



G&D RemoteAccess-IP-CPU

DE Installationsanleitung

EN Installation Guide



Zu dieser Dokumentation

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

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

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

Gewährleistungsausschluss

G&D übernimmt keine Gewährleistung für Geräte, die

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

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

Warenzeichennachweis

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

Impressum

© Guntermann & Drunck GmbH 2025. Alle Rechte vorbehalten.

Version 1.30 – 05.09.2025

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

Die in diesem Handbuch genannten Geräte erfüllen Teil 15 der FCC-Bestimmungen. Für den Betrieb gelten die folgenden Bedingungen: (1) die Geräte dürfen keine schädlichen Störungen erzeugen und (2) die Geräte müssen alle empfangenen Störungen aufnehmen, einschließlich Störungen, die den Betrieb beeinträchtigen.

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

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

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

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

Inhaltsverzeichnis

Sicherheitshinweise	1
Das Rechnermodul	
»RemoteAccess-IP-CPU«	5
Das Rechnermodul	
»RemoteAccess-IP-CPU-Fiber«	13
Ersteinrichtung der KVM-over-IP™-Verbindung	23
Grundlegende Bedienung der Webapplikation	30
Konfiguration der Network-Schnittstelle	32
Bedienung über das IP-Matrixsystem	32

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 waagerechte, horizontale Einbauweise zulässig. Ein senkrechter, vertikaler Einbau ist nur mit passenden Geräteträgern von G&D zulässig.

Keine Gegenstände durch die Öffnungen des Geräts stecken

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

Stolperfallen vermeiden

Vermeiden Sie bei der Verlegung der Kabel Stolperfallen.

Geerdete Spannungsquelle verwenden

Betreiben Sie dieses Gerät nur an einer geerdeten Spannungsquelle.

Verwenden Sie ausschließlich die G&D-Netzteile

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

Keine mechanischen oder elektrischen Änderungen am Gerät vornehmen

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

Geräteabdeckung nicht entfernen

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

Betreiben Sie das Gerät ausschließlich im vorgesehenen Einsatzbereich

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

Hinweise zum Umgang mit Lithium-Knopfzellen

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

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

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

Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

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

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

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

Check local regulations for the disposal of electronic products.

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

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

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

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

Besondere Hinweise zum Umgang mit Laser-Technologie

Die Fiber-Varianten der **RemoteAccess-IP-CPU-Serie** verwenden Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 oder besser entsprechen.

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

LASER KLASSE 1 EN 60825-1:2014	Unsichtbare Laserstrahlung, nicht direkt mit optischen Instrumenten betrachten	Complies with 21 CFR 1040.10 and 1040.11
Class 1 Laser Product EN 60825-1:2014	Invisible laser beam, avoid direct eye exposure with optical instruments	Complies with 21 CFR 1040.10 and 1040.11
Produit laser de classe 1 EN 60825-1:2014	Laser invisible, évitez l'exposition directe des yeux avec des instruments optiques	Est conforme à 21 CFR 1040.10 et 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.

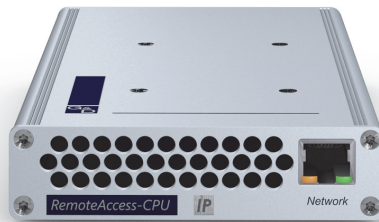
Das Rechnermodul »RemoteAccess-IP-CPU«

Mit dem Rechnermodul **RemoteAccess-IP-CPU** integrieren Sie über ein Netzwerk erreichbare virtuelle Computer in einen IP-Matrixswitch *ControlCenter-IP* oder *ControlCenter-IP-XS*.

Die Netzwerkverbindung mit den virtuellen Computern kann wahlweise über das **SSH**-, **VNC** -oder **RDP**-Protokoll erfolgen.

Zudem können Streams auch über die Transportprotokolle **RTP/TCP**, **RTSP/TCP** und **MMSH** empfangen werden. Hierbei werden die Codecs **H.265**, **H.264**, **VP8** und **VP9** für das Dekodieren von Videodaten sowie **MPGA**, **MP3** und **AC3** für das Dekodieren von Audiodaten unterstützt.

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **RemoteAccess-Streaming-Features** ist Voraussetzung für die Nutzung eines Streaming-Protokolls (siehe *Freischaltung kostenpflichtiger Zusatzfunktionen* auf Seite 31).



Nach der Konfiguration einer beliebigen Anzahl an virtuellen Computern kann der Zugriff auf einen der virtuellen Computer direkt über das IP-Matrixsystem erfolgen.

HINWEIS: Jedes Rechnermodul **RemoteAccess-IP-CPU** kann *eine* Verbindung zu einem virtuellen Computer herstellen.

Falls mehrere, *gleichzeitige* Verbindungen zu verschiedenen virtuellen Computern innerhalb des IP-Matrixsystems erforderlich sind, benötigen Sie die entsprechende Anzahl an Rechnermodulen der **RemoteAccess-IP-CPU**-Serie.

Die virtuellen Computer werden, wie auch die weiteren Targets, in das OSD und Bedienkonzept des Matrixswitches integriert: Sie schalten sich daher wie üblich über das **Select**-Menü im OSD auf einen virtuellen Computer auf und können auch Komfortfunktionen wie *Push-Get*, *Multi-User-Zugriff* oder *CrossDisplay-Switching* mit den virtuellen Computern benutzen.

Die Netzwerkverbindung zu den virtuellen Computern erfolgt über eine Ethernet-Netzwerkschnittstelle (idealerweise: Gigabit-Ethernet).

WICHTIG: Die Dauer des Verbindungsaufbaus sowie die Performance der Verbindung zum virtuellen Computer hängen maßgeblich von der Geschwindigkeit und Qualität der Netzwerkverbindung zum virtuellen Computer ab!

Die maximal darstellbare Desktop-Auflösung des virtuellen Computers beträgt 2560×1600 Bildpunkte. Stellen Sie sicher, dass sowohl das eingesetzte Arbeitsplatzmodul als auch der Monitor die gewünschte Auflösung unterstützen.

Über das RDP-Protokoll wird die Übertragung des Embedded-Audio-Signals via DisplayPort™-Kabel unterstützt. Verwenden Sie zur Wiedergabe des Embedded-Audio-Signals ein kompatibles DisplayPort-Arbeitsplatzmodul und einen kompatiblen Monitor.

Lieferumfang

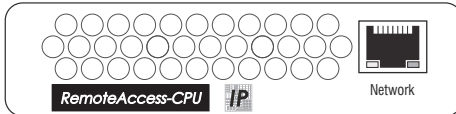
- 1 × Rechnermodul **RemoteAccess-IP-CPU**
- 1 × Netzteil (12V/2A, nur bei Varianten incl. PowerPack)
- 1 × Stromversorgungskabel (nur bei Varianten incl. PowerPack)
- 1 × Sicherheitshinweise-Flyer

Installation

HINWEIS: Platzieren Sie das Rechnermodul ausschließlich aufrecht (s. Skizze unten) oder um 90° nach links bzw. rechts geneigt.

HINWEIS: Der Lüfter saugt vorne die Außenluft in das Gerät. An den hinteren Lüftungsöffnungen wird die warme Luft ausgestoßen.

Anschluss des Computers

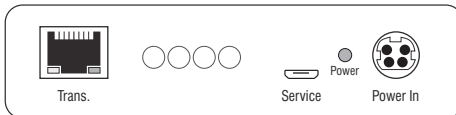


Network: Stecken Sie ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5e (oder höher) ein.

Das andere Ende des Kabels ist mit dem Netzwerk (Gigabit-Ethernet) zu verbinden.

WICHTIG: Stellen Sie sicher, dass alle virtuellen Computer über diese Schnittstelle erreichbar sind.

Verbindung zum Matrixswitch



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

Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

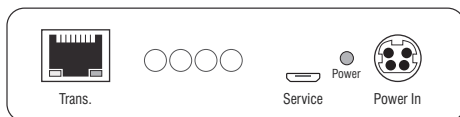
WICHTIG: Über diese Schnittstelle erfolgt die Übertragung der KVM-Daten vom und zum IP-Matrixswitch.

Stromversorgung

Power In: Stecken Sie das Anschlusskabel des Netzteils in diese Schnittstelle. Verbinden Sie das Stromversorgungskabel mit dem Netzteil und einer Netzsteckdose.

Service-Schnittstelle

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



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

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

So richten Sie eine Verbindung im Terminalemulationsprogramm ein:

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

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

Der Treiber steht auf der Website www.gdsys.com/de im Bereich **Service > 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 *GDMan 2.01b* zu verbinden.

