrixswitches ist ein *Reset*-Taster platziert. Mit diesem Taster ist sowohl die Wiederherstellung der Standardeinstellungen als auch die temporäre Deaktivierung der Netzfilterregeln möglich.

HINWEIS: Um die versehentliche Betätigung des Tasters zu vermeiden, ist dieser hinter einer Bohrung in der Frontblende platziert (zwischen den Power- und Status-LEDs).

Verwenden Sie einen dünnen und spitzen Gegenstand zur Betätigung des Tasters.

Wiederherstellung der Standardeinstellungen

Wird der Taster während des Bootvorganges gedrückt und gehalten, werden die Standardeinstellungen des IP-Matrixswitches wiederhergestellt.

HINWEIS: Nach dem Ausführen der Funktion sind die Standardeinstellungen des IP-Matrixsswitches wieder aktiv. Die freigeschalteten Zusatzfunktionen bleiben erhalten.

So stellen Sie die Standardeinstellungen des IP-Matrixswitches wieder her:

1. Schalten Sie ggf. beide Netzteile des IP-Matrixswitches aus.
2. Betätigen Sie den *Reset*-Taster an der Frontseite des Gerätes und halten Sie diesen gedrückt.
3. Halten Sie den Taster weiterhin gedrückt und schalten Sie das Gerät ein.
4. Sobald die grüne *Status*-LED blinkt, lassen Sie die Taste los.

HINWEIS: Die Wiederherstellung der Standardeinstellungen ist alternativ auch über die Webapplikation *Config Panel* möglich.

Temporäre Deaktivierung der Netzfilterregeln

Im Auslieferungszustand des IP-Matrixswitches haben alle Computer im Netzwerk Zugriff auf die IP-Adresse des Gerätes (offener Systemzugang).

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

Verhindern die aktuell eingestellten Netzfilterregeln den Zugang auf die Webapplikation können Sie die Netzfilterregeln temporär deaktivieren, um diese anschließend zu editieren.

So deaktivieren Sie die eingerichteten Netzfilterregeln temporär:

1. Schalten Sie das Zentralmodul ggf. ein und warten Sie bis das Gerät betriebsbereit ist.
2. Betätigen Sie den *Reset*-Taster auf der Frontseite des Gerätes und halten Sie diesen 5 Sekunden gedrückt.

   WICHTIG: Der offene Systemzugang ist jetzt aktiviert.

3. Bearbeiten Sie die im Gerät gespeicherten Netzfilterregeln mit der Webapplikation *Config Panel* und speichern Sie die Regeln anschließend ab.

   WICHTIG: Wird innerhalb von 15 Minuten keine neue Netzfilterkonfiguration erstellt, werden die ursprünglichen Einstellungen wieder aktiviert.

Statusanzeigen

LEDs an der Frontseite

Die LEDs an der Frontseite des IP-Matrixswitches geben Ihnen die Möglichkeit, den Betriebsstatus des Systems jederzeit zu kontrollieren:

Bereich	LED	Status	Bedeutung
Power	**Red.**	an	Das Netzteil ist eingeschaltet und liefert die erforderliche Spannung.
		aus	Das Netzteil ist ausgeschaltet oder die Verbindung mit dem Stromnetz nicht hergestellt.
	Main	an	Das Netzteil ist eingeschaltet und liefert die erforderliche Spannung.
		aus	Das Netzteil ist ausgeschaltet oder die Verbindung mit dem Stromnetz nicht hergestellt.
Status	**Ready**	blinkt	Gerät ist betriebsbereit oder wird gebootet.
		aus	Interne Kommunikation fehlerhaft.
	System	grün	Gerät betriebsbereit.
		blinkt grün	Wiederherstellung der Standardeinstellungen nach Betätigung des Reset-Tasters
		rot	Das Gerät ist nicht betriebsbereit.
		aus	Interne Kommunikation fehlerhaft.
	Fail	an	Das Gerät ist nicht betriebsbereit.
		aus	Das Gerät ist betriebsbereit oder ausgeschaltet.
	Ident.	an	Leuchtet, sobald die LED über die Webapplikation aktiviert wurde.
		aus	Das Gerät ist betriebsbereit oder ausgeschaltet.

