G&D VisionVS-IP

DE Installation und Bedienung

EN Installation and Operation



A9100426-1.01

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 2026. Alle Rechte vorbehalten.

Version 1.01 – 20.01.2026
Firmware: 2.4.000 | 4.4.3

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 erfüllt die Grenzwerte für ein digitales Gerät der Klasse A entsprechend Teil 15 der FCC-Bestimmungen.

Diese Grenzwerte sollen einen angemessenen Schutz vor schädlichen Störungen bieten, wenn das Gerät in gewerblichen Umgebungen betrieben wird. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie und kann diese ausstrahlen. Wird es nicht gemäß der Bedienungsanleitung installiert und verwendet, kann es schädliche Störungen für Funkverbindungen verursachen.

Der Betrieb dieses Geräts in Wohngebieten kann schädliche Störungen verursachen. In diesem Fall müssen Benutzer die Störung auf eigene Kosten beheben.

Inhaltsverzeichnis

Sicherheitshinweise **1**

Die VisionVS-IP-Serie **5**
Signalübertragung und Übertragungslänge 6

Lieferumfang **7**

Secure-KVM-over-IP-Lösung **8**
Mögliche Sicherheitslücken, Bedrohungen und Gefahren 8
Schutz der KVM-Systeme vor Angriffen (von außen und innen) 8
Sicherheitsanforderungen bei KVM-over-IP 8
Die sichere Lösung von G&D 9
Trusted-Computing-Platform 11
Monitoring, SNMP und Syslog 11
Update und Backup/Restore 11
Weitere sicherheitsrelevante Aspekte 12
2-Faktor-Authentifizierung (2FA) 12

Signalübertragung und Übertragungslänge **13**

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

Installation **15**
Vorbereitung 15
Installation der VisionVS-IP 16
Installation einer KVM-over-IP-Gegenstelle 21

Inbetriebnahme **22**

Startvorgang **22**

Erstkonfiguration der Netzwerkeinstellungen **23**

Ersteinrichtung der KVM-over-IP™-Verbindung **24**
Werkseinstellung der Module 25
KVM-over-IP-Verbindung der VisionVS-IP konfigurieren 26
Konfiguration der globalen Netzwerkeinstellungen 26
Konfiguration der KVM-over-IP-Verbindung 26
Erweiterte Einstellungen der KVM-over-IP-Verbindung 27
Bandbreite limitieren 27
Klassifizierung der IP-Pakete (DiffServ) 27
Signale (de)aktivieren 27
Beschränkung der KVM-over-IP-Gegenstelle (UID-Locking) 28

Integration in die AV-Lösung und RemoteAccess **29**
HTML-KVM-Client öffnen 29
In einem DHCP-Netzwerk 30
In einem statischen Netzwerk 30
Standard-Admin-Anmeldedaten ändern 31
Verbindung herstellen 31
Netzwerkeinstellungen 32
Passwort ändern 33
Videoeinstellungen 34
VuStream-350 KVM-Treiber-Installation 34
VuStream-350 KVM-Treiber-Deinstallation 34
Firmware-Update 35
Auf Werkseinstellungen zurücksetzen 36

Bedienung **37**
Konkurrierende Bedienung 37
Exklusive Bedienung 38

Konfiguration **39**
Grundlegende Bedienung der Webapplikation 39
Start der Webapplikation 40
Sprache der Webapplikation auswählen 41
Webapplikation beenden 41

Weiterführende Informationen **42**
Empfehlungen zu den Twisted-Pair-Kabeln 42
Übertragung der KVM-Daten (Transmission) 42
DDC-Weiterleitung mit Cache-Funktion 43
Ermittlung der Netzwerkeinstellungen über den Service-Port 43
Installation des Gerätetreibers 43
Einrichten einer Verbindung im Terminalemulationsprogramm 44
Ermittlung der IP-Adresse 44
Pin-Belegung der RS232-Buchse/Schnittstelle 45

Statusanzeigen **46**
Bedeutung der LEDs an der Vorderseite 46
Bedeutung der LEDs an der Rückseite (CAT-Variante) 47

Technische Daten **48**
Allgemeine Eigenschaften der Serie 48
Spezifische Eigenschaften der CAT-Variante 50
Spezifische Eigenschaften der Fiber-Varianten 51
Eigenschaften der Übertragungsmodule 52

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.

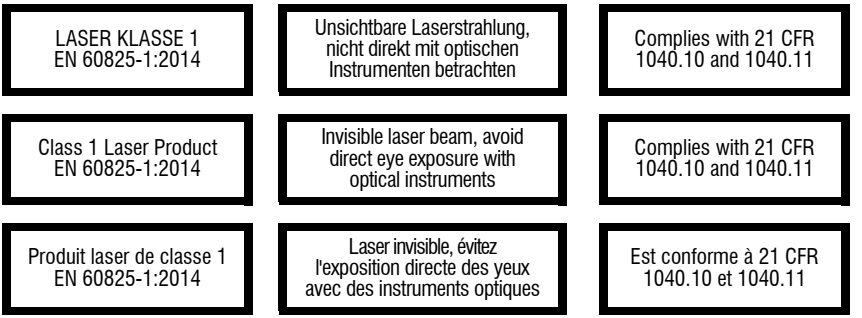
Mettre au rebut les batteries usagées conformêment aux instructions du fabricant et de manière écologique. Les batteries usagées ne doivent pas être jetées dans les ordures ménagères.

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

Besondere Hinweise zum Umgang mit Laser-Technologie

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

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



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

⚠ Blickkontakt mit dem unsichtbaren Laserstrahl vermeiden

Betrachten Sie die unsichtbare Laserstrahlung niemals mit optischen Instrumenten!

⚠ Optische Anschlüsse stets verbinden oder mit Schutzkappen abdecken

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

⚠ Ausschließlich von G&D zertifizierte Übertragungsmodule verwenden

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

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

Die VisionVS-IP-Serie

Die **VisionVS-IP** vereint ein *DP-Vision-IP*-Rechnermodul mit einem *VuStream-350* in einem Gehäuse. Es handelt sich somit um ein hybrides Rechnermodul mit Dual-Encoder, das KVM-Signale praktisch latenzfrei und in verlustfreier Qualität über eine KVM-over-IP-Matrix von G&D zum Arbeitsplatz überträgt. Parallel ermöglicht es ein latenzarmes Streaming an *VuWall-PAK*-Geräte für den Fernzugriff auf den Rechner oder für flexibles Video-Wand-Management. Die Appliance ist Bestandteil einer modularen Systemlösung und erfordert zusätzliche Komponenten für den Betrieb.

Mit diesem Kombiprodukt entstehen integrierte Systemlösungen, die G&Ds hochwertige KVM-over-IP-Technologie mit VuWalls flexiblen Videowandlösungen und zentralem Fernzugriff auf Rechnerebene vereinen – ideal für moderne Leitstand- und Kontrollraumumgebungen. Dabei profitieren Sie von der typisch schnellen und flüssigen Bedienung der G&D-Arbeitsplätze sowie von der Möglichkeit, Inhalte gleichzeitig an mehreren Stellen darzustellen – etwa am Arbeitsplatz, auf der Videowand oder für den Fernzugriff.

HINWEIS: Die **VisionVS-IP** ist in den entsprechenden Varianten kompatibel zu bestehenden G&D-Produktfamilien (*Vision-IP*, *VisionXS-IP*, *ControlCenter-IP*, *ControlCenter-IP-XS*). Der Streamingausgang ist kompatibel mit VuWall´s *PAK* und *TRx*.

Bei Fragen zur Kompatibilität kontaktieren Sie bitte das Support-Team.

Alternativ zum Matrixbetrieb können Sie die **VisionVS-IP** auch im Extenderbetrieb mit einem kompatiblen Arbeitsplatzmodul verwenden.

Konfigurieren Sie eine KVM-over-IP-Verbindung zwischen der **VisionVS-IP** und einem kompatiblen Arbeitsplatzmodul. Die konfigurierte Verbindung zwischen den Modulen wird bei jedem Neustart der Module wiederhergestellt.

Signalübertragung und Übertragungslänge

Die Signalübertragung zwischen der **VisionVS-IP** und dem Arbeitsplatzmodul erfolgt komprimiert und verschlüsselt (AES-128) mittels G&Ds **KVM-over-IP™**-Technologie über das Gigabit-Ethernet (Layer 3).

Bei ausreichend nutzbarer Bandbreite des Gigabit-Ethernets wird das Videosignal mit verlustfreier Videoqualität und nahezu latenzfrei wiedergegeben. Mittels manuellem Bandbreiten-Management können Sie die Übertragung an unterschiedliche Bandbreitenanforderungen anpassen.

Bei Beachtung der max. Länge von Teilstrecken zwischen zwei *aktiven* Netzwerkkomponenten ist die gesamte Übertragungslänge unbeschränkt.

Lieferumfang

Standardlieferumfang der VisionVS-IP-Serie

- 1 × **VisionVS-IP**, Fiber-Varianten inkl. Übertragungsmodul/SFP-Transceiver
- 1 × Stromversorgungskabel (*PowerCable-2 Standard*)
- 1 × Videokabel (*DP1.4-Cable-M/M-2*)
- 1 × USB-Gerätekabel (*USB-AM/BM-2*)
- 1 × Audio-Kabel (*Audio-M/M-2*)
- 1 × serielles Anschlusskabel (*RS232-M/F-2*)
- 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.

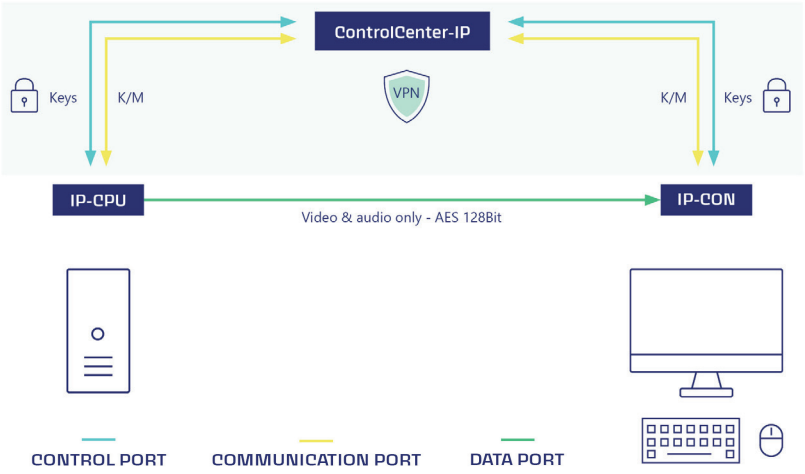
Bei KVM-over-IP-Systemen erfolgt die Übertragung IP-basiert über Ethernet-Netzwerke (OSI-Schichtenmodell Layer 3). Mit KVM-over-IP hat man aufgrund der Flexibilität und einfachen Erweiterbarkeit eine zukunftssichere Lösung. Jedoch steigt mit der IP-Übertragung auch das Sicherheitsrisiko. Es besteht hierbei 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 jeweiligen Gegenstelle oder einer KVM-over-IP-Matrix ControlCenter-IP oder ControlCenter-IP-XS verbunden. Es kommt ein AES256 Galois/Counter Mode (GCM) verschlüsselter IPSec VPN-Tunnel zum Einsatz (GCM basiert auf Counter Mode CTR, bietet aber zusätzlich einen integrierten Integritätsschutz). Es gibt zudem eine Abwärtskompatibilität für AES128-GCM.



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

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

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

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

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

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

Trusted-Computing-Platform

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

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

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

Monitoring, SNMP und Syslog

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

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

Update und Backup/Restore

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

Weitere sicherheitsrelevante Aspekte

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

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

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

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

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

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

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

2-Faktor-Authentifizierung (2FA)

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

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

Signalübertragung und Übertragungslänge

Die Signalübertragung zwischen dem Rechner- und dem Arbeitsplatzmodul erfolgt komprimiert und verschlüsselt mittels G&Ds **KVM-over-IP™**-Technologie (siehe *Die sichere Lösung von G&D* auf Seite 9) über das Gigabit-Ethernet (Layer 3). Alternativ können das Rechnermodul und das Arbeitsplatzmodul auch direkt miteinander verbunden werden. Hierbei ist die Übertragungslänge beschränkt.

Bei ausreichend nutzbarer Bandbreite des Gigabit-Ethernets wird das Videosignal mit verlustfreier Videoqualität und nahezu latenzfrei wiedergegeben. Mittels manuellem Bandbreiten-Management können Sie die Übertragung an unterschiedliche Bandbreitenanforderungen anpassen.

Bei Beachtung der max. Länge von Teilstrecken zwischen zwei *aktiven* Netzwerkkomponenten ist die gesamte Übertragungslänge unbeschränkt.

Anforderung an den Netzwerk-Switch

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

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

Voraussetzungen der Netzwerk-Switches

Folgende Voraussetzungen gelten für das Netzwerk:

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

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

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

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

  BEISPIEL: Typische Bandbreitenanforderungen bei KVM-over-IP

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

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

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

  BEISPIEL:

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

Installation

WICHTIG: Die Fiber-Varianten der VisionVS-Serie verwenden Baugruppen mit Laser-Technologie, die der Laser-Klasse 1 entsprechen.

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

Beachten Sie diesbezüglich folgende Sicherheitshinweise:

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

Vorbereitung

WICHTIG: Stellen Sie bei der Standortwahl der Geräte sicher, dass die zulässige Umgebungstemperatur (siehe *Technische Daten* auf Seite 48) in der unmittelbaren Nähe eingehalten und nicht durch andere Geräte beeinflusst wird.

Um bei Installation mehrerer Geräte übereinander eine gute Luftzirkulation zu erreichen und die gegenseitige thermische Beeinflussung zu vermeiden, wird empfohlen, maximal drei Geräte unmittelbar übereinander zu platzieren. Planen Sie im Anschluss daran einen Zwischenraum (min. 2 cm) ein.

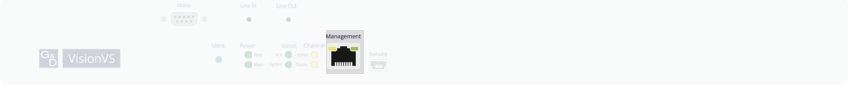
1. Stellen Sie sicher, dass der an die **VisionVS-IP** anzuschließende Rechner ausgeschaltet ist. Falls der Rechner mit einer Tastatur und einer Maus verbunden ist, ziehen Sie die Kabel der Eingabegeräte aus den Schnittstellen.
2. Platzieren Sie die **VisionVS-IP** in der Nähe des Rechners.