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

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

Statusanzeigen

Die Power-LED an der Rückseite des Rechnermoduls signalisiert den Status der Stromversorgung und hilft mit der Ident.-LED-Funktion beim Auffinden des Geräts in großen Installationen:

LED	Status	Bedeutung
Power	leuchtet grün	Das externe Netzteil ist angeschlossen und eine Spannung von 12 Volt verfügbar.
	leuchtet blau	Das externe Netzteil ist angeschlossen und eine Spannung von 12 Volt verfügbar. Die Ident.-LED zum schnellen Identifizieren des Geräts wurde (beispielsweise über die Webapplikation) aktiviert.
	aus	Das externe Netzteil ist nicht (korrekt) angeschlossen.

Das Blinken der Transmission-LEDs an der Rückseite signalisiert folgende Betriebszustände der jeweiligen Verbindung:

LED	Status	Bedeutung
links	aus	Verbindung zur Gegenstelle nicht hergestellt
	leuchtet gelb	Kommunikation mit G&D Gegenstelle hergestellt
	blinkt gelb	Verbindung zu einer Gegenstelle hergestellt
rechts	aus	kein Endgerät aufgeschaltet
	leuchtet grün	Endgerät aufgeschaltet

Das Blinken der Network-LEDs an der Vorderseite signalisiert folgende Betriebszustände der jeweiligen Verbindung:

LED	Status	Bedeutung
links	aus	keine Netzwerkaktivität
	leuchtet gelb	Netzwerkverbindung aufgebaut
	flackert gelb	Netzwerkaktivität findet statt
rechts	aus	keine Netzwerkverbindung
	leuchtet grün	Netzwerkverbindung aufgebaut
	leuchtet gelb	Nur bei älteren Hardware-Versionen wird differenziert: Netzwerkverbindung mit 10 oder 100 Mbit/s aufgebaut (leuchtet grün: Netzwerkverbindung mit 1 Gbit/s aufgebaut)

Technische Daten

REMOTEACCESS-IP-CPU		
Video	unterstützte Auflösungen:	▪ 2560×1600/60Hz/VESA CVT-RB ▪ 2560×1440/60Hz/VESA CVT-RB ▪ 1920×1200/60Hz/VESA CVT-RB ▪ 1920×1080x60Hz/CTA-861-D ▪ 1600×1200/60Hz/VESA DMT ▪ 1680×1050/60Hz/VESA CVT ▪ 1280×1024/60Hz/VESA DMT ▪ 1024×768/60Hz/VESA DMT
	Farbtiefe:	24 Bit
	Videobandbreite:	25 bis 330 MP/s
Audio » DisplayPort Digital	Übertragungsart:	2-Kanal-LPCM, stereo
	Auflösungen:	16/20/24 bit
	Abtastraten:	bis 48 kHz
Datenübertragung zur Gegenstelle	Schnittstelle:	1 × RJ45-Buchse (1 GBit/s - IEEE 802.3ab)
	Übertragungslänge:	max. 100 Meter (Cat 5e, Cat 6a)
Datenübertragung zu den Terminalservern	Schnittstelle:	1 × RJ45-Buchse
	Datenraten:	10 MBit/s, 100 MBit/s, 1000 MBit/s
	unterstützte Protokolle:	SSH, RDP, VNC
Streaming (<i>optionales kostenpflichtiges Feature</i>)	Datenrate:	bis 4 MBit/s
	unterstützte Protokolle:	RTP/TCP, RTSP/TCP, MMSH
	unterstützte Codecs zum Dekodieren von Videodaten:	H.264, VP8, VP9
	unterstützte Auflösungen:	bis 1920×1080x30Hz (Full HD/30Hz)
	unterstützte Codecs zum Dekodieren von Audiodaten:	MPGA, MP3, AC3
Generic USB » nur bei UG-Varianten Unterstützung von bis zu 4 Geräten; das eingesetzte Arbeitsplatzmodul muss die entsprechende Anzahl an Geräten unterstützen	Spezifikation:	USB 2.0
	USB-Klassen:	Human Interface Devices (HID)
	Übertragungsrate:	max. 8,5 Mbit/s
Stromversorgung	Typ:	Tischnetzteil (12V/2A)
	Anschluss:	1 × Mini-DIN 4-Buchse
	Stromaufnahme:	max. 1,2 A

REMOTEACCESS-IP-CPU		
Gehäuse	Material:	Aluminium eloxiert
	Maße (B × H × T):	105 × 26 × 184 mm
	IP-Schutzklasse:	IP20
	Gewicht:	ca. 400 g
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	

Das Rechnermodul »RemoteAccess-IP-CPU-Fiber«

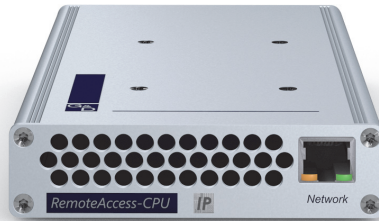
Mit dem Rechnermodul **RemoteAccess-IP-CPU-Fiber** integrieren Sie über ein Netzwerk erreichbare virtuelle Computer in einen IP-Matrixswitch *ControlCenter-IP* oder *ControlCenter-IP-XS*.

WICHTIG: Das Rechnermodul und die Fiber-Ports sind als *Singlemode*- sowie als *Multimode*-Varianten verfügbar. Stellen Sie sicher, dass alle Komponenten sowie der Lichtwellenleiter zueinander kompatibel sind.

Die Netzwerkverbindung mit den virtuellen Computern kann wahlweise über das **SSH**-, **VNC** -oder **RDP**-Protokoll erfolgen.

Zudem können Streams auch über die Transportprotokolle **RTP/TCP**, **RTSP/TCP** und **MMSH** empfangen werden. Hierbei werden die Codecs **H.265**, **H.264**, **VP8** und **VP9** für das Dekodieren von Videodaten sowie **MPGA**, **MP3** und **AC3** für das Dekodieren von Audiodaten unterstützt.

WICHTIG: Die Freischaltung des kostenpflichtig erhältlichen **RemoteAccess-Streaming-Features** ist Voraussetzung für die Nutzung eines Streaming-Protokolls (siehe *Freischaltung kostenpflichtiger Zusatzfunktionen* auf Seite 31).



Nach der Konfiguration einer beliebigen Anzahl an virtuellen Computern kann der Zugriff auf einen der virtuellen Computer direkt über das IP-Matrixsystem erfolgen.

HINWEIS: Jedes Rechnermodul **RemoteAccess-IP-CPU** kann *eine* Verbindung zu einem virtuellen Computer herstellen.

Falls mehrere, *gleichzeitige* Verbindungen zu verschiedenen virtuellen Computern innerhalb des IP-Matrixsystems erforderlich sind, benötigen Sie die entsprechende Anzahl an Rechnermodulen der **RemoteAccess-IP-CPU**-Serie.

Die virtuellen Computer werden, wie auch die weiteren Targets, in das OSD und Bedienkonzept des Matrixswitches integriert: Sie schalten sich daher wie üblich über das **Select**-Menü im OSD auf einen virtuellen Computer auf und können auch Komfortfunktionen wie *Push-Get*, *Multi-User-Zugriff* oder *CrossDisplay-Switching* mit den virtuellen Computern benutzen.

Die Netzwerkverbindung zu den virtuellen Computern erfolgt über eine Ethernet-Netzwerkschnittstelle (idealerweise: Gigabit-Ethernet).

WICHTIG: Die Dauer des Verbindungsaufbaus sowie die Performance der Verbindung zum virtuellen Computer hängen maßgeblich von der Geschwindigkeit und Qualität der Netzwerkverbindung zum virtuellen Computer ab!

Die maximal darstellbare Desktop-Auflösung des virtuellen Computers beträgt 2560×1600 Bildpunkte. Stellen Sie sicher, dass sowohl das eingesetzte Arbeitsplatzmodul als auch der Monitor die gewünschte Auflösung unterstützen.

Über das RDP-Protokoll wird die Übertragung des Embedded-Audio-Signals via DisplayPort™-Kabel unterstützt. Verwenden Sie zur Wiedergabe des Embedded-Audio-Signals ein kompatibles DisplayPort-Arbeitsplatzmodul und einen kompatiblen Monitor.