LEDs an der Rückseite

Auf der Rückseite des IP-Matrixswitches befinden sich zusätzliche Status-LEDs. Diese LEDs haben folgende Funktion:

Schnittstelle	LED	Status	Bedeutung
Status	**System**	an	Gerät betriebsbereit.
		aus	Interne Kommunikation fehlerhaft.
	Fail	an	Das Gerät ist nicht betriebsbereit.
		aus	Das Gerät ist betriebsbereit oder ausgeschaltet.
	Ready	blinkt	Gerät ist betriebsbereit oder wird gebootet.
		aus	Interne Kommunikation fehlerhaft.
	Ident.	an	Leuchtet, sobald die LED über die Webapplikation aktiviert wurde.
Network A	**links**	flackert (grün)	Aktivität auf der Netzwerkschnittstelle festgestellt.
		aus	Keine Aktivität auf der Netzwerkschnittstelle festgestellt.
	rechts	an (grün)	Netzwerkverbindung (10M/100M/1G) hergestellt.
		aus	Keine Netzwerkverbindung aufgebaut.
Network B	**links**	flackert (grün)	Aktivität auf der Netzwerkschnittstelle festgestellt.
		aus	Keine Aktivität auf der Netzwerkschnittstelle festgestellt.
	rechts	an (grün)	Netzwerkverbindung (10M/100M/1G) hergestellt.
		aus	Keine Netzwerkverbindung aufgebaut.

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

CONTROLCENTER-IP-2.0-SERIE		
Schnittstellen	Netzwerk:	2 × RJ45-Buchse (10 MBit/s, 100 MBit/s, 1 Gbit/s)
	Service:	1 × Mini-USB-Buchse (Typ B)
	USB 2.0:	2 × USB-A-Buchse
Hauptstrom-versorgung	Typ:	internes Netzteil
	Anschluss:	Kaltgerätestecker (IEC-320 C14)
	Stromaufnahme:	100-240VAC/60-50Hz, 0,7-0,4A
redundante Stromversorgung	Typ:	internes Netzteil
	Anschluss:	Kaltgerätestecker (IEC-320 C14)
	Stromaufnahme:	100-240VAC/60-50Hz, 0,7-0,4A
Gehäuse	Material:	Aluminium eloxiert
	Dimensionen (B × H × T):	ca. 436 × 44 × 210 mm
	IP-Schutzklasse:	IP20
	Gewicht:	ca. 2 kg
Einsatzumgebung	Temperatur:	+5 °C bis +45 °C
	Luftfeuchte:	20% bis 80%, nicht kondensierend
Lagerumgebung	Temperatur:	-20 °C bis +55 °C
	Luftfeuchte:	15% bis 85%, nicht kondensierend
Konformität		CE, UKCA, FCC Klasse B, TAA, EAC, RoHS, WEEE, REACH

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

All 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.

Version 1.60 – 04/03/2025
Firmware: 1.6.000

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.

Contents

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 correct installation position for devices with ventilation openings

For reasons of electric safety, devices with ventilation openings must only be installed in an upright, horizontal position.

⚠ 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.

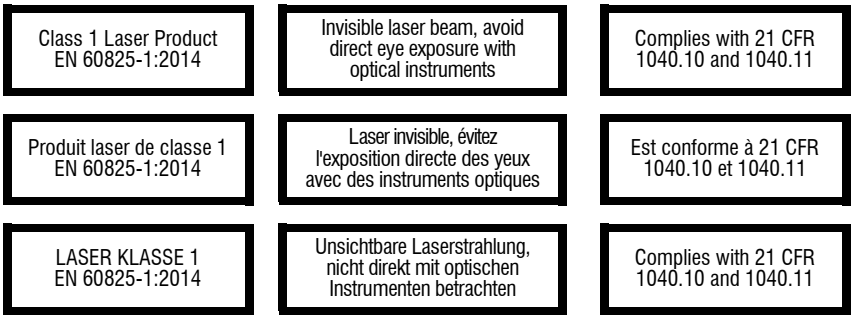
Entsorgen Sie gebrauchte Batterien umweltgerecht. Gebrauchte Batterien dürfen nicht in den Hausmüll geworfen werden.

Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

Special advices for dealing with laser technology

Some G&D device variants (*Fiber* variants) 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.

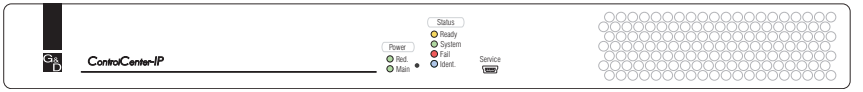
⚠ Only use G&D certified transmission modules

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 »ControlCenter-IP« IP matrix switch

The IP matrix switch *ControlCenter-IP* is the central component of the G&D IP matrix system.