HINWEIS: Die maximale Kabellänge zwischen der **VisionVS-IP** und dem anzuschließenden Rechner beträgt *fünf* Meter.

Installation der VisionVS-IP

An die **VisionVS-IP** schließen Sie den Rechner an, dessen Signale an den entfernten Arbeitsplatz, auf die Videowand oder für den Fernzugriff übertragen werden sollen. Falls gewünscht, können Sie einen lokalen Arbeitsplatz an die **VisionVS-IP** anschließen (siehe *Optional: Lokalen Arbeitsplatz anschließen* auf Seite 18).

Verbindung mit einem lokalen Netzwerk herstellen



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

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

Tastatur- und Mausschnittstelle(n) des Rechners anschließen



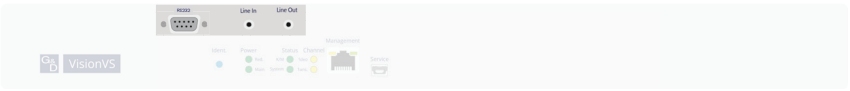
USB CPU: Verbinden Sie eine USB-Schnittstelle des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *USB-AM/BM-2*.

Videoausgang des Rechners anschließen



DisplayPort CPU: Verbinden Sie den Videoausgang des Rechners mit dieser Schnittstelle. Verwenden Sie hierzu das Kabel *DP1.4-Cable-M/M-2*.

Audio- und RS232-Schnittstellen verbinden



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

Sie können die Übertragung der RS232-Daten aktivieren und/oder die Übertragung der Audio-Daten deaktivieren .

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

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

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

WICHTIG: Die Audio- und RS232-Daten werden nur über die KVM-over-IP-Verbindung und **nicht** über den Streamingausgang übertragen.

Optional: Lokalen Arbeitsplatz anschließen



HDMI Out: Schließen Sie den Monitor des lokalen Arbeitsplatzes an.

USB K/M: Schließen Sie die USB-Tastatur und/oder die USB-Maus des lokalen Arbeitsplatzes an.

Weitere Schnittstelle



Control: Reserviert für zukünftige Funktionen.

Verbindung zu einem Netzwerk herstellen, um die VisionVS-IP in die AV-Lösung zu integrieren



Network: Stecken Sie ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5e (oder höher) ein. Das andere Ende des Kabels ist mit dem gleichen Netzwerk zu verbinden, auf dem sich Ihre AV-Lösung befindet bzw. über das der entfernte Zugriff erfolgen soll.

HINWEIS: Sie können die **VisionVS-IP** bzw. den **VuStream-350** auch zu Ihrer Anwendung hinzufügen, ohne die *VuWall-PAK-KVM-Funktion* von *TRx* zu verwenden. In diesem Fall können Sie einfach über ein Gigabit-Ethernet eine Verbindung zur **VisionVS-IP** und den entfernten Computer herstellen (siehe *Integration in die AV-Lösung und RemoteAccess* ab Seite 29).

Verbindung mit dem Gigabit-Ethernet herstellen

CAT-Varianten:



Transmission: 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.

Fiber-Varianten:



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

Betrachten Sie die unsichtbare Laserstrahlung niemals mit optischen Instrumenten!

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

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

Transmission|Rx: Stecken Sie den LC-Stecker eines weiteren Glasfaserkabels ein. Das andere Ende des Kabels ist mit dem Gigabit-Ethernet zu verbinden.

Stromversorgung herstellen

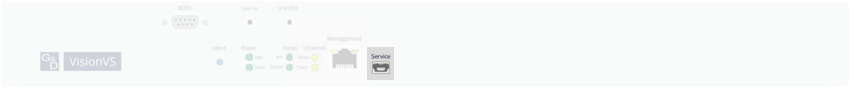


Main Power: Stecken Sie ein mitgeliefertes Kaltgerätekabel ein.

Red. Power: An diese Buchse können Sie ein optionales Tischnetzteil anschließen. Hierdurch wird eine zweite, redundante Stromversorgung des Gerätes erreicht.

Service-Schnittstelle

Das Gerät besitzt an der Vorderseite 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 **VisionVS-IP**-Systems als virtuelle serielle Schnittstelle (COM-Port) zur Verfügung. Die virtuelle Schnittstelle kann anschließend im Terminalemulationsprogramm zum Verbindungsaufbau ausgewählt werden.

Der Treiber steht auf der Website **www.gdsys.com/de** im Bereich **Service > Downloads** 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 **VisionVS-IP** zu verbinden.

HINWEIS: Der Login für das Service-Menü erfolgt über den Benutzernamen *service* und das Passwort *service*.

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

Installation einer KVM-over-IP-Gegenstelle

Installieren Sie einen kompatiblen KVM-over-IP-Matrixswitch und/oder ein kompatibles Arbeitsplatzmodul wie in den entsprechenden Handbüchern beschrieben.

Inbetriebnahme

Nach der ordnungsgemäßen Installation der Geräte können diese sofort in Betrieb genommen werden.

Beachten Sie folgende Einschaltreihenfolge bei der Erstinbetriebnahme der Geräte:

1. Schalten Sie das Arbeitsplatzmodul und/oder den KVM-over-IP-Matrixswitch ein.
2. Schalten Sie die **VisionVS-IP** ein.
3. Schalten Sie den an der **VisionVS-IP** angeschlossenen Rechner ein.

HINWEIS: Die empfohlene Einschaltreihenfolge für die Erstinbetriebnahme stellt sicher, dass die KVM-Extender die Eigenschaften des angeschlossenen Monitors auslesen und an den Rechner weiterleiten können (siehe *DDC-Weiterleitung mit Cache-Funktion* auf Seite 43).

Startvorgang

Nach dem Einschalten der **VisionVS-IP** signalisieren die LEDs an der Vorderseite den Betriebszustand des Geräts.

Weitere Hinweise hierzu erhalten Sie im Kapitel *Statusanzeigen* ab Seite 46.

Erstkonfiguration der Netzwerkeinstellungen

Die *Management*-Schnittstelle erlaubt die Integration eines Gerätes in ein separates Netzwerk für den Zugriff auf die Webapplikation und die Nutzung der erweiterten Netzwerkfunktionen (Netzfilter, Syslog, …) der Geräte.

HINWEIS: Im Auslieferungszustand sind folgende Einstellungen vorausgewählt:

- IP-Adresse der *Netzwerkschnittstelle »Network Management«*: **192.168.0.1**
- globale Netzwerkeinstellungen: Dynamischer Bezug der Einstellungen

Die erforderlichen Konfigurationseinstellungen können über die Webapplikation des integrierten Rechnermoduls durchführen.

WICHTIG: Weitere Informationen zu den Konfigurationseinstellungen finden Sie im Kapitel *Erstkonfiguration der Netzwerkeinstellungen* im separaten Handbuch zur Webapplikation der *Vision-IP-Serie*.

Ersteinrichtung der KVM-over-IP™-Verbindung

Die Geräte der **VisionVS-IP**-Serie sind mit drei Netzwerkschnittstellen ausgestattet:

- **Transmission:** Über die Schnittstelle werden die KVM-Daten über eine KVM-over-IP™-Verbindung zur Gegenstelle übertragen.

- **Management:** Diese Schnittstelle erlaubt die Integration eines Gerätes in ein separates Netzwerk für den Zugriff auf die Webapplikation und die Nutzung der erweiterten Netzwerkfunktionen (Netzfilter, Syslog, …) der Geräte.

- **Network:** Über die Schnittstelle wird die Verbindung zum VuWall-Server hergestellt (siehe *Netzwerkeinstellungen* auf Seite 32).

WICHTIG: Beachten Sie die separaten Anweisungen zur *Erstkonfiguration der Netzwerkeinstellungen* auf Seite 23.

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

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

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

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

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

WICHTIG: Die oben genannten IP-Adressen sind als '*Fallback*' vorkonfiguriert, sofern keine IP-Adresse während des Bootvorgangs über einen DHCP-Server bezogen werden konnte. Falls IP-Adressen über einen DHCP-Server bezogen werden, sind die vorkonfigurierten IP-Adressen nicht mehr gültig.

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

TIPP: Falls Ihnen die IP-Adresse eines bereits konfigurierten Arbeitsplatz- oder Rechnermoduls unbekannt ist, können Sie diese über die Log-Ausgaben des Gerätes ermitteln. Weiterführende Informationen finden Sie im Abschnitt *Ermittlung der Netzwerkeinstellungen über den Service-Port* auf Seite 43.

Werkseinstellung der Module

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

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

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

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

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

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

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

KVM-over-IP-Verbindung der VisionVS-IP konfigurieren

Die erforderlichen Konfigurationseinstellungen können Sie direkt am Arbeitsplatz durchführen.

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Konfiguration der globalen Netzwerkeinstellungen

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Konfiguration der KVM-over-IP-Verbindung

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

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Erweiterte Einstellungen der KVM-over-IP-Verbindung

Bandbreite limitieren

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Klassifizierung der IP-Pakete (DiffServ)

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

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

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Signale (de)aktivieren

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

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

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

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

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

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie in den separaten Handbüchern des eingesetzten KVM-over-IP-Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

Integration in die AV-Lösung und RemoteAccess

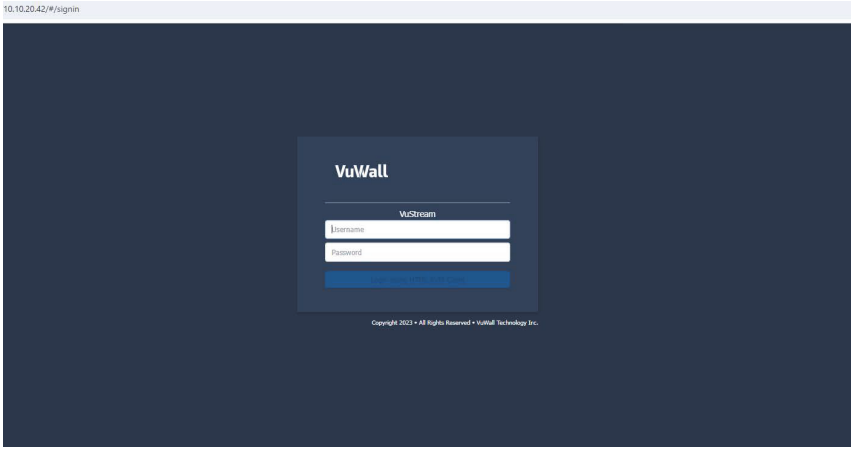
Das in der **VisionVS-IP** integrierte **VuStream-350** bietet in Kombination mit einem PAK 20 oder PAK 40 von VuWall eine extrem geringe Latenz für Ihre Videowand-Lösung. Dies ist besonders nützlich bei der Verwendung der PAK-KVM-Funktion von TRx. Sie können jedoch auch eine **VisionVS-IP**/einen **VuStream-350** zu Ihrer Lösung hinzufügen, ohne die *PAK-KVM-Funktion* von *TRx* zu nutzen.

WICHTIG: Die Audio- und RS232-Daten (siehe *Audio- und RS232-Schnittstellen verbinden* auf Seite 17) werden nur über die KVM-over-IP-Verbindung und **nicht** über den Streamingausgang übertragen.

Um eine **VisionVS-IP**/einen **VuStream-350** zu Ihrer Lösung hinzuzufügen, lesen Sie die folgenden Abschnitte.

HTML-KVM-Client öffnen

Verwenden Sie den HTML-KVM-Client, um den integrierten **VuStream-350** zu konfigurieren. Um darauf zuzugreifen, folgen Sie den Schritten in den nachstehenden Abschnitten – abhängig von Ihrem Netzwerktyp.



In einem DHCP-Netzwerk

1. Verbinden Sie die **VisionVS-IP** mit Ihrem Netzwerk über ein Ethernet-Kabel (siehe *Verbindung zu einem Netzwerk herstellen, um die VisionVS-IP in die AV-Lösung zu integrieren* ab Seite 18).

   TIPP: Wenn Sie viele **VisionVS-IP**/**VuStream-350** konfigurieren müssen, können Sie diese in diesem Schritt alle gleichzeitig mit Ihrem Netzwerk verbinden.

2. Verwenden Sie eine IP-Scanner-Software Ihrer Wahl, um die IP-Adresse jedes **VuStreams-350** zu ermitteln. Jede **VisionVS-IP**/**jedes VuStream-350** kann im IP-Scanner anhand ihrer MAC-Adresse identifiziert werden. Für detailliertere Anweisungen zur Verwendung eines IP-Scanners wenden Sie sich bitte an Ihren Netzwerkadministrator.
3. Öffnen Sie **https://<VuStream-350 IP-Adresse>**. Melden Sie sich mit den Standard-Administrator-Anmeldedaten an (siehe *Standard-Admin-Anmeldedaten ändern* ab Seite 31).

In einem statischen Netzwerk

1. Verbinden Sie die **VisionVS-IP** mit Ihrem Netzwerk über ein Ethernet-Kabel (siehe *Verbindung zu einem Netzwerk herstellen, um die VisionVS-IP in die AV-Lösung zu integrieren* ab Seite 18).

   WICHTIG: Wenn Sie mehrere **VisionVS-IP**/**VuStream-350** konfigurieren müssen, müssen Sie jede **VisionVS-IP**/**VuStream-350** nacheinander mit Ihrem Netzwerk verbinden und konfigurieren.

2. Öffnen Sie **https://kvm.local**. Melden Sie sich mit den Standard-Administrator-Anmeldedaten an (siehe *Standard-Admin-Anmeldedaten ändern* ab Seite 31).

   WICHTIG: Um auf **https://kvm.local** zugreifen zu können, stellen Sie sicher, dass *mDNS* **nicht** eingeschränkt ist.

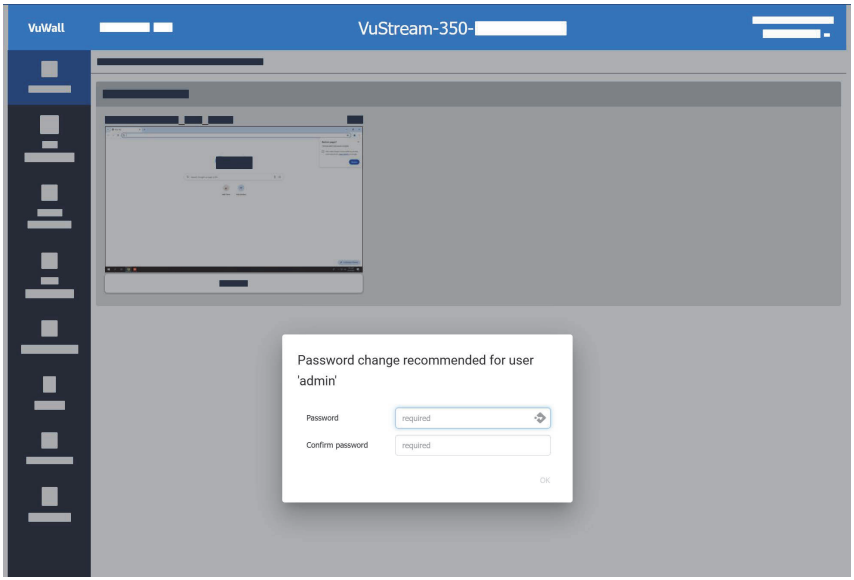
3. Folgen Sie den Schritten im Abschnitt *Netzwerkeinstellungen* (s. Seite 32 f.).