Lieferumfang

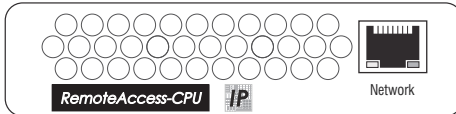
- 1 × Rechnermodul **RemoteAccess-IP-CPU-Fiber**
- 1 × Netzteil (12V/2A, nur bei Varianten incl. PowerPack)
- 1 × Stromversorgungskabel (nur bei Varianten incl. PowerPack)
- 1 × Sicherheitshinweise-Flyer

Installation

HINWEIS: Platzieren Sie das Rechnermodul ausschließlich aufrecht (s. Skizze unten) oder um 90° nach links bzw. rechts geneigt.

HINWEIS: Der Lüfter saugt vorne die Außenluft in das Gerät. An den hinteren Lüftungsöffnungen wird die warme Luft ausgestoßen.

Anschluss des Computers



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

Das andere Ende des Kabels ist mit dem Netzwerk (Gigabit-Ethernet) zu verbinden.

WICHTIG: Stellen Sie sicher, dass alle virtuellen Computer über diese Schnittstelle erreichbar sind.

Verbindung zum Matrixswitch

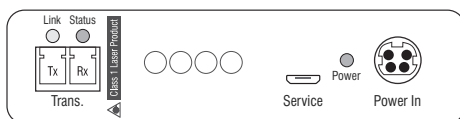
WICHTIG: Die Geräte verwenden Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 entsprechen.

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

Beachten Sie diesbezüglich folgende Sicherheitshinweise:

- *Blickkontakt mit dem unsichtbaren Laserstrahl vermeiden* auf Seite 4
- *Optische Anschlüsse stets verbinden oder mit Schutzkappen abdecken* auf Seite 4
- *Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden* auf Seite 4

HINWEIS: Verwenden Sie für die Kabelverbindungen als Zubehör erhältliche Lichtwellenleiter mit LC-Steckern.



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

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

WICHTIG: Über diese Schnittstellen erfolgt die Übertragung der KVM-Daten vom und zum IP-Matrixswitch.

Stromversorgung

Power In: Stecken Sie das Anschlusskabel des Netzteils in diese Schnittstelle. Verbinden Sie das Stromversorgungskabel mit dem Netzteil und einer Netzsteckdose.

Service-Schnittstelle

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



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

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

So richten Sie eine Verbindung im Terminalemulationsprogramm ein:

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

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

Der Treiber steht auf der Website www.gdsys.com/de im Bereich **Service > 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 *GDMan 2.01b* zu verbinden.

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

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

Statusanzeigen

Die Power-LED an der Rückseite des Rechnermoduls signalisiert den Status der Stromversorgung und hilft mit der Ident.-LED-Funktion beim Auffinden des Geräts in großen Installationen:

LED	Status	Bedeutung
Power	leuchtet grün	Das externe Netzteil ist angeschlossen und eine Spannung von 12 Volt verfügbar.
	leuchtet blau	Das externe Netzteil ist angeschlossen und eine Spannung von 12 Volt verfügbar. Die Ident.-LED zum schnellen Identifizieren des Geräts wurde (beispielsweise über die Webapplikation) aktiviert.
	aus	Das externe Netzteil ist nicht (korrekt) angeschlossen.

Das Blinken der Transmission-LEDs an der Rückseite signalisiert folgende Betriebszustände der jeweiligen Verbindung:

LED	Status	Bedeutung
links	aus	Verbindung zur Gegenstelle nicht hergestellt
	leuchtet gelb	Kommunikation mit der Gegenstelle hergestellt
	blinkt gelb	nur Rx-Verbindung zur Gegenstelle hergestellt
	blinkt schnell gelb	inkompatibles SFP-Modul eingesteckt
rechts	aus	an Gegenstelle nicht angemeldet
	leuchtet grün	an Gegenstelle angemeldet

Das Blinken der Network-LEDs an der Vorderseite signalisiert folgende Betriebszustände der jeweiligen Verbindung:

LED	Status	Bedeutung
links	aus	keine Netzwerkaktivität
	leuchtet gelb	Netzwerkverbindung aufgebaut
	flackert gelb	Netzwerkaktivität findet statt
rechts	aus	keine Netzwerkverbindung
	leuchtet grün	Netzwerkverbindung aufgebaut
	leuchtet gelb	Nur bei älteren Hardware-Versionen wird differenziert: Netzwerkverbindung mit 10 oder 100 Mbit/s aufgebaut (leuchtet grün: Netzwerkverbindung mit 1 Gbit/s aufgebaut)

Technische Daten

REMOTEACCESS-IP-CPU-FIBER		
Video	unterstützte Auflösungen:	▪ 2560×1600/60Hz/VESA CVT-RB ▪ 2560×1440/60Hz/VESA CVT-RB ▪ 1920×1200/60Hz/VESA CVT-RB ▪ 1920×1080x60Hz/CTA-861-D ▪ 1600×1200/60Hz/VESA DMT ▪ 1680×1050/60Hz/VESA CVT ▪ 1280×1024/60Hz/VESA DMT ▪ 1024×768/60Hz/VESA DMT
	Farbtiefe:	24 Bit
	Videobandbreite:	25 bis 330 MP/s
Audio ▸ DisplayPort Digital	Übertragungsart:	2-Kanal-LPCM, stereo
	Auflösungen:	16/20/24 bit
	Abtastraten:	bis 48 kHz
Datenübertragung zur Gegenstelle	Schnittstelle:	1 × LC-Duplex-Buchse
	Übertragungslänge:	▸ RemoteAccess-IP-CPU-Fiber(M) max. 220 Meter (62,5/125µm 160 MHz*km), max. 275 Meter (62,5/125µm 200 MHz*km OM1), max. 500 Meter (50/125µm 400 MHz*km OM2), max. 550 Meter (50/125µm 500 MHz*km OM2) ▸ RemoteAccess-IP-CPU-Fiber(S) max. 10.000 Meter (9/125µm 500 MHz*km OS1)
Datenübertragung zu den Terminalservern	Schnittstelle:	1 × RJ45-Buchse
	Datenraten:	10 MBit/s, 100 MBit/s, 1000 MBit/s
	unterstützte Protokolle:	SSH, RDP, VNC
Streaming (optionales kostenpflichtiges Feature)	Datenrate:	bis 4 MBit/s
	unterstützte Protokolle:	RTP/TCP, RTSP/TCP, MMSH
	unterstützte Codecs zum Dekodieren von Videodaten:	H.264, VP8, VP9
	unterstützte Auflösungen:	bis 1920×1080x30Hz (Full HD/30Hz)
	unterstützte Codecs zum Dekodieren von Audiodaten:	MPGA, MP3, AC3
Generic USB ▸ nur bei UG-Varianten Unterstützung von bis zu 4 Geräten; das eingesetzte Arbeitsplatzmodul muss die entsprechende Anzahl an Geräten unterstützen	Spezifikation:	USB 2.0
	USB-Klassen:	Human Interface Devices (HID)
	Übertragungsrate:	max. 8,5 Mbit/s

REMOTEACCESS-IP-CPU-FIBER		
Stromversorgung	Typ:	Tischnetzteil (12V/2A)
	Anschluss:	1 × Mini-DIN 4-Buchse
	Stromaufnahme:	max. 1,2 A
Gehäuse	Material:	Aluminium eloxiert
	Maße (B × H × T):	105 × 26 × 184 mm
	IP-Schutzklasse:	IP20
	Gewicht:	ca. 400 g
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	

Ersteinrichtung der KVM-over-IP™-Verbindung

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

HINWEIS: Die **Transmission**-Schnittstelle des Rechnermoduls wird für die Signalübertragung zwischen dem Rechnermodul und dem IP-Matrixswitch verwendet.

Die **Network**-Schnittstelle wird für die Kommunikation mit den virtuellen Computern verwendet.

Der Zugriff auf die Webapplikation des Rechnermoduls ist über beide Schnittstellen möglich.

Erst nach der Ersteinrichtung der KVM-over-IP™-Verbindung zwischen dem Rechnermodul und dem IP-Matrixswitch kann das Rechnermodul mit dem IP-Matrixswitch verwendet werden.

Im Auslieferungszustand ist folgende Einstellung der *Transmission*-Schnittstelle voreingestellt:

- IP-Adresse der *Transmission*-Schnittstelle:
Bezug der Adresse via **DHCPv4** (Fallback: IP-Adresse 172.17.0.10)

Im Auslieferungszustand ist folgende Einstellung der *Network*-Schnittstelle voreingestellt:

- IP-Adresse der *Network*-Schnittstelle: 192.168.0.1

Automatische Ersteinrichtung

Sie können die **KVM-over-IP™-Verbindung** komfortabel über die Webapplikation des IP-Matrixswitches einrichten (s. Abschnitt *Aufnahme von Endgeräten* im Installationshandbuch *des IP-Matrixswitches*).