You can use the IP matrix system to access an IP computer module (**CPU**) with an IP console module (**CON**). By accessing the computer connected to the computer module, the video image is displayed at the console monitor. You can now operate the accessed computer with console keyboard and console mouse.

You can use any device of the **Vision-IP**, **VisionXS-IP** and **RemoteAccess-IP-CPU** series as end devices of the IP matrix.

NOTE: In the standard scope of delivery, the IP matrix switch supports a maximum of 20 end devices. The number of devices can be increased by purchasing a feature key.

Scope of delivery

- 1 × IP matrix switch *ControlCenter-IP*
- 2 × Power cable (PowerCable-2 Standard)
- 1 × Rackmount set
- 1× »Safety instructions« flyer

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.

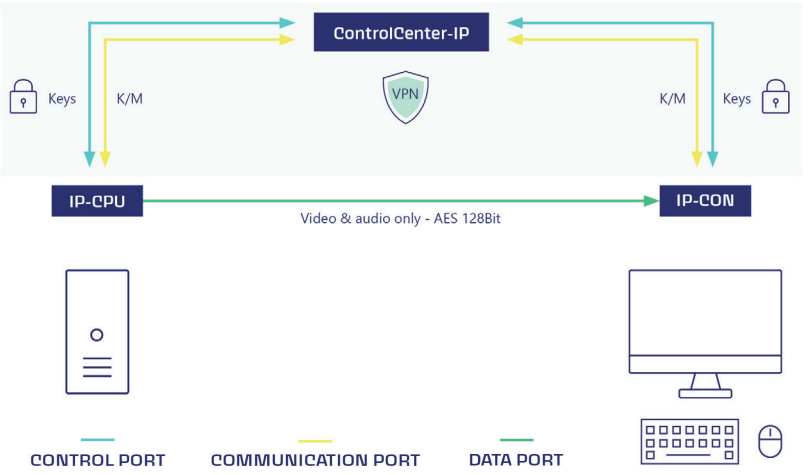
With KVM-over-IP systems, transmission is based on IP and runs on Gigabit Ethernet networks (OSI model layer 3). Using KVM-over-IP provides a future-proof solution due to its flexibility and easy expandability. However, IP transmission also increases security risks. There is an additional external risk, 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 KVM-over-IP matrix ControlCenter-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 matrix is the so-called control port. The communication between the end devices and 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 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, 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 matrix 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. 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, minimum 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.

Optional additional security-relevant functions

The matrix can be extended with the following additional functions for a fee.

2-factor authentication (2FA)

To provide a greater level of security, a second possession-based factor can be requested through the paid 2-factor authentication (2FA) option.

2FA makes use of a time-based one-time password (TOTP). Authenticator apps or hardware tokens can be used.

MatrixGuard function

If the current database leader is unavailable, the MatrixGuard function organises the forwarding of the leader role to another, available matrix switch of the Matrix-Guard.

All matrix switches of a MatrixGuard system share a common (virtual) Matrix-Guard address. The MatrixGuard automatically determines the database leader based on the availability and priority of its members

DirectRedundancyShield function (DRS)

Using DirectRedundancyShield (DRS), a second matrix switch is available directly if the first one is no longer accessible.

Once the DRS function has been configured, each console module and each computer module establishes two permanent connections to the active and the passive KVM-over-IP matrix via the network, only using one transmission line. If the primary connection is disrupted, the previously passive connection takes over automatically and immediately. The transition is almost seamless (less than 1 second).

SecureCert

The SecureCert feature can be used to activate certified security functions for the product groups ControlCenter-IP, ControlCenter-IP-XS, VisionXS-IP, 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.

Selecting a network switch

Computer modules (**IP-CPU**) send the video stream to console modules (**IP-CON**) using *multicast*.

Multicast transmission allows users with »Target multi access« rights to connect to a computer to which *another* user is already connected.

IMPORTANT: The multicast streams are controlled by the network switches and enable efficient distribution of the streams to multiple receivers at the same time.