Standard-Admin-Anmeldedaten ändern

Beim ersten Aufruf eines *Clients* nach der Inbetriebnahme des Gerätes werden Sie zur Änderung des Passworts aufgefordert.

HINWEIS: Das Standard-Passwort des Benutzers **admin** lautet **vuwall**.

Sie werden aufgefordert, das Passwort für den Administrator zurückzusetzen. Geben Sie ein Passwort Ihrer Wahl ein.



Verbindung herstellen

Sie können sich eine Vorschau anzeigen lassen und eine Verbindung zum Target herstellen.

So stellen Sie eine Verbindung zum Target her:

1. Klicken Sie auf den Bereich **Port Access**, um eine Vorschau angezeigt zu bekommen.

   HINWEIS: Das Vorschaubild wird alle 5 Sekunden aktualisiert.

2. Klicken Sie auf **Connect**, um die Verbindung zum Target herzustellen.

Netzwerkeinstellungen

Ihr *TRx*-Netzwerk muss in der Lage sein, auf Ihr **VuStream-350** zuzugreifen. In der Regel bedeutet dies, dass sich die IP-Adresse und das Gateway (optional) im gleichen Netzwerkbereich wie Ihr *TRx*-Server befinden sollten. Die Netzwerkeinstellungen werden abhängig von Ihrem Netzwerktyp angewendet:

DHCP: Die Netzwerkeinstellungen werden automatisch von Ihrem DHCP-Server zugewiesen (*Standard*).

Statische IP: Befolgen Sie die folgenden Schritte, um die IP-Einstellungen von den Standardwerten zu ändern:

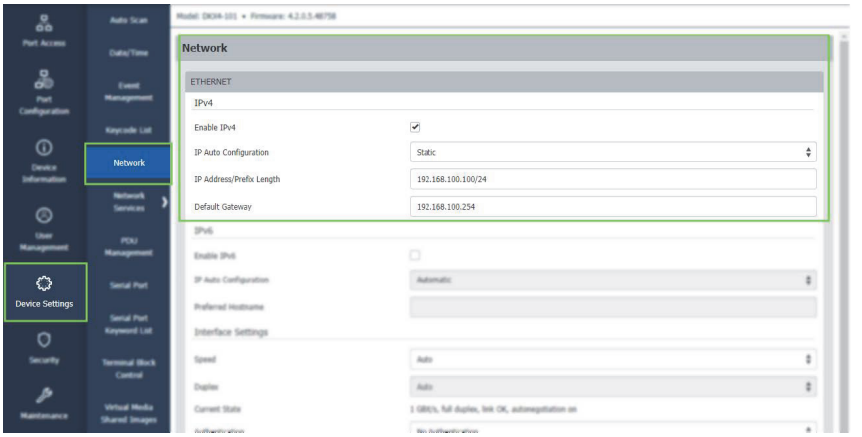
1. Klicken Sie im Client auf **Device Settings > Network**.

2. Erfassen Sie im Abschnitt **Ethernet > IPv4** folgende Daten:

Enable IPv4:	Aktivieren Sie **IPv4**.
IP Auto Configuration:	Wählen **Static**, um eine statische IP-Adresse angeben zu können.
IP Address/ Prefix Length:	Erfassen Sie eine statische IPv4-Adresse für das **VuStream-350**.
Default Gateway:	Geben Sie das Standard-Gateway für das **VuStream-350** an.

TIPP: Für größere Netzwerke oder spezielle Netzwerkkonfigurationen wenden Sie sich an Ihren Netzwerkadministrator, um Unterstützung bei der Konfiguration der Netzwerkeinstellungen Ihres Geräts zu erhalten.

3. Klicken Sie auf **Save**.



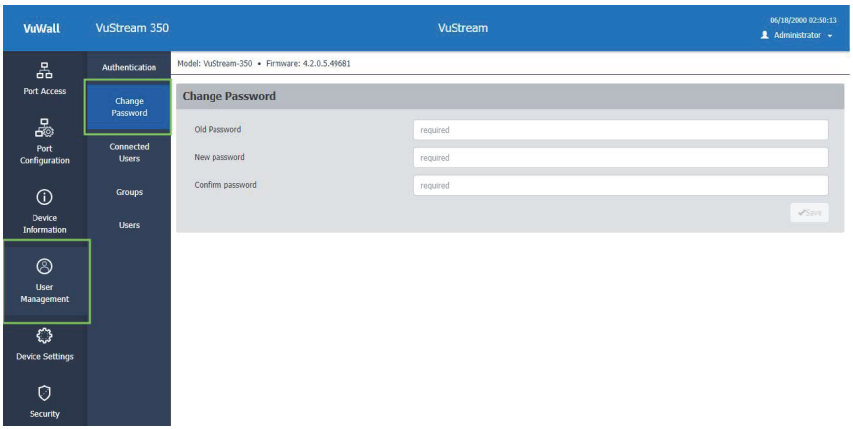
Passwort ändern

So ändern Sie das Admin-Passwort:

1. Wählen Sie im Bereich **User Management** den Bereich **Change Password** aus.
2. Erfassen Sie folgende Daten:

Old Password:	Geben Sie das bisherige Passwort ein.
New Password:	Geben Sie ein neues Passwort ein.
Confirm New Password:	Bestätigen Sie das neue Passwort.

3. Klicken Sie auf **Save**.



Videoeinstellungen

So ändern Sie die Videoeinstellungen:

1. Wählen Sie im Bereich **Port Configuration** den Bereich **Video settings**, um die Videoeinstellungen Ihrer Quelle anzuzeigen oder anzupassen. Nachfolgend finden Sie einige Hinweise zur Anpassung der Videoeinstellungen:

Default preferred video resolution:	1920x1080@60Hz
Maximum preferred video resolution:	3840x2160@60Hz
Default cycle time:	200 ms. Erhöhen Sie die Zykluszeit, wenn das Target-Video nicht auf Auflösungsänderungen reagiert.

VuStream-350 KVM-Treiber-Installation

Wenn Ihre AV-Lösung eine oder mehrere KVM-Operator-Stationen umfasst, laden Sie den KVM-Treiber herunter und installieren Sie ihn auf Ihrem **VisionVS-IP**-Source-PC.

1. Gehen Sie zum **VuWall-Partner-Portal** und laden Sie den *VuStream-350 KVM Mouse Driver* herunter.

2. Führen Sie das Installationsprogramm auf dem **VisionVS-IP**-Source-PC aus.

VuStream-350 KVM-Treiber-Deinstallation

Wenn Sie nicht mehr möchten, dass Ihre Operator-Station Zugriff auf die KVM-Funktionalität hat, folgen Sie den unten stehenden Schritten, um den *VuStream-350 KVM Mouse Driver* zu deinstallieren.

1. Öffnen Sie auf Ihrem **VisionVS-IP**-Source-PC den Datei-Explorer und navigieren Sie zu: *C:\Program Files (x86)\VuWall Technology Inc\VuWall KVM Mouse Driver.*

2. Doppelklicken Sie auf **Uninstall** und führen Sie das Deinstallationsprogramm aus.

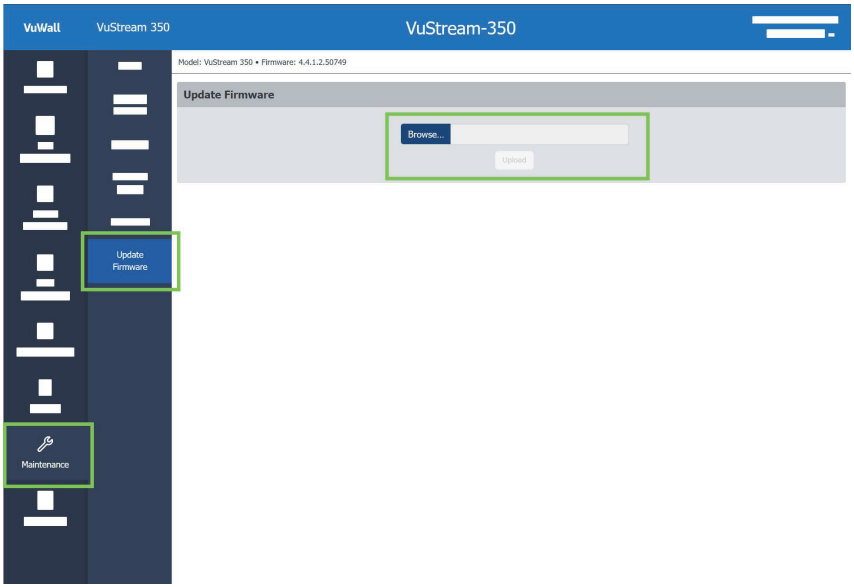
Firmware-Update

So aktualisieren Sie das integrierte VuStream-350 auf die neueste Firmware:

1. Stellen Sie sicher, dass Ihre **VisionVS-IP** mit Ihrem AV-Netzwerk verbunden ist.
2. Laden Sie von einem Computer in Ihrem AV-Netzwerk über das **VuWall-Partner-Portal** die neueste **VuStream-350-Firmware** herunter. Entpacken Sie anschließend die heruntergeladenen Dateien.
3. Verwenden Sie eine IP-Scanner-Software Ihrer Wahl, um die IP-Adresse Ihres **VuStream-350** zu ermitteln. Jedes **VuStream-350** kann im IP-Scanner über seine MAC-Adresse identifiziert werden. Für detailliertere Anweisungen zur Verwendung eines IP-Scanners wenden Sie sich bitte an Ihren Netzwerkadministrator. Gehen Sie anschließend zu *https://<VuStream350 IP-Adresse>*, um auf den HTML KVM Client zuzugreifen.

> **HINWEIS:** Für den Erstzugriff zur Konfiguration Ihres integrierten **VuStream-350** wenden Sie sich bitte an den **VuWall Support**. Je nach Netzwerkkonfiguration benötigen Sie eventuell detailliertere Anweisungen für die Anmeldung.

4. Melden Sie sich im **HTML KVM Client** mit den Admin-, Standard- oder zuvor eingerichteten Zugangsdaten an.
5. Gehen Sie zu **Maintenance** und wählen Sie **Update Firmware**. Unter **Update Firmware** klicken Sie auf **Browse**. Navigieren Sie zum Speicherort der Firmware-Datei. Wählen Sie die **.rfp**-Datei und klicken Sie auf **Upload**.



6. Wählen Sie **Update Firmware**. Der Aktualisierungsvorgang dauert etwa 5 Minuten.

> **WICHTIG:** Schalten Sie das Gerät während der Aktualisierung **nicht** aus. Nach Abschluss des Updates startet das Gerät automatisch neu.

7. Melden Sie sich im **HTML KVM Client** an. Ändern Sie das Passwort, wenn Sie dazu aufgefordert werden.
8. Wiederholen Sie die Schritte 3 bis 5 für jede **VisionVS-IP**/jedes **VuStream-350**, die/das Sie aktualisieren möchten.

> **HINWEIS:** Während des Aktualisierungsvorgangs steht die **KVM-Funktionalität** an der Operator-Station **nicht** zur Verfügung.

Auf Werkseinstellungen zurücksetzen

So setzen Sie das integrierte VuStream-350 auf die Werkseinstellungen zurück:

1. Gehen Sie zu **Maintenance** und wählen Sie **Unit Reset**.
2. Wählen Sie **Reset to Factory Defaults**.

Bedienung

Den an der **VisionVS-IP** angeschlossene Rechner können Sie sowohl am entfernten Arbeitsplatz des G&D-Arbeitsplatzmoduls als auch über VuWall-Streaming oder am lokalen Arbeitsplatz der **VisionVS-IP** bedienen.

Nach der Inbetriebnahme ist die Bedienung des Rechners für alle Arbeitsplätze freigeschaltet.

HINWEIS: Die Monitore des entfernten Arbeitsplatzes am Arbeitsplatzmodul und des VuWall-Streamings sowie des lokalen Arbeitsplatzes der **VisionVS-IP** zeigen in der Standardeinstellung *immer* das gleiche Bild an.

HINWEIS: Wird die **VisionVS-IP** im **Extenderbetrieb** verwendet, können Anpassungen im Bereich **konkurrierende/exklusive Bedienung** vorgenommen werden.

Konkurrierende Bedienung

Wird im Extenderbetrieb an einem Arbeitsplatz eine Eingabe per Tastatur oder Maus durchgeführt, werden automatisch die Eingabegeräte des konkurrierenden Arbeitsplatzes gesperrt. Die Sperre wird aufgehoben, wenn innerhalb der eingestellten Zeitspanne der Eingabesperre (*Standard*: 1 Sekunde) keine weitere Eingabe am aktiven Arbeitsplatz erfolgt.

Nach der automatischen Aufhebung der Sperre ist die Bedienung des Rechners wieder an allen Arbeitsplätzen freigeschaltet.

Alternativ zur konkurrierenden Bedienung des Rechners durch die Arbeitsplätze kann die exklusive Bedienung aktiviert werden.

Exklusive Bedienung

Um die exklusive Bedienung durch einen Arbeitsplatz zu ermöglichen, kann im Extenderbetrieb die Berechtigung für den exklusiven Zugriff des Arbeitsplatzes aktiviert werden.

Ist diese Funktion eingeschaltet, kann die exklusive Bedienung mit einer Tastenkombination aktiviert werden. Sofort nach Betätigung dieser Tastenkombination sind die Eingabegeräte des konkurrierenden Arbeitsplatzes deaktiviert. Durch erneutes Ausführen der Tastenkombination am aktiven Arbeitsplatz, wird die Bedienung wieder für alle Arbeitsplätze freigeschaltet.

TIPP: In der Standardkonfiguration wird das Videosignal des Rechners sowohl am Monitor des aktiven als auch am Monitor des konkurrierenden Arbeitsplatzes ausgegeben. Ändern Sie ggf. die Videobetriebsart der Arbeitsplätze, um das Bild des konkurrierenden Arbeitsplatzes auszuschalten, während Sie den Rechner an einem anderen Arbeitsplatz bedienen.