HINWEIS: Die manuelle Konfiguration, wie im folgenden Abschnitt beschrieben, ist in diesem Fall *nicht* erforderlich.

Manuelle Ersteinrichtung über Direktverbindung

Falls Sie die Netzwerkverbindung vor der Integration des Rechnermoduls in das KVM-Matrixsystem vornehmen möchten, erledigen Sie dies über die eigene Webapplikation des Rechnermoduls.

Verbindung der Netzwerkschnittstelle

So verbinden Sie einen Rechner mit der Netzwerkschnittstelle des Rechnermoduls:

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

HINWEIS: Verwenden Sie beispielsweise die IP-Adresse <i>192.168.0.100</i> .
--

3. Schalten Sie das Rechnermodul ein.

Start der Webapplikation

1. Starten Sie den Webbrowser des Rechners und geben Sie in der Adresszeile die URL **192.168.0.1** ein.
2. Geben Sie in die Login-Maske folgende Daten ein:

Nutzungsbedingungen zustimmen:	Klicken Sie auf den Text, um die Nutzungsbedingungen zu lesen. Klicken Sie auf die Checkbox, um die Nutzungsbedingungen zu akzeptieren.
HINWEIS: Die Nutzungsbedingungen erscheinen nur, wenn eine entsprechende Konfiguration vorgenommen wurde. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.	
Benutzername:	Geben Sie Ihren Benutzernamen ein.
Passwort:	Geben Sie das Passwort Ihres Benutzerkontos ein.
2-Factor Auth Code (TOTP):	Geben Sie den 2-Faktor-Authentifizierungscode (TOTP) der Zwei-Faktor-Authentifizierung ein.
HINWEIS: Der 2-Faktor-Authentifizierungscode (TOTP) wird nur abgefragt, wenn die Zwei-Faktor-Authentifizierung eingerichtet und aktiviert wurde. Ausführliche Hinweise hierzu finden Sie im separaten Handbuch der Webapplikation.	

WICHTIG: Ändern Sie das voreingestellte Passwort des Administratorkontos. Melden Sie sich hierfür mit dem Administratorkonto in die Webapplikation ein und ändern Sie anschließend das Passwort.

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

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

Konfiguration der Transmission-Schnittstelle

So konfigurieren Sie die Einstellungen der *Transmission-Schnittstelle*:

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!

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

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Schnittstellen**.

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

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

6. Klicken Sie auf **Speichern**.

Konfiguration der globalen Netzwerkeinstellungen

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

So konfigurieren Sie die globalen Netzwerkeinstellungen:

1. Klicken Sie im Menü auf **RemoteGateways**.
2. Klicken Sie auf das Rechnermodul und anschließend auf **Konfiguration**.
3. Klicken Sie auf den Reiter **Netzwerk**.
4. Wählen Sie den Bereich **Globale Netzwerkeinstellungen**.
5. Erfassen Sie folgende Daten:

Betriebsmodus:	Wählen Sie den gewünschten Betriebsmodus: ▪ Statisch: Verwendung von statischen Einstellungen. ▪ Dynamisch: Zum Teil automatischer Bezug der unten beschriebenen Einstellungen von einem DHCP-Server (IPv4) oder mithilfe von SLAAC (IPv6).
Host-Name:	Geben Sie den Host-Namen des Gerätes ein.
Domäne:	Geben Sie die Domäne an, welcher das Gerät angehören soll.
Gateway IPv4:	Geben Sie die IPv4-Adresse des Gateways an.
Gateway IPv6:	Geben Sie die IPv6-Adresse des Gateways an.
DNS-Server 1:	Geben Sie die IP-Adresse des DNS-Servers an..
HINWEIS: Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das %-Zeichen hinter der link-lokalen IPv6-Adresse angefügt.	
DNS-Server 2:	Geben Sie <i>optional</i> die IP-Adresse eines weiteren DNS-Servers an..
HINWEIS: Wird eine link-lokale IPv6-Adresse eingetragen, muss die Zone-ID der Schnittstelle angegeben werden. Die Zone-ID wird abgetrennt durch das %-Zeichen hinter der link-lokalen IPv6-Adresse angefügt.	
Priorisierung von IPv6:	Klicken Sie auf den Schieberegler, falls IPv6 bevorzugt werden soll, wenn ein Ziel sowohl eine IPv6- als auch eine IPv4-Adresse hat (grün/rechts = IPv6 wird bevorzugt). Klicken Sie auf den Schieberegler, falls IPv6 nicht bevorzugt werden soll (grau/links = IPv6 wird nicht bevorzugt, <i>Standard</i>).

Verwende IPv6 Stateless Address Auto-configuration (SLAAC):	Klicken Sie auf den Schieberegler, falls SLAAC verwendet werden soll (grün/rechts = SLAAC wird verwendet, <i>Standard</i>, wenn <i>SecureCert-Feature</i> nicht aktiviert ist). Klicken Sie auf den Schieberegler, falls SLAAC nicht verwendet werden soll (grau/links = SLAAC wird nicht verwendet, <i>Standard</i> bei aktiviertem <i>SecureCert-Feature</i>).
ICMP Echo-Reply auf Echo-Request einer Multicast-/Anycast-Adresse senden (IPv6):	Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests beantwortet werden sollen (grün/rechts = Echo-Requests werden beantwortet, <i>Standard</i>). Klicken Sie auf den Schieberegler, falls ICMPv6 Echo-Requests nicht beantwortet werden sollen (grau/links = Echo-Requests werden nicht beantwortet).
ICMP-Destination-Unreachable-Nachrichten senden (IPv6):	Klicken Sie auf den Schieberegler, falls eine ICMPv6-Fehlermeldung an den Absender gesendet werden soll, wenn ein Paket nicht zugestellt werden kann (grün/rechts = Fehlermeldung wird gesendet, <i>Standard</i>). Klicken Sie auf den Schieberegler, falls keine ICMPv6-Fehlermeldungen gesendet werden sollen (grau/links = Fehlermeldung wird nicht gesendet).
Redirect-Meldungen verarbeiten (IPv6):	Klicken Sie auf den Schieberegler, falls Redirect-Meldungen akzeptiert und verarbeitet werden sollen (grün/rechts = Redirect-Meldungen werden verarbeitet, <i>Standard</i>). Klicken Sie auf den Schieberegler, falls Redirect-Meldungen nicht verarbeitet werden sollen (grau/links = Redirect-Meldungen werden nicht verarbeitet).
Duplicate Address Detection (IPv6):	Klicken Sie auf den Schieberegler, falls auf doppelte IPv6-Adressen geprüft werden soll, bevor eine Adresse verwendet wird (grün/rechts = es wird auf doppelte Adressen geprüft, <i>Standard</i>). Klicken Sie auf den Schieberegler, falls nicht auf doppelt IPv6-Adressen geprüft werden soll (grau/links = es wird nicht auf doppelte Adressen geprüft).

6. Klicken Sie auf **Speichern**.

HINWEIS: Integrieren Sie das Rechnermodul nach der erfolgreichen Einstellung der IP-Adresse in das Netzwerk des IP-Matrixswitches.

Über die Funktion **Manuell hinzufügen** des IP-Matrixswitches können Sie das Rechnermodul dem IP-Matrixswitch hinzufügen.

Grundlegende Bedienung der Webapplikation

Die Webapplikation *Config Panel* bietet eine grafische Benutzeroberfläche zur Konfiguration und Überwachung des Geräts.

Die Webapplikation kann unabhängig vom Standort des angeschlossenen Geräts im gesamten Netzwerk eingesetzt werden (siehe *Start der Webapplikation* auf Seite 25).

HINWEIS: Grundlegende Informationen zu den Systemvoraussetzungen, der erforderlichen Konfiguration der Netzwerkschnittstellen des Geräts und zum Einsatz der Webapplikation finden Sie im separaten Handbuch.

Sprache der Webapplikation auswählen

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

So ändern Sie die Sprache der Webapplikation:

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

DE

Freischaltung kostenpflichtiger Zusatzfunktionen

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

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

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

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

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

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

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

5. Klicken Sie auf **Speichern**.

Webapplikation beenden

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

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

Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die Webapplikation:

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



Konfiguration der Network-Schnittstelle

Grundlegende Voraussetzung für die Verbindung zu den virtuellen Computern ist die Konfiguration der *Network-Schnittstelle* des Gerätes.