Requirements of network switches

The following requirements apply to the network:

- At least **layer 2 managed switch** that has additional control and monitoring features, such as prioritization for Quality of Service (QoS) and VLAN support, in addition to basic switch functions.
- **Gigabit Ethernet:** User and computer modules are connected to the network using 1 GBit network connections (in accordance with IEEE 802.3ab).
- **Multicast:** The computer modules (**IP-CPU**) transmit the video stream via multicast. The switch manages the multicast groups and maintains multicast tables.
- **IGMP:** The *Internet Group Management Protocol* (IGMP) was designed for organising multicast groups. The console modules (**IP-CON**) use the protocol (min. *IGMPv2*) to notify the switch which multicast group they want to join or which they want to leave.
- **IGMP snooping:** *IGMP snooping* is the interception of IGMP network traffic through a network switch. By listening to the IGMP conversation, the switches can determine which of their *own* hosts have requested a multicast stream. Only these hosts are supplied with the required multicast stream.

IMPORTANT: Without *IGMP snooping*, the switch floods all ports with the multicast stream so that potential users can receive the stream.

Since the multicast stream of a single computer module already uses the *full* GBit, packet loss occurs if a port receives more than one multicast stream at the same time.

- **IGMP Snooping Querier:** An IGMP snooping querier (function of the switch) regularly asks all subscribers of a multicast group whether they still want to receive this group (IGMP query). The answers (IGMP reports) are identified and evaluated by all local switches.

  NOTE: Ports that do not regularly confirm their subscription to the respective multicast groups *no longer* receive their packets.

  If *no* querier is available, a switch disables the port after reaching the timeout of a member port for receiving multicast packets.

- **Ensure sufficient performance of the network switch:** Check the switch's specifications regarding *forwarding bandwidth*, *switching bandwidth* and *forwarding performance* and calculate the expected values of your IP matrix switch installation in advance.

  EXAMPLE: Typical bandwidth requirements for KVM-over-IP:

  - 3840 × 2160 = 800-900 Mbit/s
    (office application with approx. 40% of changes)
  - 2560 × 1440 = 600-500 Mbit/s
    (office application with approx. 40% of changes)
  - 1920 × 1080 = 300-400 Mbit/s
    (office application with approx. 40% of changes)
  - Window maximization: 900 Mbit/s at 3840 × 2160
  - Still image: 20 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.

  Parameters such as the size of the *MAC address table* and the *packet buffer memory* can have a significant impact on the performance.

- **Avoid bottlenecks when using multiple network switches:** If the IP end devices are distributed across more than one switch, the connection between the switches may be a bottleneck.

  Define the multicast streams required at the same time in advance and plan the network topology accordingly.

  IMPORTANT: Note that the computer modules (**IP-CPU**) should be connected to the switch on which the *IGMP Snooping Querier* is running.

Recommended settings of network switches

Make the following settings in the network switches to ensure a smooth operation of the IP matrix:

- **Activation of »Fast Leave«/»Immediate Leave«:** If a console module (**IP-CON**) sends an *IGMP leave packet* to the switch, the switch shortly continues to send the multicast group to the port.

  This leads to image interferences when switching from one multicast group to another because for a short time *both* multicast streams are sent to the port.

  IMPORTANT: Activate *Fast Leave/Immediate Leave* to disable the multicast stream *immediately*.

- **Deactivation of »Spanning Tree TCN Flooding«:** When multiple network switches are in use, *spanning tree* is used to ensure (loop avoidance) that only one data path exists at a time.

  If a new data path is detected, the switch briefly activates the *TCN flooding* (*topology chance notification*). In this case multicast groups are flooded to all ports. This leads to image interferences at the console modules (**IP-CON**), which are currently connected to a multicast stream of a computer module (**IP-CPU**).

  IMPORTANT: Disable *Spanning Tree TCN flooding* for the ports to which IP matrix devices are connected.

- **QoS incl. DiffServ/DSCP support:** IP KVM traffic can be prioritised over other network traffic. In overload situations, a *strict priority* prevents the loss of KVM data.

  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!

Special Case: Unicast Transmission

If you do not want to allow users in your IP matrix system to connect to a computer on which *another* user is already connected, the IP matrix switch can alternatively be operated in *unicast* mode
(see *Determination of the type of video transmission* on page 27 ff.).

In unicast mode, the computer modules (**IP-CPU**) send the video streams via unicast to the console modules (**IP-CON**). The connection of a user to a computer to which *another* user is already connected is not possible in this mode (message: **No multicast video**)!

NOTE: If *multicast* transmission is not used, the network switch will have to meet considerably fewer requirements.

The following requirements and settings of the network switch listed above do not apply in this case:

Multicast, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* and *Spanning Tree TCN Flooding*.