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

HINWEIS: Weitere Informationen zu den Konfigurationseinstellungen finden Sie im separaten Handbuch zur Webapplikation der *Vision-Serie (digital)*.

Konfiguration

Die Konfiguration des in der **VisionVS-IP** integrierten Rechnermoduls kann wahlweise im On-Screen-Display (OSD) auf dem Monitor des Arbeitsplatzes oder über die Webapplikation **Config Panel** durch den Anwender geändert werden:

- Das *On-Screen-Display* wird auf dem Monitor des Arbeitsplatzes angezeigt. Die meisten Konfigurationseinstellungen können Sie im OSD direkt am Arbeitsplatz einstellen.

TIPP: Weitere Informationen zu den Konfigurationseinstellungen finden Sie im separaten Handbuch zur Konfiguration des eingesetzten Matrixswitches oder – falls die **VisionVS-IP** im direkten Extenderbetrieb eingesetzt wird – im separaten Handbuch zur Installation und Bedienung des eingesetzten Arbeitsplatzmoduls.

- Mit der Webapplikation **Config Panel** steht eine grafische Benutzeroberfläche zur Konfiguration und Überwachung des KVM-Extenders über einen Webbrowser zur Verfügung.

Grundlegende Bedienung der Webapplikation

Die Webapplikation **Config Panel** bietet eine grafische Benutzeroberfläche zur Konfiguration und Überwachung des in der **VisionVS-IP** integrierten Rechnermoduls.

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

WICHTIG: Grundlegende Informationen zu den Systemvoraussetzungen, der erforderlichen Konfiguration der Netzwerkschnittstellen der **VisionVS-IP**-Geräte und zum Einsatz der Webapplikation finden Sie im separaten Handbuch zur Webapplikation der *Vision-IP-Serie*.

Start der Webapplikation

So starten Sie die Webapplikation Config Panel:

1. Geben in der Adresszeile folgende URL ein:

   https://[IP-Adresse des integrierten Rechnermoduls]

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

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

WICHTIG: Ändern Sie das voreingestellte Passwort des Administratorkontos!

Die *voreingestellten* Zugangsdaten zum Administratorkonto lauten:

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

HINWEIS: Die Felder *Bedingungen* und *Akzeptieren* erscheinen nur, wenn das Anzeigen von Nutzungsbedingungen aktiviert wurde.

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

3. Klicken Sie auf **Login**.

Sprache der Webapplikation auswählen

So ändern Sie die Sprache der Webapplikation:



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

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

Webapplikation beenden

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

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

Die Webapplikation wird so gegen unautorisierten Zugriff geschützt.

So beenden Sie die Webapplikation:



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

Weiterführende Informationen

Empfehlungen zu den Twisted-Pair-Kabeln

Die **VisionVS-IP** ist mit einer **Transmission**-Schnittstelle ausgestattet, über die folgende Daten übertragen werden:

- **Transmission:** Tastatur, Video, Maus, Audio, RS232

In den folgenden Abschnitten erhalten Sie Empfehlungen bezüglich des Einsatzes bestimmter Twisted-Pair-Kabel.

> **HINWEIS:** Das Verbinden mehrerer Teilstrecken einer Kabelverbindung über Patchfelder und Anschlussdosen ist möglich.
>
> Die Einbindung aktiver Komponenten wie Netzwerk-Switches, Hubs oder Repeater, ist nicht zulässig.

Übertragung der KVM-Daten (Transmission)

Die Übertragung der Signale *Tastatur*, *Video*, *Maus*, *Audio* und *RS232* der **VisionVS-IP** erfolgt über Twisted-Pair-Kabel der Kategorie 5e (oder höher).

Abhängig von der Drahtstärke und des Kabeltyps der Twisted-Pair-Verkabelung können folgende Entfernungen zwischen der **VisionVS-IP** und einem Matrixswitch oder einem Arbeitsplatzmodul überbrückt werden:

Drahtstärke	Kabeltyp	Kategorie	Empfehlung
AWG 22	Installationskabel	5e, 6 oder 7	bis 140 Meter
AWG 24	Installationskabel	5e, 6 oder 7	bis 100 Meter
AWG 26	Patchkabel	5e, 6 oder 7	bis 80 Meter

Während des Testbetriebs unter Laborbedingungen haben folgende Kabel die besten Ergebnisse erzielt:

- **bis 140 Meter:** Kerpen MegaLine ® G12-150 S/F (AWG 22)
- **bis 100 Meter:** Dätwyler uninet ® 5502 S-STP (AWG 24)
- **bis 80 Meter:** Dätwyler uninet ® 7702 Flex (AWG24)

DDC-Weiterleitung mit Cache-Funktion

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

Damit der an der **VisionVS-IP** angeschlossene Rechner schon während des Bootvorgangs Zugriff auf die Eigenschaften des entfernten Monitors hat, ist eine Cache-Funktion in den KVM-Extender integriert. Auch wenn das Rechner- oder das Arbeitsplatzmodul ausgeschaltet oder nicht miteinander verbunden sind, stehen entweder die Eigenschaften des zuletzt angeschlossenen Monitors oder die Werksvorgabe des KVM-Extenders zu Verfügung.

Üblicherweise werden die DDC-Informationen des Monitors unverändert an den Rechner weitergeleitet. Stellt der KVM-Extender aber fest, dass sich die Informationen des Monitors nicht vollständig auslesen lassen oder diese unzulässige Einträge enthalten, werden die Informationen (wenn möglich) vervollständigt oder korrigiert.

Ermittlung der Netzwerkeinstellungen über den Service-Port

Falls Ihnen die IP-Adresse eines Arbeitsplatz- oder Rechnermoduls unbekannt ist, können Sie diese über den Service-Port des Moduls anzeigen.

Verwenden Sie ein beliebiges Terminalemulationsprogramm (beispielsweise *Tera Term* oder *PuTTY*) um die Log-Meldungen der Module anzuzeigen.

Installation des Gerätetreibers

Installieren Sie vor der Einrichtung der Verbindung im Terminalemulations-programm den Gerätetreiber **CP210x USB to UART Bridge VCP**.

> **HINWEIS:** Der Treiber stellt die per Servicekabel verbundene *Service*-Buchse eines Arbeitsplatz- oder Rechnermoduls als *virtuelle* serielle Schnittstelle (COM-Port) zur Verfügung. Die virtuelle Schnittstelle kann anschließend im Terminal-emulationsprogramm zum Verbindungsaufbau ausgewählt werden.

So installieren Sie den Gerätetreiber zur Adressierung der Service-Buchse:

1. Öffnen Sie im Webbrowser des Computer die Website **www.gdsys.com/de**.
2. Navigieren Sie in den Bereich **Service > Downloads > Tools & Treiber** der Website.
3. Downloaden Sie den Gerätetreiber für das Betriebssystem des Computers.
4. Führen Sie die Datei aus und folgen Sie den Hinweisen des Installationsassistenten.

Einrichten einer Verbindung im Terminalemulationsprogramm

So richten Sie die Verbindung im Terminalemulationsprogramm ein:

1. Starten Sie ein beliebiges Terminalemulationsprogramm (beispielsweise *Tera Term* oder *PuTTY*).
2. Erstellen Sie eine neue Verbindung im Terminalemulationsprogramm und erfassen Sie folgende Verbindungseinstellungen:
   - Bits pro Sekunde: 115.200
   - Datenbits: 8
   - Parität: Keine
   - Stoppbits: 1
   - Flusssteuerung: Keine
3. Verwenden Sie das mitgelieferte USB-Servicekabel, um den Rechner mit der *Service*-Buchse an der Vorderseite des Arbeitsplatz- bzw. Rechnermodul zu verbinden.

Ermittlung der IP-Adresse

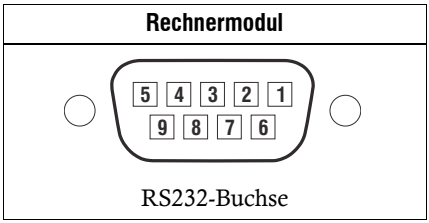
So ermitteln Sie die IP-Adresse des Arbeitsplatz- bzw. Rechnermoduls:

1. Starten Sie das Arbeitsplatz- bzw. Rechnermodul neu.

   Während des Bootvorgangs werden verschiedene Statusmeldungen im Terminalemulationsprogramm angezeigt.
2. Nach Abschluss der Boot-Vorgangs wird die IP-Adresse gemeinsam mit anderen **Systeminformationen** ausgegeben.

Pin-Belegung der RS232-Buchse/Schnittstelle

Die Pin-Belegungen der RS232-Buchse zeigt die folgende Abbildung:



Die Tabelle zeigt die Zuordnung der verschiedenen Leitungen der Datenverbindung zu den entsprechenden Pins auf:

Pin-Nr.	Leitung	Rechnermodul
1	DCD (Data Carrier Detect)	Ausgang
2	RxD (Receive Data)	Ausgang
3	TxD (Transmit Data)	Eingang
4	DTR (Data Terminal Ready)	Eingang
5	GND (Ground)	Ground
6	DSR (Dataset Ready)	Ausgang
7	RTS (Request to Send)	Eingang
8	CTS (Clear to Send)	Ausgang
9	*nicht belegt*	n/c

Statusanzeigen

Die LEDs an der Vorder- und Rückseite der **VisionVS-IP** geben Ihnen die Möglichkeit, den Betriebsstatus des KVM-Extenders jederzeit zu kontrollieren.

Bedeutung der LEDs an der Vorderseite

Bereich	LED	Farbe	Status	Bedeutung
Ident.	**Ident.**	blau	an	Leuchtet, sobald die LED über die Webapplikation aktiviert wurde.
Power	**Red.**	grün	an	Das optionale Netzteil ist angeschlossen und eine Spannung von 12 Volt verfügbar.
			aus	Das optionale Netzteil ist nicht (korrekt) angeschlossen.
	Main	grün	an	Das Netzteil ist eingeschaltet und liefert die erforderliche Spannung.
			aus	Das Netzteil ist ausgeschaltet oder die Verbindung mit dem Stromnetz nicht hergestellt.
Status	**K/M**	grün	an	Die Tastatur wurde erkannt.
			blinkt	Keine Tastatur angeschlossen oder nicht erkannt.
	System	grün	an	Gerät betriebsbereit.
			blinkt	Update wird ausgeführt.
			blinkt schnell	Rücksetzung auf Werkseinstellungen nach langem Druck auf den Reset-Taster.
		rot	an	interner Fehler oder Gerät bootet
Channel	**Video**	gelb	an	Am Videoeingang wurde ein stabiles Bildsignal festgestellt.
			aus	Das eingehende Videosignal wurde nicht erkannt oder es ist qualitativ nicht ausreichend, um verarbeitet zu werden.
	Trans.	gelb	an	Es besteht eine aktive Verbindung zur Gegenstelle.
			aus	Es besteht keine aktive Verbindung zur Gegenstelle.
Management	**links**	gelb	an	Die Verbindung mit dem Netzwerk wurde erfolgreich aufgebaut.
			aus	Es konnte keine Verbindung hergestellt werden.
	rechts	grün	flackert	Netzwerkaktivität findet statt.
			aus	keine Netzwerkaktivität

Bedeutung der LEDs an der Rückseite (CAT-Variante)

Bereich	LED	Status	Bedeutung
Transmission	**gelb**	an	Kommunikation mit Gegenstelle hergestellt.
		blinkt	Verbindung zur Gegenstelle hergestellt.
		aus	Verbindung zur Gegenstelle nicht hergestellt.
	grün	an	An Gegenstelle angemeldet.
		aus	An Gegenstelle nicht angemeldet.

Bedeutung der LEDs an der Rückseite (Fiber-Variante)

Bereich	LED	Status	Bedeutung
Transmission	**gelb**	an	Kommunikation mit der Gegenstelle erfolgreich aufgebaut
		blinkt	Es kann nur über die Rx-Schnittstelle eine Verbindung zur Gegenstelle aufgebaut werden. Prüfen Sie die Kabelverbindung der Tx-Schnittstelle mit der Gegenstelle.
		blinkt schnell	inkompatibles SFP-Modul
		aus	Verbindung zur Gegenstelle kann nicht hergestellt werden.
	grün	an	An Gegenstelle angemeldet.
		aus	An Gegenstelle nicht angemeldet.

Verwendete Netzwerk-Ports und Protokolle

HINWEIS: Eine Übersicht über die Netzwerk-Ports und Protokolle, die bei KVM-over-IP von G&D verwendet werden können, finden Sie im separaten Handbuch zur Webapplikation.