Nach der Integration des Rechnermoduls in den IP-Matrixswitch können Sie die Konfiguration der Netzwerkschnittstelle des Moduls dort ändern (s. Anleitung der *Webapplikation des IP-Matrixswitches*).

Bedienung über das IP-Matrixsystem

Die über das Rechnermodul **RemoteAccess-IP-CPU** angebundenen, virtuellen Computer werden, wie auch die weiteren Rechnermodule, in das OSD und Bedienkonzept des IP-Matrixswitches integriert:

Sie schalten sich wie üblich über das **Auswahl**-Menü im OSD auf einen virtuellen Computer (**Remote-Target**) auf und können auch Komfortfunktionen wie *Push-Get*, *Multi-User-Zugriff* oder *CrossDisplay-Switching* mit den virtuellen Computern benutzen.

Konfiguration der Remote-Targets

Über die Webapplikation des Matrixswitches können Sie eine beliebige Anzahl an **Remote-Targets** im Bereich **Konfiguration > Matrixsysteme > [Name] > Remote-Targets** konfigurieren.

Die Konfigurationseinstellungen eines *Remote-Targets* enthalten u.a. die IP-Adresse sowie das Protokoll über das der virtuelle Computer angebunden ist.

Jedes *Remote-Target* und jedes *Remote Gateway* (Rechnermodul der **RemoteAccess-IP-CPU**-Serie) können Sie optional einem bestimmten **Remote-Pool** zuordnen.

Ein Remote-Pool gruppiert alle Remote-Targets, die über die im Pool vorhandenen Remote-Gateways erreichbar sind.

HINWEIS: Ausführliche Informationen zu diesem Thema finden Sie im Handbuch der Webapplikation des Matrixswitches.

NOTIZEN

Deutsch

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 trade-marks of the holder of rights.

© Guntermann & Drunck GmbH 2025. All rights reserved.

Version 1.30 – 05/09/2025

Guntermann & Drunck GmbH
Obere Leimbach 9
57074 Siegen

Germany

Phone +49 (0) 271 23872-0
Fax +49 (0) 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 determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Table of Contents

Safety instructions	1
»RemoteAccess-IP-CPU« computer module	5
»RemoteAccess-IP-CPU-Fiber« computer module	13
Establishing a KVM-over-IP™ connection for the first time	23
Basic operation of the web application	30
Configuration of the network interface	32
Operation via the IP matrix system	32

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, only upright, horizontal installation is permitted for devices with ventilation openings. Vertical installation is only permitted with suitable equipment from G&D.

⚠ Do not insert any objects through the device's openings

Objects should never be inserted through the device's openings. Dangerous voltage could be present. Conductive foreign bodies can cause a short circuit, which can lead to fires, electric shocks or damage to your devices.

⚠ Avoid tripping hazards

Avoid tripping hazards while laying cables.

⚠ Use earthed voltage source

Only operate this device with an earthed voltage source.

⚠ Use exclusively the G&D power pack

Only operate this device with the power packs included in delivery or listed in this operating manual.

⚠ Do not make any mechanical or electrical alternations to the device

Do not make any mechanical or electrical alternations to this device. Guntermann & Drunck GmbH is not responsible for compliance with regulations in the case of a modified device.

⚠ Do not remove device cover

The cover may only be removed by a G&D service technician. Unauthorised removal voids the guarantee. Failure to observe this precautionary measure can result in injuries and damage to the device.

⚠ Operate the device exclusively in the intended field of application

The devices are designed for indoor use. Avoid extreme cold, heat or humidity.

Instructions on how to handle Lithium button cells

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

CAUTION: Risk of explosion if the battery is replaced by an incorrect battery type. Dispose of used batteries in an environmentally friendly manner. Do not dispose of batteries in municipal waste.
Check local regulations for the disposal of electronic products.

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

ATTENTION: Il y a danger d'explosion s'il y a remplacement incorrect de la batterie. Mettre au rebut les batteries usagées conformément aux instructions du fabricant et de manière écologique. Les batteries usagées ne doivent pas être jetées dans les ordures ménagères.
Respectez les prescriptions valables pour l'élimination des produits électroniques.

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

VORSICHT: Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Batterie-Typ ersetzt wird.
Entsorgen Sie gebrauchte Batterien umweltgerecht. Gebrauchte Batterien dürfen nicht in den Hausmüll geworfen werden.
Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

Special advices for dealing with laser technology

The *fiber* variants of the **RemoteAccess-IP-CPU** series use components with laser technology which comply with laser class 1 or better.

They meet the requirements according to **EN 60825-1:2014** as well as **U.S. CFR 1040.10** and **1040.11**.

Class 1 Laser Product EN 60825-1:2014	Invisible laser beam, avoid direct eye exposure with optical instruments	Complies with 21 CFR 1040.10 and 1040.11
Produit laser de classe 1 EN 60825-1:2014	Laser invisible, évitez l'exposition directe des yeux avec des instruments optiques	Est conforme à 21 CFR 1040.10 et 1040.11
LASER KLASSE 1 EN 60825-1:2014	Unsichtbare Laserstrahlung, nicht direkt mit optischen Instrumenten betrachten	Complies with 21 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.

»RemoteAccess-IP-CPU« computer module

RemoteAccess-IP-CPU computer modules let you integrate virtual machines into a IP matrix switch *ControlCenter-IP* or *ControlCenter-IP-XS*. You can access these virtual machines via network.

To establish a network connection to virtual machines, use the **SSH**, **VNC** or **RDP** protocol.

In addition, streams can also be received via **RTP/TCP**, **RTSP/TCP** and **MMSH** transport protocols. The **H.265**, **H.264**, **VP8** and **VP9** codecs for decoding video data and **MPGA**, **MP3** and **AC3** for decoding audio data are supported.

IMPORTANT: The activation of the fee-based **RemoteAccess Streaming Feature** is prerequisite for using a streaming protocol (see *Activating premium functions* on page 31).



After configuring any number of virtual machines, you can access one of the virtual machines directly through the IP matrix system.

NOTE: Each **RemoteAccess-IP-CPU** computer module can establish *one* connection to a virtual machine.

Establishing more *simultaneous* connections to different virtual machines within the IP matrix system requires the respective number of computer modules of the **RemoteAccess-IP-CPU** series.

Like other targets, the virtual machines connected are integrated into the OSD and the operating concept of the matrix switch: As usual, you connect to a virtual machine via the **Select** menu in the OSD and can also use functions such as *push-get*, *multi-user access* or *CrossDisplay-Switching* with these virtual machines.

The network connection to the virtual machines is established via an Ethernet network interface (ideally: Gigabit Ethernet).

IMPORTANT: How long it takes to establish a connection as well as the performance of the connection to the virtual machine depends largely on the speed and quality of the network connection to the virtual machine.

The maximum desktop resolution of the virtual machine is 2560×1600 pixels. Make sure that both the console module in use and the monitor support the desired resolution.

The RDP protocol supports transmission of the embedded audio signal via DisplayPort™ cable. Use a compatible DisplayPort console module and a compatible monitor to play the embedded audio signal.

Scope of delivery

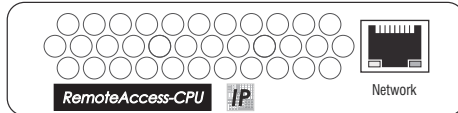
- 1 × **RemoteAccess-IP-CPU** computer module
- 1 × power pack (12V/2A, only with variants incl. PowerPack)
- 1 × power cable (only with variants incl. PowerPack)
- 1 × »Safety instructions« flyer

Installation

NOTE: Place the computer module only upright (see sketch below) or at a 90° angle to the left or right.

NOTE: The fan draws the outside air into the device *at the front*. Warm air is emitted *at the rear* ventilation openings.

Connecting a computer

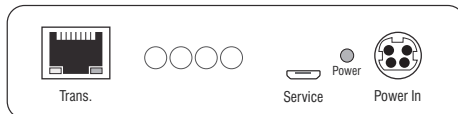


Network: Plug a category 5e (or better) twisted pair cable, which is available as accessory, into this interface.

Connect the other end of the cable with the network (Gigabit Ethernet).

IMPORTANT: Make sure that all virtual machines can be accessed via this interface.