Installation

The following pages describe the installation of the devices of the IP matrix switch.

NOTE: When choosing a place for the device, please ensure to comply with the ambient temperature limit (see *Technical data* on page 35) close to the device. The ambient temperature limit must not be influenced by other devices.

Ensure sufficient air circulation.

Power supply

Main Power: Plug one of the supplied power cable in this interface. Connect the power cable with a power outlet and turn the power button on.

Red. Power: If required, plug one of the supplied power cable in this interface to establish a redundant power supply. Connect the power cable with a power outlet of *another* power circuit and turn the power button on.

Network interfaces

Network A: Plug in a category 5e (or better) twisted-pair cable, which is available as accessory.

Connect the other end of the cable to a network interface of the local network.

Network B: If required, plug in a category 5e (or better) twisted-pair cable, which is available as accessory.

Connect the other end of the cable to a network interface of the local network.

Service interface

The device has a service interface on the front 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*). A service menu gives technicians the option of reading out information about the device, resetting the device to the factory settings or performing 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 *ControlCenter-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 **More from G&D > 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: 115.200
   - 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 front panel of the *ControlCenter-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:
   - 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.

Installing and connecting console modules

IMPORTANT: The **Fiber** variants of the console modules 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**.

Mind the following instructions when dealing with laser beams:

- *Avoid direct eye exposure to beam* on page 4
- *Always connect optical connections or cover them with protection caps* on page 4
- *Only use G&D certified transmission modules* on page 4

- Connect the console devices to the different console modules.
  The steps required to connect these devices are described in the manuals of the modules.

NOTE: The manuals of the modules are available on the website **www.gdsys.com/en/start** in the section *More from G&D > Manuals > KVM-over-IP extender system manuals*.

- Connect the *Transmission* interfaces of each individual console module to the Gigabit Ethernet.

Installing and connecting computer modules

IMPORTANT: The **Fiber** variants of the computer modules 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**.

Mind the following instructions when dealing with laser beams:

- *Avoid direct eye exposure to beam* on page 4
- *Always connect optical connections or cover them with protection caps* on page 4
- *Only use G&D certified transmission modules* on page 4

- Connect the computers to the different computer modules.
  The steps required to connect these devices are described in the EasyStart flyer of the matrix system and the manual supplied with the modules.

NOTE: The manuals of the modules are available on the website **www.gdsys.com/en/start** in the section *More from G&D > Manuals > KVM-over-IP extender system manuals.*

- Connect the *Transmission* interfaces of each individual computer module to the Gigabit Ethernet.

Network settings

Initial configuration of the network settings

A basic requirement to access the web application is to configure the network settings of the IP matrix switch on which the web application is operated.

NOTE: In the defaults, the following settings are pre-selected:

- IP address of *network interface A*: **192.168.0.1**
- IP address of *network interface B*: address obtained using **DHCP**
- global network settings: settings obtained using **DHCP**

How to configure the network settings before integrating the device into the local network:

1. Use a category 5 (or better) twisted pair cable to connect the network interface of any computer to the device's *Network A* interface.
2. Ensure that the IP address of the computer's network interface is part of the subnet to which the device's IP address belongs to.

   NOTE: Use the IP address *192.168.0.100*, for example.
3. Switch on the device.
4. Start the computer's web browser and enter the URL **https://192.168.0.1** in the address bar.
5. 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.

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 default *admin* password for devices manufactured before June 2020 is **4658**.

NOTE: The *Terms* field and the *Accept* field only appear if Showing terms of use is activated. For detailed information, please refer to the separate manual of the web application.

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.

6. Click on **Login**.
7. Click on **Config Panel 21**.
8. In the menu, click on **Matrix systems > [Name] > Matrix.**
9. Click on the device you want to configure and then click on **Configuration**.
10. Click on the tab **Network**.
11. Go to the paragraph **Interfaces**.
12. Use the **Interface A** and/or **Interface B** paragraphs to enter the following data:

Operational mode:	Use the pull-down menu to select the operational mode of **Interface A** or **Interface B**: ▪ **Off:** switch network interface off. ▪ **Static:** a static IP address is being assigned. ▪ **DHCP:** obtains the IP address from a DHCP server.
IP address:	Only when the *Static* operating mode has been selected: Enter the interface IP address.