Technische Daten

Allgemeine Eigenschaften der Serie

VISIONVS-IP-SERIE		
Schnittstellen für Rechner	Video:	1 × DisplayPort-Buchse
	USB-Tastatur/Maus:	1 × USB-B-Buchse
	Audio:	3,5-mm-Klinkenbuchse (Line In) 3,5-mm-Klinkenbuchse (Line Out)
	RS232:	1 × RS232-Buchse
Schnittstellen für lokalen Arbeitsplatz	Monitor:	1 × HDMI (HDMI Out)
	USB-Tastatur/Maus:	2 × USB-A-Buchse
Schnittstellen zur KVM-Gegenstelle	KVM, Audio und RS232:	‣ siehe spezifische Eigenschaften
	Übertragungsart:	KVM-over-IP™
Sonstige Schnittstellen	Netzwerkanbindung:	1 × RJ45-Buchse (Management)
		1 × RJ45-Buchse (Network)
	Service:	1 × Mini-USB-Buchse (Typ B)
	Control:	5-poliger Klemmblock (nicht unterstützt)
Audio ‣ DisplayPort Digital	Übertragungsart:	2-Kanal-LPCM, stereo
	Auflösungen:	16/20/24 bit
	Abtastraten:	bis 48 kHz
Audio	Übertragungsart:	transparent, bidirektional
	Auflösung:	24 bit digital, Stereo
	Abtastrate	96 kHz
	Bandbreite:	22 kHz
RS232	Übertragungsart:	transparent
	Übertragungsrate:	max. 115.200 bit/s
	Übertragene Signale:	RxD, TxD, RTS, CTS, DTR, DSR, DCD

VISIONVS-IP-SERIE		
Grafik (Videoeingang)	Format:	DisplayPort (DP 1.1a)
	Farbtiefe:	24 bit
	Pixelrate:	ca. 25 bis 300 MP/s
	max. Auflösung:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Auflösungsbeispiele:	▪ 4096 × 2160 (24 oder 25 Hz) ▪ 3840 × 2160 (24, 25 oder 30 Hz) ▪ 2048 × 2160 (60 Hz) ▪ 2048 × 2048 (60 Hz) › Weitere VESA und CTA standardisierte Auflösungen im Rahmen der Videobandbreite/Pixelrate und Horizontal-/Vertikalfrequenz möglich.
	Vertikalfrequenz:	24 Hz bis 120 Hz
	Horizontalfrequenz:	25 kHz bis 185 kHz
Grafik (Videoausgang)	Format:	HDMI 1.4
	Farbtiefe:	24 bit
	Pixelrate:	ca. 25 bis 297MP/s
	max. Auflösung:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Auflösungsbeispiele:	▪ 4096 × 2160 (24 oder 25 Hz) ▪ 3840 × 2160 (24, 25 oder 30 Hz) ▪ 2048 × 2160 (60 Hz) ▪ 2048 × 2048 (60 Hz) › Weitere VESA und CTA standardisierte Auflösungen im Rahmen der Videobandbreite/Pixelrate und Horizontal-/Vertikalfrequenz möglich.
Hauptstromversorgung	Typ:	internes Netzteil
	Anschluss:	Kaltgerätestecker (IEC-320 C14)
	Spannung:	100-240 VAC/60-50Hz
redundante Stromversorgung	Typ:	externes Netzteil
	Anschluss:	miniDIN-4 Power-Buchse
	Spannung:	12 VDC
Einsatzumgebung	Temperatur:	+5C bis +40°C
	Luftfeuchte:	20% bis 80%, nicht kondensierend
Lagerumgebung	Temperatur:	-20°C bis +60°C
	Luftfeuchte:	15% bis 85%, nicht kondensierend

Spezifische Eigenschaften der CAT-Variante

VISIONVS-IP-CAT		
Schnittstelle zur KVM-Gegenstelle	KVM, Audio und RS232:	1 × RJ45-Buchse
Gehäuse	Material:	Aluminium eloxiert
	Dimensionen (B × H × T):	ca. 436 × 44 × 284 mm
	IP-Schutzklasse:	IP20

Spezifische Eigenschaften der Fiber-Varianten

VISIONVS-IP-FIBER		
Schnittstelle zur KVM-Gegenstellen	KVM, Audio und RS232:	1 × LC-Duplex-Buchse, inkl. Übertragungsmodul/ SFP-Transceiver
Gehäuse	Material:	Aluminium eloxiert
	Dimensionen (B × H × T):	ca. 436 × 44 × 284 mm
	IP-Schutzklasse:	IP20

Eigenschaften der Übertragungsmodule

MULTIMODE-ÜBERTRAGUNGSMODUL		
Datenübertragung	Art:	Lichtwellenleiter (2 Glasfasern)
	Schnittstellentyp:	LC-Duplex
Kabellänge (max.)	Multimode 50/125µm, Klasse OM4:	550 Meter (Fasern mit 4700MHz*km)
	Multimode 50/125µm, Klasse OM3:	550 Meter (Fasern mit 2000MHz*km)
	Multimode 50/125µm, Klasse OM2:	550 Meter (Fasern mit 500MHz*km)
	Multimode 50/125µm:	500 Meter (Fasern mit 400MHz*km)
	Multimode 62,5/125µm, Klasse OM1:	275 Meter (Fasern mit 200MHz*km)
	Multimode 62,5/125µm, FDDI-Grade:	220 Meter (Fasern mit 160MHz*km)

SINGLEMODE-ÜBERTRAGUNGSMODUL		
Datenübertragung	Art:	Lichtwellenleiter (2 Glasfasern)
	Schnittstellentyp:	LC-Duplex
Kabellänge (max.)	Singlemode 9/125µm, Klasse OS1:	10 Kilometer (Fasern mit 500MHz*km)

NOTIZEN

NOTIZEN

About this manual

This manual has been carefully compiled and examined to the state-of-the-art.

G&D neither explicitly nor implicitly takes guarantee or responsibility for the quality, efficiency and marketability of the product when used for a certain purpose that differs from the scope of service covered by this manual.

For damages which directly or indirectly result from the use of this manual as well as for incidental damages or consequential damages, G&D is liable only in cases of intent or gross negligence.

Caveat Emptor

G&D will not provide warranty for devices that:

- Are not used as intended.
- Are repaired or modified by unauthorized personnel.
- Show severe external damages that was not reported on the receipt of goods.
- Have been damaged by non G&D accessories.

G&D will not be liable for any consequential damages that could occur from using the products.

Proof of trademark

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.

© Guntermann & Drunck GmbH 2026. All rights reserved.

Version 1.01 – 20/01/2026
Firmware: 2.4.000 | 4.4.3

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 A digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Table of contents

Safety instructions **1**

The VisionVS-IP series **5**
Signal transmission and transmission length 6

Package contents **7**

Secure KVM-over-IP solution **8**
Potential security vulnerabilitites, threats and dangers 8
Protection of KVM systems from external or internal attacks 8
Security requirements with KVM-over-IP 8
The secure solution from G&D 9
Trusted Computing Platform 11
Monitoring, SNMP and Syslog 11
Update and Backup/Restore 11
Further security-relevant aspects 12
2-factor authentication (2FA) 12

Signal transmission and transmission length **13**

Selecting a network switch **13**
Requirements of network switches 13

Installation **15**
Preparation 15
Installing the VisionVS-IP 16
Installing a KVM-over-IP counterpart 21

Start-up **22**

Starting process **22**

Initial configuration of the network settings **23**

Establishing a KVM-over-IP™ connection for the first time **24**
Default setting of the modules 25
Configuring a KVM-over-IP connection of a computer module 26
Configuring the global network settings 26
Configuring a KVM-over-IP connection 26
Extended settings of KVM-over-IP connection 27
Limiting the bandwidth 27
Classifying IP packets (DiffServ) 27
(De)Activating signals 27
Restricting KVM-over-IP remote stations (UID locking) 28

Integration into the AV solution and RemoteAccess **29**
Access the HTML KVM client 29
On a DHCP network 30
On a static network 30
Change the default admin credentials 31
Establishing a connection 31
Network settings 32
Change password 33
Video settings 34
VuStream-350 KVM Driver install 34
VuStream-350 KVM Driver uninstall 34
Update firmware 35
Factory reset 36

Operation **37**
Concurrent operation 37
Exclusive operation 38

Configuration **39**
Basic operation of the web application 39
Starting the web application 40
Selecting the language of the web application 41
Closing the web application 41

Further information **42**
Recommendations for twisted pair cables 42
Transmission of KVM data 42
DDC transmission with cache function 43
Determining network settings via service port 43
Installing the device driver 43
Establishing a connection by using a terminal emulator 44
Determining the IP address 44
Pin assignment of the RS232 socket/interface 45

Status LEDs **46**
Meaning of the LEDs on the front panel 46
Meaning of the LEDs on the back panel (CAT variant) 47

Technical data **48**
General features of the series 48
Specific features of the CAT variant 50
Specific features of fiber variants 51
Features of transmission modules 52

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.

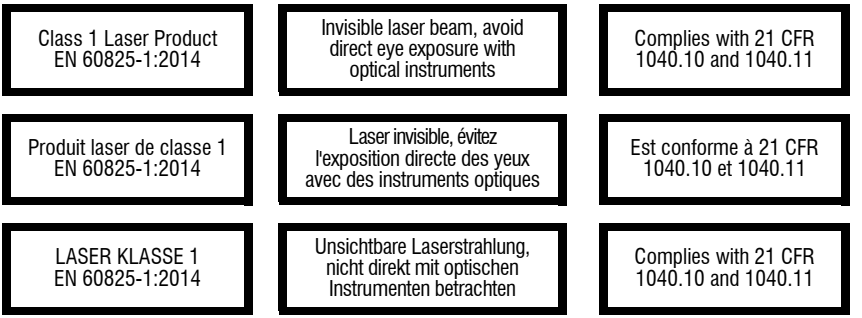
Entsorgen Sie gebrauchte Batterien umweltgerecht. Gebrauchte Batterien dürfen nicht in den Hausmüll geworfen werden.

Beachten Sie die gültigen Vorschriften zur Entsorgung elektronischer Produkte.

Special advices for dealing with laser technology

The devices of the **VisionVS-IP-Fiber** series use components with laser technology which comply with laser class 1 or better.

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



Mind the following advices when dealing with laser beams:

⚠ Avoid direct eye exposure to beam

Never stare directly into the beam when wearing optical instruments!

⚠ Always connect optical connections or cover them with protection caps

Always cover the optical connections of the *Transmission* socket and the cable plugs with a connector or a protection cap.

⚠ Only use G&D certified transmission modules

It is not permitted to use fibre optic modules, which do not meet the requirements of laser class 1 in accordance to **EN 60825-1:2014**. By using such modules, the compliance with regulations and advices for the safe handling of laser technology cannot be guaranteed.

The guarantee of complying with all relevant instructions can only be given by applying original components. Therefore, the devices have to be operated with G&D certified transmission modules only.

The VisionVS-IP series

The **VisionVS-IP** combines a *DP-Vision-IP* computer module with a *VuStream-350* in a single housing. It is therefore a hybrid computer module with a dual encoder that transmits KVM signals with virtually zero latency and in lossless quality to the workplace via a G&D KVM-over-IP matrix from G&D. In parallel, it enables low-latency streaming to *VuWall PAK* devices for remote access to the computer or for flexible video wall management. The appliance is part of a modular system solution and requires additional components for operation.

This combined product enables integrated system solutions that unite G&D's high-quality KVM-over-IP technology with VuWall's flexible video wall solutions and centralized, computer level remote access – ideal for modern control room and command center environments. You benefit from G&D's signature fast and seamless workplace operation, along with the ability to display content simultaneously in multiple locations—at the workstation, on the video wall, or via remote access.

NOTE: The **VisionVS-IP** is compatible – depending on the variant – with existing G&D product families (*Vision-IP*, *VisionXS-IP*, *ControlCenter-IP*, *ControlCenter-IP-XS*). The streaming output is compatible with VuWall *PAK* and *TRx*.

If you have questions about compatibility, please contact the support team.

As an alternative to matrix operation, you can also use the **VisionVS-IP** in extender mode with a compatible console module.

Configure a KVM-over-IP connection between the **VisionVS-IP** and a compatible console module. The configured connection between the modules is restored each time the modules are restarted.

Signal transmission and transmission length

G&D's **KVM-over-IP™** technology makes it possible to transmit signals between the computer and the console module compressed and encrypted (AES-128) using Gigabit Ethernet (Layer 3).

If the bandwidth of the Gigabit Ethernet is sufficient, the video signal is reproduced in a loss-free video quality and almost without any latency. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

When observing the max. length of sections between two *active* network components, the entire transmission length is unrestricted.

Package contents

Standard package contents of the VisionVS-IP series

- 1 × **VisionVS-IP**, fiber variants incl. transmission module/SFP transceiver
- 1 × power cable (*PowerCable-2 Standard*)
- 1 × video cable (*DP1.4-Cable-M/M-2*)
- 1 × USB device cable (*USB-AM/BM-2*)
- 1 × audio cable (*Audio-M/M-2*)
- 1 × serial connection cable (*RS232-M/F-2*)
- 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.

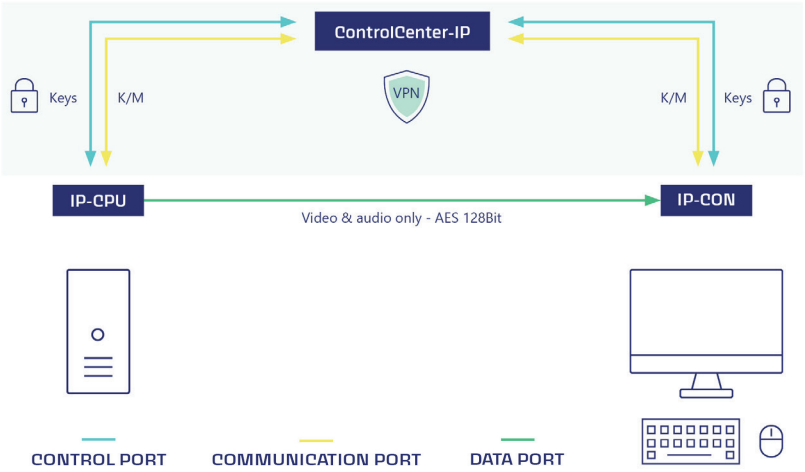
With KVM-over-IP systems, transmission is based on IP and runs on Gigabit Ethernet networks (OSI model layer 3). Using KVM-over-IP provides a future-proof solution due to its flexibility and easy expandability. However, IP transmission also increases security risks. There is an additional external risk, 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 respective counterpart or to the KVM-over-IP matrix Control-Center-IP or ControlCenter-IP-XS. An AES256 Galois/Counter Mode (GCM) encrypted IPSec VPN tunnel is used (GCM is based on Counter Mode CTR, but also offers integrated integrity protection). There is also downward compatibility for AES128-GCM.



The first port that is established from all KVM-over-IP end devices to the respective counterpart or to the matrix is the so-called control port. The communication between the end devices or with the matrix is negotiated through a self-developed authentication plug-in. This ensures that only G&D devices can establish a connection based on their UID, serial number and the Trusted Platform Module. The control port is also used to exchange the respective security keys the KVM-over-IP matrix generates within matrix operation or the computer module generates within extender operation for each end device.

The keyboard and mouse data are transmitted bidirectionally via the second port, the so-called communication port.

The key exchange for the highly security-relevant keyboard and mouse data as well as the control data is fully dynamic and occurs every 40 to 80 minutes.

Video data is transmitted directly from the computer module to the console module via UDP and MultiCast/UniCast (data port). For audio, GenericUSB and RS232 data as well as the video stream, which is converted to G&D's own proprietary protocol before being sent, AES128 Counter Mode (CTR) is used. A secret device key, which is required to unpack the video data, provides additional protection.

The proprietary protocol for dedicated connections is supplemented by fully dynamic encryption for KVM-over-IP. The key exchange for this high-speed data takes place every three to five hours or in the case of switching events. Each time a console module connects to a computer module, a security key is generated for that connection. Whenever another console module connects to this computer module within matrix operation, both console modules receive new security keys. In reverse, a new security key is also sent to the remaining console module when the other module is disconnected.

By separating control data (control port) and keyboard and mouse data (communication port) from video, audio, GenericUSB and RS232 data (data port), diverse attack scenarios, such as man-in-the-middle attacks, are prevented from the outset. If the target IP address or VPN tunnel is compromised, no new security keys are issued and the KVM end devices as well as the matrix system switch to security mode and stop the transmission of data.