Connection to a matrix switch



Trans.: Plug a category 5e (or better) twisted pair cable, which is available as accessory, into this interface.

Connect the other end of the Gigabit Ethernet.

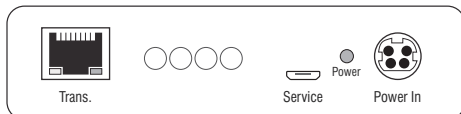
IMPORTANT: This interface is used to transfer KVM data to and from the IP matrix switch.

Power supply

Power In: Plug the connection cable of the power pack into this interface. Connect the power cable with the power pack and a power socket.

Service interface

The device has a service interface on the back panel. This interface has no relevant function for the user in normal operation.



Debug, error and status messages can be displayed in a terminal emulator (e.g. *HyperTerminal* or *PuTTY*). Via a service menu, technicians have the ability to retrieve information about the device, temporarily disable the network filter rules, reset the device to factory settings, or perform a restart.

The service menu can be operated via any terminal emulator. Use a service cable to connect the computer on which the terminal emulator is installed with the *Service* port of the device.

How to establish a connection within the terminal emulator:

NOTE: Before establishing a connection using the terminal emulator, install the device driver *CP210x USB to UART Bridge VCP*.

This driver provides the *Service* port of the device, which is connected via service cable, as virtual serial interface (COM port). Now, the virtual interface can be selected in the terminal emulator to establish the connection.

The driver is provided as download on the website www.gdsys.com/en under **Service > 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 *GDMan 2.01b*.

NOTE: To log in into the service menu, enter the user name *service* and the password *service*. The service menu is freely accessible on devices with *SecureCert* feature activated.

4. In the service menu, you have the following options:

- Quit (**not** visible on devices with *SecureCert* feature activated)
- System information
- Set system defaults: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.
- Reboot: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.
- Temporary deactivation of the network filter rules: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.

Status displays

The Power LED on the back of the computer module shows the status of the power supply. The Ident. LED function helps you find the device in large installations:

LED	Status	Meaning
Power	Lights up green	The external power pack is connected, and voltage of 12 Volt is available.
	Lights up blue	The external power pack is connected, and voltage of 12 Volt is available. The Ident. LED to quickly identify the device has been activated (for example, via the web application).
	Off	The external power pack is not (properly) connected.

Flashing transmission LEDs on the rear panel indicate the following operating states of the respective connection:

LED	Status	Meaning
Left	Off	Connection to the remote party not established
	Lights up yellow	Communication with G&D remote station established
	Yellow flashing	Connection to a remote station established
Right	Off	No end device connected
	Green flashing	End device connected

Flashing network LEDs on the front panel indicate the following operating states of the respective connection:

LED	Status	Meaning
Left	Off	No network activity
	Lights up yellow	Network connection established
	Yellow flickering	Network activity
Right	Off	No network connection
	Lights up green	Network connection established
	Lights up yellow	Only older hardware versions differentialte: Network connection established with 10 or 100 Mbit/s (lights up green: Network connection established with 1 Gbit/s)

Technical data

REMOTEACCESS-IP-CPU		
Video	Supported resolutions:	▪ 2560×1600/60Hz/VESA CVT-RB ▪ 2560×1440/60Hz/VESA CVT-RB ▪ 1920×1200/60Hz/VESA CVT-RB ▪ 1920×1080x60Hz/CTA-861-D ▪ 1600×1200/60Hz/VESA DMT ▪ 1680×1050/60Hz/VESA CVT ▪ 1280×1024/60Hz/VESA DMT ▪ 1024×768/60Hz/VESA DMT
	Colour depth:	24 bits
	Video bandwidth:	25 to 330 MP/s
Audio ‣ DisplayPort Digital	Transmission type:	2-channel LPCM, stereo
	Resolutions:	16/20/24 bit
	Refresh rates:	Up to 48 kHz
Data transmission to counterpart station	Interface:	1 × RJ45 socket (1 GBit/s - IEEE 802.3ab)
	Transmission length:	Max. 100 Meters (Cat 5e, Cat 6a)
Data transmission to terminal servers	Interface:	1 × RJ45 socket
	Data rates:	10 MBit/s, 100 MBit/s, 1000 MBit/s
	Supported protocols:	SSH, RDP, VNC
Streaming (<i>optional fee-based feature</i>)	Data rate:	Up to 4 MBit/s
	Supported protocols:	RTP/TCP, RTSP/TCP, MMSH
	Supported codecs for decoding video data:	H.264, VP8, VP9
	Supported resolutions:	Up to 1920×1080x30Hz (Full HD/30Hz)
	Supported codecs for decoding audio data:	MPGA, MP3, AC3
Generic USB ‣ only with UG variants support up to 4 devices; the used console module must support the same account of devices	Specification:	USB 2.0
	USB classes:	Human Interface Devices (HID)
	Transmission rate:	max. 8,5 Mbit/s
Power supply	Type:	Portable power pack (12 V/2A)
	Connection:	1 × Mini DIN 4 socket
	Power consumption:	max. 1.2 A
Housing	Material:	Anodised aluminium
	Dimensions (W × H × D):	105 × 26 × 184 mm
	IP protection class:	IP20
	Weight:	Approx. 400 g

REMOTEACCESS-IP-CPU		
Operating 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	

»RemoteAccess-IP-CPU-Fiber« computer module

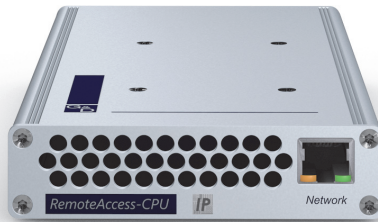
A **RemoteAccess-IP-CPU-Fiber** computer module lets you integrate virtual machines into a IP matrix switch *ControlCenter-IP* or *ControlCenter-IP-XS*. You can access these virtual machines via network.

IMPORTANT: The computer module and the fiber ports are available as *singlemode* and *multimode* variants. Make sure that all components and the fiber optic cable are compatible with each other.

To establish a network connection to virtual machines, use the **SSH**, **VNC** or **RDP** protocol.

In addition, streams can also be received via **RTP/TCP**, **RTSP/TCP** and **MMSH** transport protocols. The **H.265**, **H.264**, **VP8** and **VP9** codecs for decoding video data and **MPGA**, **MP3** and **AC3** for decoding audio data are supported.

IMPORTANT: The activation of the fee-based **RemoteAccess Streaming Feature** is prerequisite for using a streaming protocol (see *Activating premium functions* on page 31).



After configuring any number of virtual machines, you can access one of the virtual machines directly through the IP matrix system.

NOTE: Each **RemoteAccess-IP-CPU** computer module can establish *one* connection to a virtual machine.

Establishing more *simultaneous* connections to different virtual machines within the IP matrix system requires the respective number of computer modules of the **RemoteAccess-IP-CPU** series.

Like other targets, the virtual machines connected are integrated into the OSD and the operating concept of the matrix switch: As usual, you connect to a virtual machine via the **Select** menu in the OSD and can also use functions such as *push-get*, *multi-user access* or *CrossDisplay-Switching* with these virtual machines.

The network connection to the virtual machines is established via an Ethernet network interface (ideally: Gigabit Ethernet).

IMPORTANT: How long it takes to establish a connection as well as the performance of the connection to the virtual machine depends largely on the speed and quality of the network connection to the virtual machine.

The maximum desktop resolution of the virtual machine is 2560×1600 pixels. Make sure that both the console module in use and the monitor support the desired resolution.

The RDP protocol supports transmission of the embedded audio signal via DisplayPort™ cable. Use a compatible DisplayPort console module and a compatible monitor to play the embedded audio signal.

Scope of delivery

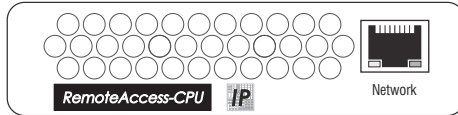
- 1 × **RemoteAccess-IP-CPU-Fiber** computer module
- 1 × power pack (12V/2A, only with variants incl. PowerPack)
- 1 × power cable (only with variants incl. PowerPack)
- 1 × »Safety instructions« flyer

Installation

NOTE: Place the computer module only upright (see sketch below) or at a 90° angle to the left or right.

NOTE: The fan draws the outside air into the device *at the front*. Warm air is emitted *at the rear* ventilation openings.

Connecting a computer



Network: Plug a category 5e (or better) twisted pair cable, which is available as accessory, into this interface.

Connect the other end of the cable with the network (Gigabit Ethernet).