IMPORTANT: The IP address *192.168.0.1* should **not** be used on the *ControlCenter-IP*. As this IP address is also used as standard IP address for the network management interfaces of the KVM-over-IP end devices, conflicts may otherwise occur during communication. If possible, select an IP address in a different subnet.

IMPORTANT: It is not possible to use both network interfaces within the same subnet!

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:	Only when the *Static* operating mode has been selected: Enter the network netmask.

13. Enter the following data in the section **Global network settings**:

Operational mode:	Select the desired operational mode: ▪ **Static:** use static settings. ▪ **DHCP:** obtain the settings from a DHCP server.
Hostname:	Enter the hostname of the device.
Domain:	Enter the domain to which the device is to be assigned to.
Gateway:	Enter the gateway IP address.
DNS-Server 1:	Enter the DNS server IP address.
DNS-Server 2:	Optionally, enter the IP address of another DNS server.

14. Click **Save**.

15. Click the **user icon** at the top right and then click **Logout**.

16. Remove the twisted pair cable between the computer and the computer or the IP matrix switch.

17. Integrate the IP matrix switch into the local network.

Resetting the netfilter rules

In the default settings, all network computers can access the system's IP address (open system access).

With the web application, you can create netfilter rules to control the access to the matrix system. 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:

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Press **F11** to call the *Configuration* menu.
3. Select the **System** entry and press **Enter**.
4. Select the **Reset netfilter configuration** entry and press **Enter**.
5. Use the arrow keys to select **Yes** and press **Enter** to respond to the prompt for confirmation.

Basic configuration of the KVM-over-IP™ connection

This section explains the settings required for start-up the IP matrix switch.

NOTE: All settings of the KVM-over-IP™ connection are described in detail in the documentation of the web application of the IP matrix switch.

Adding end devices

Compatible devices can be automatically searched for and added by the IP matrix switch.

The KVM-over-IP™ connection of the end device is automatically configured by the IP matrix switch and is then immediately ready for operation.

NOTE: Alternatively, you can set up the initial KVM-over-IP™ connection of each end device manually, as described in the chapter *Establishing a KVM-over-IP™ connection for the first time* of the end device manuals.

How to add (more) end devices:

1. Start the computer's web browser and enter the URL in the address line.

   https://[IP address of the device]

2. 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.

NOTE: The *Terms* field and the *Accept* field only appear if Showing terms of use is activated. For detailed information, please refer to the separate manual of the web application.

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**.
4. Click on **Config Panel 21**.
5. In the menu, click on **Matrix systems > [Name] > Matrix.**
6. Click on **Add end devices** on the context menu.

   The table *Device detector* shows you the following information about the devices found:

Name:	List of end devices, which can be added to the IP matrix switch.
IP transmission:	IP address of the *transmission* interface
IP management:	IP address of the *management* interface
MAC transmission:	MAC address of the *transmission* interface
MAC management:	MAC address of the *management* interface
UID:	physical ID of the device
Status:	Display whether the device is generally **available** for adding to this matrix switch or already **occupied**.

7. Activate the **Add** slider in the row of each device you want to add to the IP matrix switch.

> **ADVICE:** To add all allowed devices to the IP matrix switch at the same time, select the check box in the column header of the **Add** column.

> **NOTE:** You can also click **Add manually** to manually enter the host name of a device to be added or the IP address range of several devices to be added.

8. Click on **Save**.

Unpair an end device

How to unpair an end device:

1. Start the computer's web browser and enter the URL in the address line.

   https://[IP address of the device]

2. 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.

NOTE: The *Terms* field and the *Accept* field only appear if Showing terms of use is activated. For detailed information, please refer to the separate manual of the web application.

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**.
4. Click on **Config Panel 21**.
5. In the menu, click on **Matrix systems > [Name] > Console modules**, **Computer modules** or **RemoteGateways**.
6. Select the end device to be unpaired.

   ADVICE: Multiple selection of devices is possible.

7. Click on **Unpair device**.

Determination of the type of video transmission

In the default setting, the computer modules (**IP-CPU**) send the video streams via multicast to the console modules (**IP-CON**).

This option allows users with »MultiAccess« right to connect to a computer to which *another* user is already connected.

> **IMPORTANT:** The multicast streams are controlled by the network switches and enable efficient distribution of the streams to multiple recipients at the same time.
>
> Please note the requirements for the *network switch* for sending the video streams via multicast. Refer to the Installation Guide for detailed information.

Alternatively, you can specify that the computer modules (**IP-CPU**) send the video streams via *unicast* to the console modules (**IP-CON**).