Trusted Computing Platform

The bootloader, the operating system and the firmware of the devices form a Trusted Computing Platform. Based on a core component complying with the FIPS140-2 security standard, an integrated Trusted Platform module secures all access and configuration data against third-party spying or manipulation. Here, an RSA encryption method with a key length of 2048 bits is used.

Sensitive data such as login information and passwords are stored permanently and encrypted in the database of the ControlCenter-IP or ControlCenter-IP-XS within matrix operation or in the database of the computer module within extender operation. This database is implemented in G&D's operating system, is TPM-protected and with the ControlCenter-IP additionally based on a hardware raid. Possible firmware modifications can be detected at an early stage, leading to an interruption of the boot process. Thus, any attempts at manipulation, such as smuggling in a keyboard sniffer, are prevented.

TPM ensures that a device is only booted with software that has been classified as trustworthy by the manufacturer.

Monitoring, SNMP and Syslog

Monitoring and SNMP features enable system administrators to monitor the status of devices installed and peripherals connected. Any information is provided via the web interface of the respective devices. Permanent detection and reporting makes it possible to react at an early stage to critical conditions such as exceeding temperatures, loss of communication on the keyboard interface, or a compromised redundancy system. This preemptively prevents system failures, increases the system's availability and allows operators and system administrators to work more efficiently.

Syslog (System Logging Protocol) is used to generate various events in response to changing conditions. The events are logged locally and can be checked and analyzed by an administrator. The syslog messages can also be sent to a syslog server. Syslog can be used, for example, to log relevant system changes, logins and login failures.

Update and Backup/Restore

Configuration settings can be saved using the backup function. With the auto backup function an automatic backup can be saved on a network drive at a defined interval. This means there ist no need to make a manual backup after a configuration option has been changed. Backed-up data can be restored using the restore function.

Further security-relevant aspects

All G&D computer modules (CPUs) can be configured to automatically log off the computer‘s operating system when a user logs off the console module. This prevents unintentional open access to the computer and the possibility of another user accessing the computer without logging in.

The use of optional UID locking reliably restricts the end devices that can be used. Once activated, no further end devices can be added or replaced.

Optional USB 2.0 data connections can also be disabled via intelligent user management at hardware level.

Another important aspect is the security of the device on the user side. G&D KVM end devices do not store any information. It is therefore not possible to read out a stolen device to obtain cached login data.

The system wide password complexity (minimum password length, mimimum number of capitals/lowercases, minimum number of digits, minimum number of special characters, minimum number of characters that must be different compared with the previous password) can be configured to comply with individual password guidelines and to improve security.

To enhance security, further configuration options are available in the login options area. It is possible to specify how many failed attempts are accepted when entering a password and how long a user is locked out after exceeding the maximum number of failed attempts. In this area, it can also be determined how many simultaneous superuser sessions are permitted.

In addition, terms of use can be stored that a user must accept before each (new) device access.

2-factor authentication (2FA)

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

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

Signal transmission and transmission length

G&D's **KVM-over-IP™** technology (see *The secure solution from G&D* on page 9) makes it possible to transmit signals between the computer and the console module compressed and encrypted using Gigabit Ethernet (Layer 3). Alternatively, the computer module and the console module can also be connected directly to each other. In this case, the transmission length is limited.

If the bandwidth of the Gigabit Ethernet is sufficient, the video signal is reproduced in a loss-free video quality and almost without any latency. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

When observing the max. length of sections between two *active* network components, the entire transmission length is unrestricted.

Selecting a network switch

NOTE: No *multicast* transmission is provided within extender operation. This places significantly fewer requirements on the network switch than is the case within matrix operation.

IMPORTANT: If possible, the network switches should also meet the requirements for matrix operation (*Multicast*, *IGMP*, *IGMP Snooping*, *IGMP Snooping Querier*, *Fast Leave/Immediate Leave* and *Spanning Tree TCN Flooding*) with regard to system expansion. Further information on this can be found in the installation manual of the matrix switch.

Requirements of network switches

The following requirements apply to the network:

- At least **Layer 2 managed switch**
- **VLAN support** to separate KVM-over-IP™ traffic from other network operations.

- **QoS with DiffServ/DSCP** support for performance enhancement and prioritization:
  Quality of Service (QoS) is a packet prioritization mechanism that ensures time-critical or important applications receive their data preferentially over the network.
  With DiffServ / DSCP support, data packets are marked and processed by the network according to the configuration. DSCP specifies how exactly a packet is handled.

> **NOTE:** Take into consideration that some network switches automatically assign the service class **Network Control** (DSCP name: **CS6**) for *all* data packets. In such environments, the **DSCP 48** option must not be selected!

- **Ensure adequate performance** of the network switch: check forwarding bandwidth, switching capacity, and forwarding performance.

> **EXAMPLE:** Typical bandwidth requirements for KVM-over-IP
>
> VisionXS-IP models are available in several variants: DVI-I, DP-HR and DP-HR-DH with 1 Gbit; DP-UHR and TypeC-UHR with multi-Gbit (1-10 Gbit). The bandwidth is unlimited by default but can optionally be restricted.
>
> - 1920 × 1080 = 300-400 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DVI-I)
> - 2560 × 1440 = 500-600 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-HR)
> - 2 × 2560 × 1440 = 800-900 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-HR-DH)
> - 3840 × 2160 = 2000-2500 Mbit/s
>   (office application with approx. 40% of change: e.g. VisionXS-IP-DP-UHR)
>   the maximum video bandwidth usage is 5 Gbit/s
> - Static image: 25 Mbit/s at 3840 × 2160

> **IMPORTANT:** Make sure that the uplink from access switch to core/main switch is sufficiently dimensioned for the number and operating mode of the connected end devices.

> **EXAMPLE:**
>
> - 30 × *VisionXS-IP-DP-HR-CPU* at 10Gbit uplink
> - uplink with 10 Gbit/s is a bottleneck, since 30 × 1Gbit/s would have to be ensured with the CPUs.

Installation

IMPORTANT: The fiber variants of the VisionVS series use components with laser technology which comply with laser class 1.

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

Consider the following safety guidelines regarding this matter:

- *Avoid direct eye exposure to beam* on page 4
- *Always connect optical connections or cover them with protection caps* on page 4

Preparation

IMPORTANT: When choosing a location for the devices, please ensure to comply with the ambient temperature limit (see *Technical data* on page 48 ff.) close to the device. The ambient temperature limit must not be influenced by other devices.

When installing the devices, make sure to only place a maximum of three devices directly on top of each other. This way, a good circulation of air is provided and mutual thermal interference can be avoided. After having installed three devices, provide for a distance (at least 2 cm).

1. Ensure that the computer to be connected to the **VisionVS-IP** is switched off. If the computer is provided with keyboard and mouse, unplug the cables of the input devices from the interfaces.
2. Place the **VisionVS-IP** close to the computer.

   NOTE: Please mind the maximum cable length of *five* meters between the **VisionVS-IP** and the computer to be connected.

Installing the VisionVS-IP

Connect the computer whose signals are to be transmitted to the remote console, to the video wall, or for remote access to the **VisionVS-IP**. If desired, connect a local console to the **VisionVS-IP** (see *Optional: Connecting a local console* on page 18).

Establishing a connection to a local network



NOTE: If desired, connect the management interface to a local network. This enables you to access the **Config Panel** web application of the into the **VisionVS-IP** integrated computer module from this network and to send syslog messages to this network.

Management: Insert a category 5 twisted pair cable (or better), which is available as accessory. Connect the other end of the cable to the local network.

Connecting keyboard and mouse to the computer



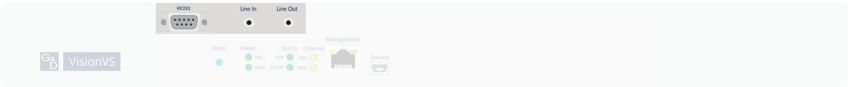
USB CPU: Use the *USB-AM/BM-2* cable to connect one of the computer's USB interfaces to this interface.

Connecting the computer's video output



DisplayPort CPU: Use the *DP1.4-Cable-M/M-2* cable to connect the computer's video output to this interface.

Connecting audio and RS232 interfaces



NOTE: By *default*, the KVM extender transfers audio data. The transmission of RS232 data is deactivated.

You can enable the transmission of RS232 data and/or disable the transmission of audio data.

Line In: Use an *Audio-M/M-2* audio connection cable to connect the omputer's *Line-Out* interface to this interface

Line Out: Use an *Audio-M/M-2* audio connection cable to connect the omputer's *Line-In* interface to this interface.

RS232: Use the *RS232-M/F-2* cable to connect one of the computer's 9-pin serial interfaces to this interface.

IMPORTANT: The audio and RS232 data are transmitted only via KVM-over-IP connection and **not** through the streaming output.

Optional: Connecting a local console



HDMI Out: Connect the monitor of the local console.

USB K/M: Connect the USB keyboard and/or the USB mouse of the local console.

Further interface



Control: Reserved for future functions.

Establishing a connection to a network to integrate the VisionVS-IP into the AV solution

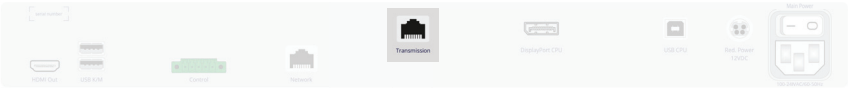


Network: Plug in a category 5e (or higher) twisted-pair cable, which is available as accessory. Connect the other end of the cable to a the same network on which your AV solution is running or through which remote access is to be provided.

> **NOTE:** You can also the **VisionVS-IP/VuStream-350** to your application without using the *VuWall PAK KVM feature* of *TRx*. In this case, you can simply establish a connection to the **VisionVS-IP** and the remote computer via Gigabit Ethernet (see *Integration into the AV solution and RemoteAccess* on page 29 ff.).

Establishing a connection to the Gigabit Ethernet

CAT variants:



Transmission: Plug a category 5e (or better) twisted pair cable, which is available as accessory, into this interface. Connect the other end of the cable to the Gigabit Ethernet.

Fiber variants:



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

Never stare directly into the beam when wearing optical instruments!

NOTE: Remove the protection caps from the *Transmission* interfaces and from the cable plug.

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

Transmission|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.

Establishing the power supply

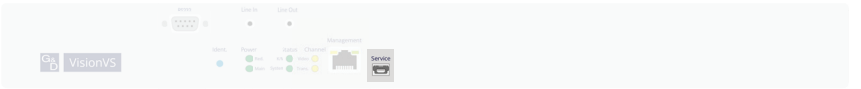


Main Power: Insert one of the supplied IEC cables here.

Red. Power: To provide a second, redundant power supply, connect a portable power pack to this interface.

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 **VisionVS-IP** system, which is connected via service cable, as virtual serial interface (COM port). Now, the virtual interface can be selected in the terminal emulator to establish the connection.

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

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 **VisionVS-IP**.

NOTE: To log in into the service menu, enter the user name *service* and the password *service*.

4. In the service menu, you have the following options:
   - Quit
   - System information
   - Set system defaults: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Reboot: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.
   - Temporary deactivation of the network filter rules: A confirmation *Are you sure? [y]es, [N]o* (*default*) is displayed.

Installing a KVM-over-IP counterpart

Install a compatible KVM-over-IP matrix switch and/or a compatible console module as described in the corresponding manuals.

Start-up

After the proper installation of the devices they can be immediately put into operation.

Mind the following activation sequence when starting the devices:

1. Turn on the console module and/or the KVM-over-IP matrix switch.
2. Turn on the **VisionVS-IP**.
3. Turn on the computer that is connected to the **VisionVS-IP**.

NOTE: The recommended activation sequence ensures that the KVM extenders are able to read out the features of the connected monitor and to transmit them to the computer (see *DDC transmission with cache function* on page 43).

Starting process

After the **VisionVS-IP** is turned on, the LEDs on the front panel show the device's operating status.

For further information about this topic, also see the chapter *Status LEDs* on page 46 ff.

Initial configuration of the network settings

The *Management* interface allows the integration of a device into a separate network for accessing the web application and using the extended network functions (network filter, syslog,...) of the devices.

NOTE: In the default settings the following settings are preselected:

- IP address of *Network Interface »Network Management«*: **192.168.0.1**
- global network settings: obtain settings dynamically

The required configuration settings can be made in the web application of the integrated computer module.

IMPORTANT: For more information on the configuration settings, refer to the chapter *Initial configuration of the network settings* in the separate manual for the *Vision-IP Series* web application.

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

The **VisionVS-IP** series devices are equipped with three network interfaces:

- **Transmission:** The KVM data is transmitted via the interface to the counterpart station via a KVM-over-IP™ connection.
- **Management:** This interface allows the integration of a device into a separate network for accessing the web application and using the extended network functions (network filter, syslog,...) of the devices.
- **Network:** This interface establishes the connection to the VuWall server (see *Establishing a connection* on page 31).

IMPORTANT: Please mind the separate instructions regarding *Initial configuration of the network settings* on page 23.

IMPORTANT: If you use the **VisionVS-IP** as a matrix module with the IP matrix switch **ControlCenter IP** or **ControlCenter-IP-XS**, you can conveniently set up the **KVM-over-IP™ connection** via the web application of the IP matrix switch (see instructions for the *web application of the IP matrix switch*).

Manual configuration as described in this chapter is *not* necessary in this case.

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

The communication between two modules requires various settings. In the default settings, the modules are configured in a way that a computer and a console module can immediately establish a direct connection.

All computer modules are preconfigured with the IP address **172.17.0.10,** all console modules with the IP address **172.17.0.11**.

IMPORTANT: These IP addresses are preconfigured as '*fallback*' if no IP address could be obtained via a DHCP server during the boot process. If IP addresses are obtained via a DHCP server, the preconfigured IP addresses are no longer valid.

IMPORTANT: Change the default IP addresses before integrating several computer or console modules into the productive network.

ADVICE: If you do not know the IP address of an already configured console or computer module, it can be determined via the log messages of the device. For more information, see the section *Determining network settings via service port* on page 43.

Default setting of the modules

The default setting of the modules allows users to quickly establish a direct connection between a computer and a console module. The configuration of both modules can be adjusted after their initial operation.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Both the IP addresses and the **KVM-over-IP** settings are preconfigured as follows:

DEFAULT SETTING OF THE COMPUTER MODULE (CPU)	
IP address Transmission:	172.17.0.10
Netmask	255.255.0.0
Control port:	18246
Communication port:	18245
Data port:	18244

DEFAULT SETTING OF THE CONSOLE MODULE (CON)	
IP address Transmission:	172.17.0.11
Netmask	255.255.0.0
Local control port:	18246
Local communication port:	18245
Local data port:	18244
Remote host:	172.17.0.10
Remote control port:	18246

NOTE: The **IP address** of the computer module (host) as well as the **control port** of the computer module must be specified to establish a **KVM-over-IP** connection through the console module.