IMPORTANT: Make sure that all virtual machines can be accessed via this interface.

Connection to a matrix switch

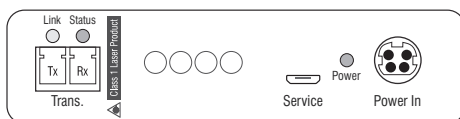
IMPORTANT: The devices use components with laser technology complying with laser class 1.

They meet the requirements according to **EN 60825-1:2014** as well as **U.S. CFR 1040.10** and **1040.11**.

Please observe the following safety instructions:

- *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*

NOTE: For the cable connections, use fiber optic cables with LC connectors. These cables are available as accessories.



Trans. | Tx: Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

Trans. | Rx: Insert the LC plug of a fibre optic cable, which is available as accessory, into this interface. Connect the other end to the Gigabit Ethernet.

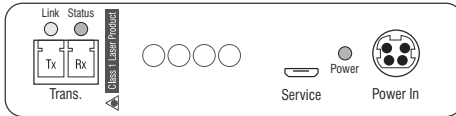
IMPORTANT: KVM data is transferred to and from the IP matrix switch via these interfaces.

Power supply

Power In: Plug the connection cable of the power pack into this interface. Connect the power cable with the power pack and a power socket.

Service interface

The device has a service interface on the back panel. This interface has no relevant function for the user in normal operation.



Debug, error and status messages can be displayed in a terminal emulator (e.g. *HyperTerminal* or *PuTTY*). Via a service menu, technicians have the ability to retrieve information about the device, temporarily disable the network filter rules, reset the device to factory settings, or perform a restart.

The service menu can be operated via any terminal emulator. Use a service cable to connect the computer on which the terminal emulator is installed with the *Service* port of the device.

How to establish a connection within the terminal emulator:

NOTE: Before establishing a connection using the terminal emulator, install the device driver *CP210x USB to UART Bridge VCP*.

This driver provides the *Service* port of the device, which is connected via service cable, as virtual serial interface (COM port). Now, the virtual interface can be selected in the terminal emulator to establish the connection.

The driver is provided as download on the website www.gdsys.com/en under **Service > 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 *GDMan 2.01b*.

NOTE: To log in into the service menu, enter the user name *service* and the password *service*. The service menu is freely accessible on devices with *SecureCert* feature activated.

4. In the service menu, you have the following options:

- Quit (**not** visible on devices with *SecureCert* feature activated)
- System information
- Set system defaults: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.
- Reboot: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.
- Temporary deactivation of the network filter rules: A confirmation *Are you sure? [y]es, [N]o (default)* is displayed.

Status displays

The Power LED on the back of the computer module shows the status of the power supply and the Ident. LED function helps you find the device in large installations:

LED	Status	Meaning
Power	Lights up green	The external power pack is connected, and voltage of 12 Volt is available.
	Lights up blue	The external power pack is connected, and voltage of 12 Volt is available. The Ident. LED to quickly identify the device has been activated (for example, via the web application).
	Off	The external power pack is not (properly) connected.

Flashing transmission LEDs on the rear panel indicate the following operating states of the respective connection:

LED	Status	Meaning
Left	Off	Connection to the remote station not established
	Lights up yellow	Communication with remote station established
	Yellow flashing	Only Rx connection to the remote station established
	Fast yellow flashing	Incompatible SFP module plugged in
Right	Off	Not logged on to remote station
	Green flashing	Logged on to remote station

Flashing network LEDs on the front panel indicate the following operating states of the respective connection:

LED	Status	Meaning
Left	Off	No network activity
	Lights up yellow	Network connection established
	Yellow flickering	Network activity
Right	Off	No network connection
	Lights up green	Network connection established
	Lights up yellow	Only older hardware versions differentialte: Network connection established with 10 or 100 Mbit/s (lights up green: Network connection established with 1 Gbit/s)

Technical data

REMOTEACCESS-IP-CPU-FIBER		
Video	Supported resolutions:	2560×1600/60Hz/VESA CVT-RB 2560×1440/60Hz/VESA CVT-RB 1920×1200/60Hz/VESA CVT-RB 1920×1080x60Hz/CTA-861-D 1600×1200/60Hz/VESA DMT 1680×1050/60Hz/VESA CVT 1280×1024/60Hz/VESA DMT 1024×768/60Hz/VESA DMT
	Colour depth:	24 bits
	Video bandwidth:	25 to 330 MP/s
Audio ‣ DisplayPort Digital	Transmission type:	2-channel LPCM, stereo
	Resolutions:	16/20/24 bit
	Refresh rates:	Up to 48 kHz
Data transmission to counterpart station	Interface:	1 × LC duplex socket
	Transmission length:	‣ RemoteAccess-IP-CPU-Fiber(M) Max. 220 Meters (62,5/125µm 160 MHz*km), Max. 275 Meters (62,5/125µm 200 MHz*km OM1), Max. 500 Meters (50/125µm 400 MHz*km OM2), Max. 550 Meters (50/125µm 500 MHz*km OM2) ‣ RemoteAccess-IP-CPU-Fiber(S) Max. 10.000 Meters (9/125µm 500 MHz*km OS1)
Data transmission to terminal servers	Interface:	1 × RJ45 socket
	Data rates:	10 MBit/s, 100 MBit/s, 1000 MBit/s
	Supported protocols:	SSH, RDP, VNC
Streaming (optional fee-based feature)	Data rate:	Up to 4 MBit/s
	Supported protocols:	RTP/TCP, RTSP/TCP, MMSH
	Supported codecs for decoding video data:	H.264, VP8, VP9
	Supported resolutions:	Up to 1920×1080x30Hz (Full HD/30Hz)
	Supported codecs for decoding audio data:	MPGA, MP3, AC3
Generic USB ‣ only with UG variants support up to 4 devices; the used console module must support the same account of devices	Specification:	USB 2.0
	USB classes:	Human Interface Devices (HID)
	Transmission rate:	max. 8,5 Mbit/s

REMOTEACCESS-IP-CPU-FIBER		
Power supply	Type:	Portable power pack (12 V/2A)
	Connection:	1 × Mini DIN 4 socket
	Power consumption:	Max. 1.2 A
Housing	Material:	Anodised aluminium
	Dimensions (W × H × D):	105 × 26 × 184 mm
	IP protection class:	IP20
	Weight:	Approx. 400 g
Operating 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

Establishing a KVM-over-IP™ connection for the first time

G&D's **KVM-over-IP™** technology makes it possible to transmit signals between the computer module and the IP matrix switch using a Gigabit Ethernet (layer 3).

NOTE: The **Transmission** interface of the computer module is used for signal transmission between the computer module and the IP matrix switch.

The **Network Interface** is used for communication with the virtual computers.

Access to the device's web application is possible via both interfaces.

Only after the initial setup of the KVM-over-IP™ connection between the computer module and the IP matrix switch can the computer module be used with the IP matrix switch.

By default, the following setting of the *Transmission* interface is preselected:

- IP address of the *Transmission* interface:
Obtain address via **DHCPv4** (Fallback: IP address: 172.17.0.10)

By default, the following setting of the *Network* interface is preselected:

- IP address of the *Network Interface A*: 192.168.0.1

Automatic initial setup

You can conveniently set up the **KVM-over-IP™ connection** via the web application of the IP matrix switch (see section *Adding end devices* in the installation guide of the *IP matrix switch*).

NOTE: Manual configuration as described in the following section is *not* necessary in this case.

Manual initial setup via direct connection

If you want to establish the network connection before integrating the computer module into the KVM matrix system, you can do this via the computer module's web application.

Establishing a connection to the network interface

How to connect a computer to the network interface of the computer module:

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

NOTE: Use the IP address *192.168.0.100*, for example.

3. Switch on the computer module.

Starting the web application

1. Start the computer's web browser and enter the URL 192.168.0.1 in the address line.
2. Enter the following data in the login mask:

Agree to the terms of use: Click on the text to read the terms of use. Click on the checkbox to accept the terms of use.

NOTE: The terms of use only appear if a corresponding configuration has been made. For detailed information, please refer to the separate manual of the web application.

Username: Enter a username.

Password: Enter a password for your user account.

2-Factor Auth Code (TOTP): Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.

NOTE: The 2-Factor Auth Code (TOTP) is only requested if two-factor authentication has been configured and activated. For detailed information, please refer to the separate manual of the web application.

IMPORTANT: Change the administrator account's default password.

To do this, log into the web application with the administrator account and then change the password.