The connection of a user to a computer to which another user is already connected is *not* possible in this mode (message: **No multicast video**)!

> **NOTE:** If *multicast* transmission is not used, the network switch will have to meet considerably fewer requirements (see page 12 ff.).
>
> The following requirements and settings of the network switch listed above do not apply in this case:
>
> *Multicast*, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* and *Spanning Tree TCN Flooding*.

You can define the type of video transmission system-wide. The system-wide setting is applied by default by all computer modules. In addition, you can specify the type of video transmission individually for each computer module.

How to configure the system-wide multicast or unicast video transmission setting:

1. Press the **Ctrl**+**Num** (*default*) hotkey to open the on-screen display (OSD).
2. Press **F11** to call the **Configuration** menu.
3. Select the **System** entry and press **Enter**.

4. Select the **Multicast video** entry and press **F8** to select one of the following options:

on:	By default, the computer modules (**IP-CPU**) send the video stream via *multicast* to the console modules (**IP-CON**). This option (*standard*) allows users with »MultiAccess« right to connect to a computer to which *another* user is already connected.
off:	The computer modules (**IP-CPU**) send the video stream via *unicast* to the console modules (**IP-CON**) by default. The connection of a user to a computer to which another user is *already* connected is *not* possible in this mode (message: **No multicast video**)!

5. Press **F2** to save your settings.

IMPORTANT: The selected setting is only applied when a new connection is established. Existing connections are retained unchanged.

How to configure the individual multicast or unicast video transmission settings of a computer module:

1. Press the **Ctrl+Num** (*default*) hotkey to open the OSD.
2. Press **F11** to call the **Configuration** menu.
3. Select the **Target** entry and press **Enter**.
4. Select the computer module you want to configure and press **F5**.

ADVICE: Use the menu's *search function*, the *view filter* or the *sort criteria* to limit the selection of list entries.

5. Select the **Multicast video** entry and press **F8** to select one of the following options:

system:	Apply system-wide setting (see above).
on:	This computer module (**IP-CPU**) sends the video stream via multicast to other console modules (**IP-CON**). This option allows users with »MultiAccess« right to connect to this computer, even if *another* user is already connected.
off:	This computer module (**IP-CPU**) sends the video stream via unicast to other console modules (**IP-CON**). It is not possible to connect a user to this computer if *another* user is already connected (message: **No multicast video**).

6. Press **F2** to save your settings.

IMPORTANT: The selected setting is only applied when a new connection is established. Existing connections are retained unchanged.

Restricting KVM-over-IP counterparts (UID locking)

By default, *each* IP matrix, *each* console module and *each* computer module is allowed to establish a KVM-over-IP connection to the matrix switch.

ADVICE: Activate the function **UID locking** if you want to *specify* which counterparts should be able to connect to the matrix switch.

How to enable/disable UID locking:

1. In the menu, click on **Matrix systems > [Name] > Matrix.**
2. Click on the device you want to configure and then click on **Configuration**.
3. Click on the tab **KVM connection**.
4. Enter your setting in the paragraph **UID locking**:

UID locking:	Only the counterparts specified in the list may establish a KVM-over-IP connection (**Enabled**), or all counterparts may establish a connection (**Disabled**).
Connected device UIDs:	If UID locking is switched on, activate the **Permitted** slider in the line of each device that is allowed to establish a connection to the matrix switch.
Add computer module:	Click this button and enter the UID of the computer module that is allowed to connect to this matrix switch. Click on **Save**.
Add console module:	Click this button and enter the UID of the console module that is allowed to connect to this matrix switch. Click on **Save**.
Add RemoteAccess-IP-CPU:	Click this button and enter the UID of the computer module that is allowed to connect to this matrix switch. Click on **Save**.
Add IP matrix:	Click this button and enter the UID of the IP matrix that is allowed to connect to this matrix switch. Click on **Save**.
Remove:	Click on a permitted counterpart and then on **Remove** to revoke the permission.

5. Click on **Save**.

Reset button

The *Reset* button is placed on the front panel of the IP matrix switch. This button allows you to reset the default settings and disable the netfilter rules.

NOTE: To prevent you from pressing the button by accident, it is placed behind a hole in the front panel (between the power and status LEDs).

You are required to use a thin, pointed object for pressing the button.

Resetting the default settings

Pressing and holding the button during the booting process resets the default settings of the IP matrix switch.