The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

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

Configuring a KVM-over-IP connection of a computer module

You can carry out the required configuration settings directly on the console.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Configuring the global network settings

Even in complex networks global network settings ensure that the KVM extender is available from all partial networks.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Configuring a KVM-over-IP connection

The **IP address** of the console module (host) as well as the **control port** of the computer module must be specified to establish a **KVM-over-IP** connection through the computer module.

NOTE: The configuration of both the **communication ports** and the **data ports** are automatically exchanged between the two modules.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Extended settings of KVM-over-IP connection

Limiting the bandwidth

By default, the KVM extender uses the maximum available bandwidth of a Gigabit Ethernet. By means of manual bandwidth management you can adapt the transmission to different bandwidth requirements.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Classifying IP packets (DiffServ)

For QoS purposes (Quality of Service) you have the possibility to use **Differentiated Services Codepoints** (DSCP) to classify the IP packets.

Through this classification, you can prioritize the data packets, for example, through a switch.

You can define a DSCP for the IP packets of the keyboard, mouse and control data (**Communication** data packets), as well as the IP packets of the video, audio and RS232 data (**Data** data packets).

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

(De)Activating signals

By default, not only keyboard, video and mouse data but also audio data are transmitted.

In addition, you can enable the transmission of RS232 data and, alternatively, disable the transmission of audio data.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Restricting KVM-over-IP remote stations (UID locking)

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

ADVICE: Activate the function **UID locking** if you want to *specify* which IP matrix switches or console modules should be able to connect to the computer module.

NOTE: For more information on the configuration settings, refer to the separate manuals of the KVM-over-IP matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

Integration into the AV solution and RemoteAccess

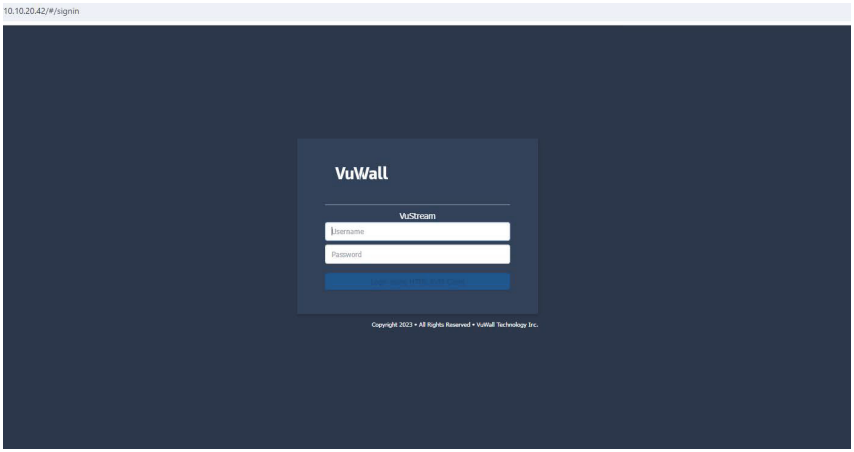
The **VuStream-350** integrated into the **VisionVS-IP**, in combination with a PAK 20 or PAK 40 from VuWall, provides ultra-low latency for your video wall solution. This is particularly useful when using TRx's PAK KVM feature. However, can also add a **VisionVS-IP** to your solution without using *TRx's PAK KVM feature*.

> **IMPORTANT:** The audio and RS232 data (see *Connecting audio and RS232 interfaces* on page 17) are transmitted only via KVM-over-IP connection and **not** through the streaming output.

To add a **VisionVS-IP**/**VuStream-350** to your solution, see the sections below.

Access the HTML KVM client

Use the HTML KVM client to configure the integrated **VuStream-350**. To access it, follow the steps in the sections below depending on your network type.



On a DHCP network

1. Connect the **VisionVS-IP** to your network using an ethernet cable (see *Establishing a connection to a network to integrate the VisionVS-IP into the AV solution* on page 18 ff.).

> **ADVICE:** If you have many **VisionVS-IP**/**VuStream-350** to configure, you can connect them all to your network during this step.

2. Use an IP Scanner software of your choice to find the IP address of each **VuStream-350**. Each **VisionVS-IP**/**VuStream-350** can be identified by its MAC address in the IP Scanner. For more detailed instructions on how to do use an IP Scanner contact your network administrator.
3. Go to **https://<VuStream-350 IP address>**. Sign in with the default admin credentials (see *Change the default admin credentials* on page 31 ff.).

On a static network

1. Connect the **VisionVS-IP** to your network using an ethernet cable (see *Establishing a connection to a network to integrate the VisionVS-IP into the AV solution* on page 18 ff.).

> **IMPORTANT:** If you have several **VisionVS-IP**/**VuStream-350** to configure, you must connect and configure each **VisionVS-IP**/**VuStream-350** to your network one at a time.

2. Go to **https://kvm.local**. Sign in with the default admin credentials (see *Change the default admin credentials* on page 31 ff.).

> **IMPORTANT:** To access **https://kvm.local** make sure *mDNS* is **not** restricted.

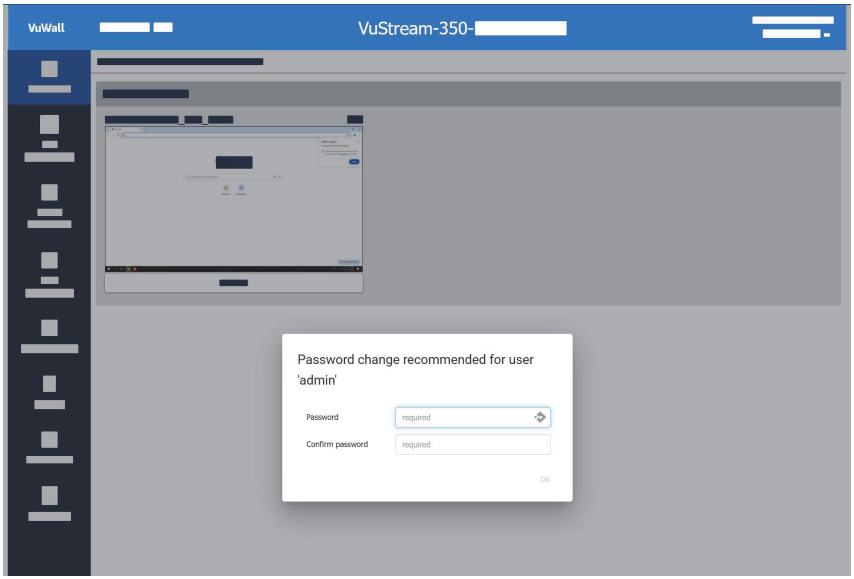
3. Follow the steps in section *Network settings* (see page 31 f.).

Change the default admin credentials

The first time you call up a client after you have set up the device, you will be prompted to change the password.

> **NOTE:** The default **admin** password is **vuwall**.

You will prompted to reset the password for the admin. Enter a password of your choise..



Establishing a connection

You can view a preview and connect to the target.

How to connect to the target:

1. Click on **Port Access** to display a preview.

   > **NOTE:** The preview image refreshes every 5 seconds.

2. Click **Connect** to establish the connection to the target:

Network settings

Your *TRx* network needs to be able to access your **VuStream-350**. Typically, this means the IP address and Gateway (optional) should be on the same network range as your *TRx* Server. Network settings are applied depending on the type of network you have:

DHCP: Network settings are applied automatically by your DHCP server (*default*).

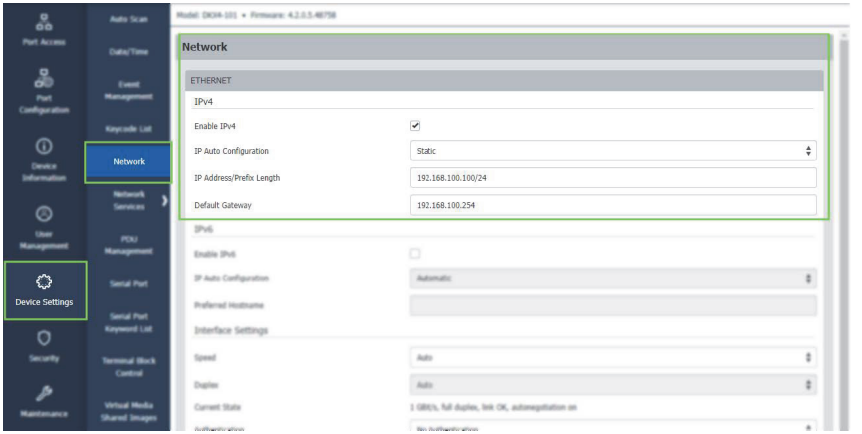
Static IP: Follow these steps to change the IP settings from the default values:

1. In the client, click on **Device Settings > Network**.
2. Enter the following values under **Ethernet > IPv4**:

Enable IPv4:	Enable **IPv4**.
IP Auto Configuration:	Select **Static** to enter a static IP address.
IP Address/ Prefix Length:	Assign a static IP address for the **VuStream-350**.
Default Gateway:	Enter the default gateway for the **VuStream-350**.

ADVICE: For larger networks or unique network designs, contact your network administrator for help with configuring your device's network settings.

3. Click **Save**.



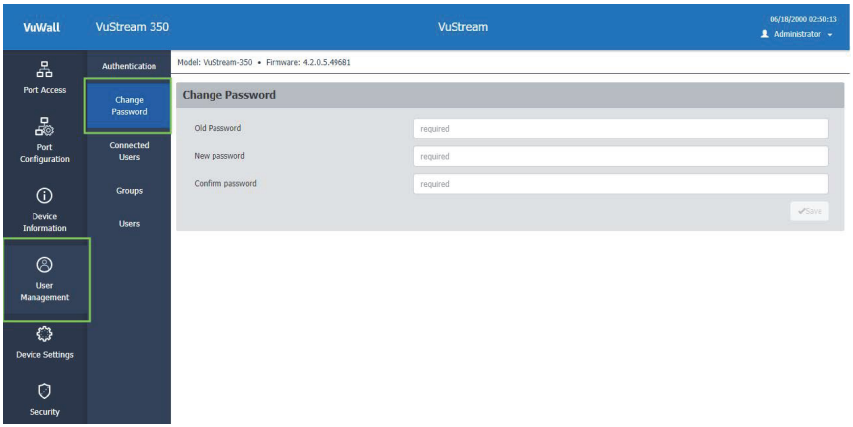
Change password

How to change the admin password:

1. Go to **User Management** and select **Change password**.
2. Enter the following values:

Old Password:	Enter the old password.
New Password:	Enter the new password.
Confirm New Password:	Confirm the new password.

3. Click **Save**.



Video settings

How to change the video settings:

1. Go to **Port Configuration** and select **Video settings** to view or adjust your source´s video settings. Below are some considerations when adjusting video settings:

Default preferred video resolution:	1920x1080@60Hz
Maximum preferred video resolution:	3840x2160@60Hz
Default cycle time:	200 ms. Increase the cycle time if the target video doesn´t respond to resolution changes.

VuStream-350 KVM Driver install

If your AV solution includes one or more KVM operator stations, download the KVM Driver and install it on your **VisionVS-IP** Source PC.

1. Go to the **VuWall Partner Portal** and download the *VuStream-350 KVM Mouse Driver*.
2. Run the installer on the **VisionVS-IP** Source PC.

VuStream-350 KVM Driver uninstall

If you no longer want your operator station to have access to KVM functionality, follow the steps below to uninstall the *VuStream-350 KVM Mouse Driver*.

1. On your **VisionVS-IP** Source PC, open File Explorer, and go to *C:\Program Files (x86)\VuWall Technology Inc\VuWall KVM Mouse Driver.*
2. Double-click **Uninstall** and run the uninstaller.

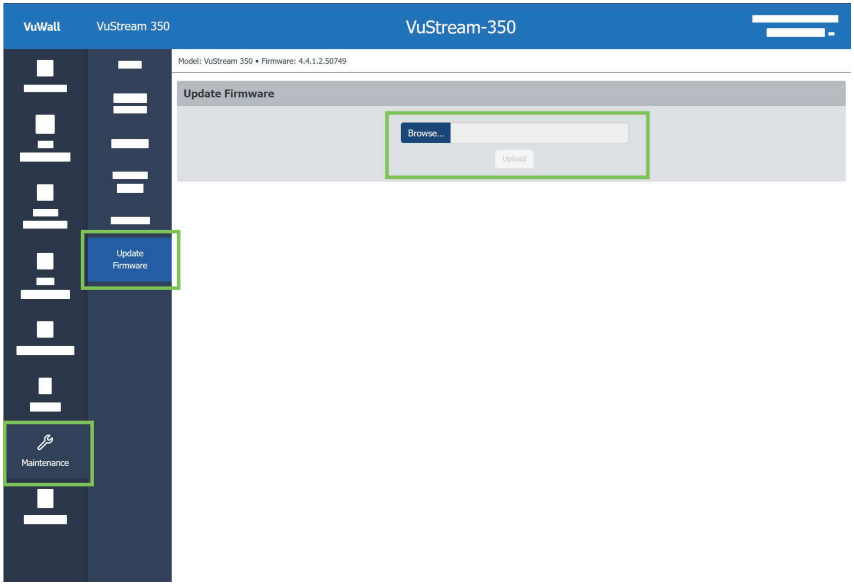
Update firmware

How to update the integrated VuStream-350 to the latest firmware:

1. Make sure your **VisionVS-IP** is connected to your AV network.
2. From a computer on your AV network, go to the **VuWall´s Partner Portal** and download the latest **VuStream-350 firmware**. Extract the downloaded files.
3. Use an IP Scanner software of your choice to find the IP address of your **VuStream-350**. Each **VuStream-350** can be identified by its mac address in the IP Scanner. For more detailed instructions on how to use an IP Scanner contact your network administrator. Go to *https://<VuStream350 IP address>* to access the HTML KVM client.

> **NOTE:** To access the HTML KVM Client for first time configuration of your **VisionVS-IP**/**VuStream-350** contact **VuWall Support**. Depending on your network type you may need more detailed instructions to sign in.

4. Sign in to the **HTML KVM Client** with the admin, default, or previously set credentials.
5. Go to **Maintenance**, select **Update Firmware**. Under **Update Firmware**, select **Browse**. Browse to the location of the firmware file. Select the **.rfp** file and select **Upload**.



6. Select **Update Firmware**. The update process takes about 5 minutes.

> **IMPORTANT:** Do not turn off your device while it is updating. Once the update is complete the device will reboot.