The *default* access data to the administrator account are:

- **Username:** Admin
- **Password:** see *login* information on the label on the bottom of the device

3. Click on **Login**.
4. Click on the **Config Panel 21** icon.

Configuring the Transmission interface

How to configure the settings of the *Transmission* interface:

NOTE: The *Link Local* address space 169.254.0.0/16 is reserved for internal communication between devices according to RFC 3330. It is not possible to assign an IP address of this address space!

IMPORTANT: Configuration of **IPv6** should only be performed **by technically experienced users**. While IPv6 offers advanced features and a larger address space, it also introduces **more complex requirements regarding network structure, security, and compatibility**. Incorrect settings may lead to **connectivity issues or unexpected network behavior**. If you are **not familiar** with the IP addressing and network topology specific to IPv6, we recommend that you thoroughly **inform yourself about the implications** before enabling IPv6, or consult with your network administration.

1. In the menu, click on **RemoteGateways**.
2. Click on the computer module and then click on **Configuration**.
3. Click on the tab **Network**.
4. Select the section **Interfaces**.

5. Enter the following values under **Transmission**:

Operating mode:	Select the operating mode of the interface: ▪ Off: switches off network interface. ▪ Static IPv4: A static IPv4 address is assigned. ▪ DHCPv4: Obtain IPv4 address from a DHCP server.
IP address:	Enter the IPv4 address of the interface. <i>This setting is auto obtained in the DHCPv4 operating mode.</i>
Netmask:	Enter the network netmask. <i>This setting is auto obtained in the DHCP operating mode.</i>
IPv6:	Press F8 to enable IPv6 (enabled). By default, IPv6 is disabled . NOTE: When IPv6 is enabled, a link-local IPv6 address is automatically generated based on the MAC address of the interface by default, in accordance with RFC 4921. This link-local IPv6 address cannot be modified by the user.
Static IPv6 address:	Enter the static IPv6 address of the interface.
Prefix:	Specify the prefix length (<i>default: 64</i>) for the interface according to the notation rules defined in RFC 5952.

6. Click on **Save**.

Configuring global network settings

Global network settings ensure that the web application is accessible from all subnetworks, even in complex networks.

How to configure global network settings:

1. In the menu, click on **RemoteGateways**.
2. Click on the computer module and then click on **Configuration**.
3. Click on the tab **Network**.
4. Select the section **Global network settings**.
5. Enter the following values:

Operating mode:	Enter the desired operating mode: ▪ Static: Use of static settings. ▪ Dynamic: Partial automatic retrieval of the settings described below from a DHCP server (IPv4) or via SLAAC (IPv6).
Hostname:	Enter the hostname of the device.
Domain:	Enter the domain to which the device should belong.
Gateway IPv4:	Enter the IPv4 address of the gateway.
Gateway IPv6:	Enter the IPv6 address of the gateway.
DNS server 1:	Enter the IP address of the DNS server..
NOTE: If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign %.	
DNS server 2:	<i>Optionally</i> , enter the IP address of another DNS server..
NOTE: If a link-local IPv6 address is entered, the zone ID of the interface must be specified. The zone ID is appended to the link-local IPv6 address, separated by the percent sign %.	
Prioritization of IPv6:	Click the toggle switch if IPv6 should be preferred when a destination has both an IPv6 and an IPv4 address (green/right = IPv6 is preferred). Click the toggle switch if IPv6 should not be preferred (grey/left = IPv6 is not preferred, <i>default</i>).

Use IPv6 Stateless Address Auto-configuration (SLAAC):	Click the toggle switch if SLAAC should be used (green/right = SLAAC is used, <i>default</i> if the <i>SecureCert</i> feature is not activated). Click the toggle switch if SLAAC should not be used (grey/left = SLAAC is not used, <i>default</i> if the <i>SecureCert</i> feature is activated).
Send ICMP Echo Reply to Echo Request from a Multicast/anycast address (IPv6):	Click the toggle switch if ICMPv6 Echo Requests should be answered (green/right = Echo Requests are answered, <i>default</i>). Click the toggle switch if ICMPv6 Echo Requests should not be answered (grey/left = Echo Requests are not answered).
Send ICMP destination unreachable messages (IPv6):	Click the toggle switch if an ICMPv6 error message should be sent to the sender when a packet cannot be delivered (green/right = error message is sent, <i>default</i>). Click the toggle switch if no ICMPv6 error messages should be sent (grey/left = error message is not sent).
Process redirect messages (IPv6):	Click the toggle switch if redirect messages should be accepted and processed (green/right = redirect messages are processed, <i>default</i>). Click the toggle switch if redirect messages should not be processed (grey/left = redirect messages are not processed).
Duplicate Address Detection (IPv6):	Click the toggle switch if a check for duplicate IPv6 addresses should be performed before an address is used (green/right = duplicate address check is performed, <i>default</i>). Click the toggle switch if no check for duplicate IPv6 addresses should be performed (grey/left = no duplicate address check is performed).

6. Click on **Save**.

NOTE: After successfully setting the IP address, integrate the computer module into the network of the IP matrix switch.

You can add the computer module to the IP matrix switch using the **Add end devices** function of the IP matrix switch.

Basic operation of the web application

The *Config Panel* web application provides a graphical user interface to configure and monitor the device.

The web application can be used in the entire network independently from the locations of the connected device (see *Starting the web application* on page 25).

NOTE: The separate manual provides information about system requirements, the required configuration of the network interfaces at the device and the operation of the web application.

Selecting the language of the web application

NOTE: The selected language is saved in the user settings of the active user. The next time this user logs on, the previously selected language setting is applied.

How to change the language of the web application:

1. Click the language identifier of the current language in the upper right corner.
2. Switch the language to be used by clicking on the desired language.



Activating premium functions

With every purchase of a premium function, you receive a feature key. This file contains a key to activate the purchased function(s).

The premium function(s) is/are activated by importing this key to the web application.

How to import a feature key to activate the purchased function(s):

1. In the menu, click on **RemoteGateways**.
2. Click on the device you want to configure.
3. Open the menu **Service tools** and select the entry **Features**.
4. Click on **Import feature key from file...** and import the feature key (file) via the file interface.

After the file is loaded, the clear text of the feature key is displayed in the text field.

NOTE: The clear text of the feature key can also be copied into the text field.

5. Click on **Save**.

Closing the web application

Use the *Close* button to end the active session of the web application.

IMPORTANT: To protect the web application against unauthorised access, always use the *Logout* function after finishing your work with the web application.

How to close the web application:

1. Click on the **user icon** at the top right.
2. Click on **Logout** to exit the active session.



Configuration of the network interface

The basic requirement for connecting to the virtual computers is the configuration of the network *Interface* of the device.

After integrating the computer module into the IP matrix switch, you can change the configuration of the module's network interface there (see the manual of the *web application of the IP matrix switch*).

Operation via the IP matrix system

Like other targets, the virtual machines connected via the **RemoteAccess-IP-CPU** computer module are integrated into the OSD and operating concept of the IP matrix switch:

As usual, you connect to a virtual machine (**remote target**) via the **Select** menu in the OSD and can also use convenient functions such as *push-get*, *multi-user access* or *Cross-Display-Switching* with these virtual machines.

Configuring remote targets

By using the web application of the matrix switch, you can configure any number of **remote targets** via **Configuration > Matrix systems > [Name] > Remote targets**.

The configuration settings of a remote target include the IP address and the protocol used to connect to the virtual machine.

You can optionally assign each *remote target* and each *remote gateway* (computer module of the **RemoteAccess-IP-CPU** series) to a specific **remote pool**.

A remote pool groups all remote targets that are accessible via the remote gateways included in the pool.

NOTE: More information on this topic is provided in the web application manual of the matrix switch.

NOTES

English

NOTES

NOTES

English



G&D. FEELS RIGHT.

Headquarters | Hauptsitz

Guntermann & Drunck GmbH Systementwicklung

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

US Office

G&D North America Inc.
4540 Kendrick Plaza Drive | Suite 100
Houston, TX 77032 | United States
Phone +1-346-620-4362
sales.us@gdsys.com

Middle East Office

Guntermann & Drunck GmbH
Dubai Studio City | DSC Tower
12th Floor, Office 1208 | Dubai, UAE
Phone +971 4 5586178
sales.me@gdsys.com

APAC Office

Guntermann & Drunck GmbH
60 Anson Road #17-01
Singapore 079914
Phone +65 9685 8807
sales.apac@gdsys.com