NOTE: After the function has been carried out, the default settings of the IP matrix switch do apply again. However, the purchased premium functions remain unaltered.

How to reset the default settings of the IP matrix switch:

1. Turn off both power packs of the IP matrix switches.
2. Press and hold the *Reset* button on the front panel of the device.
3. Keep the button pressed and turn the device on.
4. Release the button when the green *Status*-LED starts blinking.

NOTE: You can also use the *Config Panel* web application to reset the default settings.

Disabling the netfilter rules temporarily

In the default status of the IP matrix switch, all network computers have access to the extender's IP address (open system access).

The web application enables you to create netfilter rules to control the access to the device. If a netfilter rule is created, the open access to the system is disabled and all incoming data packets are compared to the netfilter rules.

If the currently adjusted netfilter rules prevent access to the *Config Panel* web application, they can be can temporarily disabled in order to be edited.

How to disable the netfilter rules temporarily:

1. If necessary, switch on the central module and wait until the device is ready for operation.
2. Press and hold the *Reset* button on the front panel of the device for 5 seconds.

   IMPORTANT: Now, the open system access is enabled.

3. Use the *Config Panel* web application to edit the netfilter rules that are stored in the appliance and, afterwards, save these rules.

   IMPORTANT: The former settings are reactivated if no new netfilter rules are created within 15 minutes.

Status displays

LEDs at the front panel

The LEDs on the front panel of the IP matrix switch show the system's operating status:

Section	LED	Status	Meaning
Power	**Red.**	on	The power pack is turned on and supplies the required voltage.
		off	The power pack is turned off or the connection to the mains could not be established.
	Main	on	The power pack is turned on and supplies the required voltage.
		off	The power pack is turned off or the connection to the mains could not be established.
Status	**Ready**	blinking	Device is ready for operation or is being booted.
		off	Defective internal communication.
	System	green	Device is ready for operation.
		blinking green	Restoring the default settings after pressing the reset button
		red	The device is not ready for operation.
		off	Defective internal communication.
	Fail	on	The device is not ready for operation.
		off	The device is ready for operation or switched off.
	Ident.	on	The LED to identify the device in the web application is activated.
		off	The device is ready for operation or turned off.

LEDs at the back panel

The back panel of the IP matrix switch provides additional status LEDs. The LEDs have the following function:

Interface	LED	Status	Meaning
Status	**System**	on	Device is ready for operation.
		off	Defective internal communication.
	Fail	on	The device is not ready for operation.
		off	The device is ready for operation or switched off.
	Ready	blinking	Device is ready for operation or is being booted.
		off	Defective internal communication.
	Ident.	on	The LED to identify the device in the web application is activated.
Network A	**left**	flickering (green)	Activity at network interface
		off	No activity at network interface
	right	on (green)	Network connection (10M/100M/1G) established
		off	No network connection
Network B	**left**	flickering (green)	Activity at network interface
		off	No activity at network interface
	right	on (green)	Network connection (10M/100M/1G) established
		off	No network connection

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

CONTROLCENTER-IP 2.0 SERIES		
Interfaces	Network connection:	2 × RJ45 socket (10 MBit/s, 100 MBit/s, 1 Gbit/s)
	Service:	1 × Mini-USB socket (Typ B)
	USB 2.0	2 × USB-A socket
Main power supply	Type:	internal power pack
	Connector:	1 × IEC plug(IEC-320 C14)
	Current consumption:	100-240VAC/60-50Hz, 0.7-0.4A
Redundant power supply	Type:	internal power pack
	Connector:	1 × IEC plug(IEC-320 C14)
	Current consumption:	100-240VAC/60-50Hz, 0.7-0.4A
Housing	Material:	anodised aluminium
	Dimensions (W × H × D):	approx. 436 × 44 × 210 mm
	IP protection class:	IP20
	Weight:	approx. 2 kg
Operational environment	Temperature:	+5 °C to +45 °C
	Air humidity:	20% to 80%, non-condensing
Storage environment	Temperature:	-20 °C to +55 °C
	Air humidity:	15% to 85%, non-condensing
Conformity		CE, UKCA, FCC class B, TAA, EAC, RoHS, WEEE, REACH

NOTES

NOTES

NOTES

G&D. FEELS RIGHT.

Hauptsitz | Headquarter

Guntermann & Drunck GmbH Systementwicklung

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

US-Büro | US-Office

G&D North America Inc.

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