7. Sign in to the **HTML KVM Client**. When prompted, change the password.

8. Repeat steps 3 to 5 for each **VisionVS-IP**/**VuStream-350** you need to update.

> **NOTE:** The **KVM functionality** on the operator station will **not** be available during the update process.

Factory reset

How to reset the integrated VuStream-350:

1. Go to **Maintenance**, and select **Unit Reset**.

2. Select **Reset to Factory Defaults**.

Operation

The computer connected to the **VisionVS-IP** can be operated at the remote console of a console module as well as via VuWall streaming or at the local console of the **VisionVS-IP**.

After their initiation, all consoles are enabled to operate the computer.

NOTE: The monitors of a remote console of a console module and the VuWall streaming as well as the local console of the **VisionVS-IP** *always* display the same image.

NOTE: When the **VisionVS-IP** is used in **extender mode**, adjustments can be made in the area of **concurrent/exclusive operation**.

Concurrent operation

If a user carries out a keyboard or a mouse input, the input devices of the concurrent console are automatically locked in extender mode. The lock is lifted if no inputs are made at the active console during the adjusted timing of the automatic input lock (*default*: 1 second).

After the automatic input lock has been lifted, all consoles are again able to operate the computer.

As an alternative to operate the computer concurrently via consoles, the exclusive operation can be activated.

Exclusive operation

To enable exclusive operation by a console, the authorization for permanent console access can be activated in extender mode.

If this function is activated, the exclusive operation can be activated by pressing a hotkey. Immediately after pressing this hotkey, the input devices of the concurrent console are deactivated. By pressing the hotkey again at the active console, users at all consoles are again able to operate the computer.

ADVICE: In the standard configuration, the computer's video signal is output at the active as well as the concurrent console monitor.

If necessary, change the video modes of the consoles to switch off the image of the concurrent console while you operate the computer at another console.

NOTE: For more information on the configuration settings, refer to the separate manual for the installation and operation of the console module in use.

NOTE: For more information on the configuration settings, refer to the separate manual for the *Vision Series (digital)* web application.

Configuration

The configuration of the into the **VisionVS-IP** integrated computer module can be changed either using the on-screen display (OSD) on the console monitor or the web application **Config Panel**:

- The *on-screen display* is shown on the console monitor. Most configuration settings can be changed directly on the OSD of the console.

ADVICE: For more information on the configuration settings, refer to the separate manual for configuring the matrix switch in use or – if the **VisionVS-IP** is operated in direct extender mode – to the separate manual for the installation and operation of the console module in use.

- The web application **Config Panel** provides a graphical user interface to configure and monitor the KVM extender via web browser.

Basic operation of the web application

The **Config Panel** web application provides a graphical user interface to configure and monitor the into the **VisionVS-IP** integrated computer module.

The web application can be used in the entire network independently from the locations of the devices and consoles connected to the KVM system.

IMPORTANT: The separate manual for the *Vision-IP Series* web application provides information about system requirements, the required configuration of the network interfaces and the operation of the web application.

Starting the web application

How to start the Config Panel web application:

1. Enter the following URL in the address bar:

   https://[IP address of the integrated computer module]

2. Enter the following data in the login mask:

Terms (of use):	Press **Enter** to display the terms of use.
Accept (of terms of use):	Press **F8** to accept the terms of use.
Username:	Enter your username.
Password:	Enter your user account password.
2-Factor Auth Code (TOTP):	Enter the 2-Factor Auth Code (TOTP) from two-factor authentication.

IMPORTANT: Change the administrator account's default password.

The *default* access data is:

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

NOTE: The *Terms* field and the *Accept* field only appear if Showing terms of use is activated.

NOTE: The *2-Factor Auth Code (TOTP)* field only appears if 2-factor-authentication is enabled. For detailed information, please refer to the separate manual of the web application.

3. Click on **Login**.

Selecting the language of the web application

How to change the language of the web application:



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

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

Closing the web application

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

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

How to close the web application:



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

Further information

Recommendations for twisted pair cables

The **VisionVS-IP** provides an **Transmission** interfaces to transmit the following data.

- **Transmission:** keyboard, video, mouse, audio, RS232

The following paragraphs give you recommendations regarding the use of specific twisted pair cables.

> **NOTE:** Several segments of a cable connection can be connected with patch panels and connection ports.
>
> It is, however, not permitted to connect active components such as network switches, hubs or repeaters.

Transmission of KVM data

The signals *keyboard, video, mouse, audio* and *RS232* of the **VisionVS-IP** are transmitted via category 5e (or better) twisted pair cables.

Depending on the wire gauge and the type of twisted pair cable, the following distances can be bridged between the **VisionVS-IP** and a matrix switch or a console module.

Wire gauge	Cable type	Category	Recommendation
AWG 22	Installation cable	5e, 6 or 7	up to 140 m
AWG 24	Installation cable	5e, 6 or 7	up to 100 m
AWG 26	Patch cable	5e, 6 or 7	up to 80 m

The following cables achieved the best results during test operation:

- **up to 140 metres:** Kerpen MegaLine ® G12-150 S/F (AWG 22)
- **up to 100 metres:** Dätwyler uninet ® 5502 S-STP (AWG 24)
- **up to 80 metres:** Dätwyler uninet ® 7702 Flex (AWG24)

DDC transmission with cache function

The KVM extender supports *Enhanced-DDC* (Enhanced Display Data Channel) to read out the data from the monitor that is connected to the console module and transmit them to the computer. This data includes information regarding the preferred resolution and the supported monitor frequencies.

To make sure that the computer connected to the **VisionVS-IP** can already access the features of the remote monitor during booting, the KVM extender contains a cache function. Even when the computer module or the console module are switched off or the devices are not interconnected, the properties of the most recently connected monitor or a default data block are provided in the KVM extender.

The monitor's DDC information is usually transmitted one-to-one to the computer. Should the KVM extender determine that the display cannot be read without errors or that the entries are invalid, the information is completed or corrected (if possible).

Determining network settings via service port

If you do not know the IP address of an already configured user or computer module, you can use the service port of the module to find out the address.

Use any terminal emulator (e.g. *Tera Term* or *PuTTY*) to show the log messages of the modules.

Installing the device driver

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

> **NOTE:** When connected to a service cable, the driver provides the *Service* port of a user or a computer module as a virtual serial interface (COM port). The virtual interface can then be selected to establish a connection using the terminal emulator.

How to install the device driver to address the service port:

1. Use any web browser to open the website **www.gdsys.com/en**.
2. Go to **Service > Download > Tools & Driver**.
3. Download the device driver for the operating system installed on the computer.
4. Execute the file and follow the instructions of the installation wizard.

Establishing a connection by using a terminal emulator

How to establish a connection using a terminal emulator:

1. Start any terminal emulator (e.g. *Tera Term* oder *PuTTY*).
2. Establish a new connection via terminal emulator and enter the follwoing settings:
   - Bits per second: 115.200
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
3. Use the supplied USB service cable to connect the computer to the *Service* port on the front panel of the user or computer module.

Determining the IP address

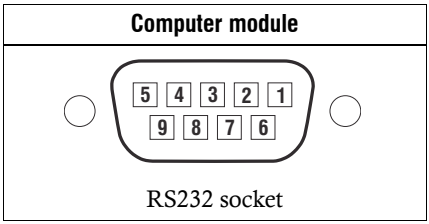
How to determine the IP address of a user or computer module:

1. Restart the user or computer module.

   During the boot process, the terminal emulator shows various status messages.
2. After the boot process, the IP address and other **system information** are displayed.

Pin assignment of the RS232 socket/interface

The following figure shows the pin assignments of the RS232 socket:



The table shows how the different lines of the data connection are assigned to the according pins:

Pin no.	Line	Computer module
1	DCD (Data Carrier Detect)	Output
2	RxD (Receive Data)	Output
3	TxD (Transmit Data)	Input
4	DTR (Data Terminal Ready)	Input
5	GND (Ground)	Ground
6	DSR (Dataset Ready)	Output
7	RTS (Request to Send)	Input
8	CTS (Clear to Send)	Output
9	*not occupied*	n/c

Status LEDs

The LEDs on the front and back panel of the **VisionVS-IP** let you control the operational status of the KVM extender at any time.

Meaning of the LEDs on the front panel

Area	LED	Color	Status	Meaning
Ident.	**Ident.**	blue	on	On as soon as the LED has been activated via web application.
Power	**Red.**	green	on	The optional power pack is connected and supplies voltage of 12 Volt.
			off	The optional power pack is not (properly) connected.
	Main	green	on	The power pack is switched on and supplies the required voltage.
			off	The power pack is switched off or a connection to the power network could not be established.
Status	**K/M**	green	on	The keyboard has been detected.
			blinking	No keyboard connected or keyboard could not be detected.
	System	green	on	Device is ready for operation.
			blinking	Executing update.
			fast blinking	Device is reset to default settings after pushing the Reset button for a long time.
		red	on	Internal error or device booting
Channel	**Video**	yellow	on	A stable video signal has been detected at the video input.
			off	The incoming video signal could not be detected or its quality is not good enough to be processed.
	Trans.	yellow	on	The connection to the remote station has been established.
			off	The connection to the remote station could not be established.
Management	**left**	yellow	on	The connection to the network has been successfully established.
			off	A connection could not be established.
	right	green	flickering	Network activity.
			off	No network activity

Meaning of the LEDs on the back panel (CAT variant)

Area	LED	Status	Meaning
Transmission	**yellow**	on	Communication with the counterpart has been established.
		blinking	Connection to counterpart has been established.
		off	Connection to counterpart has not been established.
	green	on	Logged on at counterpart.
		off	Not logged on at counterpart.

Meaning of the LEDs on the back panel (fiber variant)

Area	LED	Status	Meaning
Transmission	**yellow**	on	Communication with the counterpart has been successfully established.
		blinking	Only the RX interface can be used to establish a connection to the counterpart. Check the cable connection of the Tx interface with the counterpart.
		fast blinking	incompatible SFP module
		off	The connection to the counterpart could not be established.
	green	on	Logged on at counterpart
		off	Not logged on at counterpart

Used network ports and protocols

NOTE: You can find a list of the network ports and protocols that can be used by G&D KVM-over-IP in the separate manual of the web application.

Technical data

General features of the series

VISIONVS-IP SERIES		
Interfaces for computers	Video:	1 × DisplayPort jack
	USB keyboard/mouse:	1 × USB-B socket
	Audio:	3.5-mm jack plug (Line In) 3.5-mm jack plug (Line Out)
	RS232:	1 × RS232 socket
Interfaces for local console	Monitor:	1 × DisplayPort jack
	USB keyboard/mouse:	2 × USB-A socket
Interfaces to KVM counterpart	KVM, Audio and RS232:	‣ see specific features
	Transmission type:	KVM-over-IP™
Other interfaces	Connection to network:	1 × RJ 45 socket (Management)
		1 × RJ 45 socket (Network)
	Service:	1 × Mini-USB socket (type B)
	Control:	5-pole terminal block (not supported)
Audio ‣ DisplayPort Digital	Transmission type:	2 channel LPCM, stereo
	Resolutions:	16/20/24 bit
	Sampling rates:	up to 48 kHz
Audio	Transmission type:	transparent, bidirectional
	Resolution:	24 bit digital, Stereo
	Sampling rate:	96 kHz
	Bandwidth:	22 kHz
RS232	Transmission type:	transparent
	Transmission rate:	max. 115.200 bit/s
	Supported signals:	RxD, TxD, RTS, CTS, DTR, DSR, DCD

VISIONVS-IP SERIES		
Graphics (Video input)	Format:	DisplayPort (DP 1.1a)
	Colour depth:	24 bit
	Pixel rate:	approx. 25 to 300 MP/s
	Max. resolution:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Exemplary resolutions:	▪ 4096 × 2160 (24 or 25 Hz) ▪ 3840 × 2160 (24, 25 or 30 Hz) ▪ 2048 × 2160 (60 Hz) ▪ 2048 × 2048 (60 Hz) › Further VESA and CTA standardised resolution possible for video bandwidth/pixel rate and horizontal/vertical frequency.
	Vertical frequency:	24 Hz to 120 Hz
	Horizontal frequency:	25 kHz to 185 kHz
Graphics (Video output)	Format:	HDMI 1.4
	Colour depth:	24 bit
	Pixel rate:	approx. 25 to 297MP/s
	Max. resolution:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Exemplary resolutions:	▪ 4096 × 2160 (24 or 25 Hz) ▪ 3840 × 2160 (24, 25 or 30 Hz) ▪ 2048 × 2160 (60 Hz) ▪ 2048 × 2048 (60 Hz) › Further VESA and CTA standardised resolution possible for video bandwidth/pixel rate and horizontal/vertical frequency.
Main power supply	Type:	internal power pack
	Connector:	IEC plug (IEC-320 C14)
	Voltage:	100-240 VAC/60-50Hz
Redundant power suppply	Type:	external power pack
	Connector:	miniDIN-4 Power socket
	Voltage:	12 VDC
Operating environment	Temperature:	+5°C to +40°C
	Air humidity:	20% to 80%, non-condensing
Storage environment	Temperature:	-20°C to +60C
	Air humidity:	15% to 85%, non-condensing

Specific features of the CAT variant

VISIONVS-IP-CAT		
Interface to KVM counterpart	KVM, Audio and RS232:	1 × RJ 45 socket
Casing	Material:	anodised aluminium
	Dimensions (W × H × D):	approx. 436 × 44 × 284 mm
	IP protection class:	IP20

Specific features of fiber variants

VISIONVS-IP-FIBER		
Interfaces to KVM counterpart	KVM, Audio and RS232:	1 × LC duplex socket, incl. transmission module/ SFP transceiver
Casing	Material:	anodised aluminium
	Dimensions (W × H × D):	approx. 436 × 44 × 284 mm
	IP protection class:	IP20

Features of transmission modules

MULTIMODE TRANSMISSION MODULE		
Data transmission	Type:	fibre optics (2 glass fibres)
	Interface type:	LC duplex
Cable length (max.)	Multimode 50/125µm, Class OM4:	550 metres (fibres with 4700MHz*km)
	Multimode 50/125µm, Class OM3:	550 metres (fibres with 2000MHz*km)
	Multimode 50/125µm, Class OM2:	550 metres (fibres with 500MHz*km)
	Multimode 50/125µm:	500 metres (fibres with 400MHz*km)
	Multimode 62,5/125µm, Class OM1:	275 metres (fibres with 200MHz*km)
	Multimode 62,5/125µm, FDDI grade:	220 metres (fibres with 160MHz*km)

SINGLEMODE TRANSMISSION MODULE		
Data transmission	Type:	fibre optics (2 glass fibres)
	Interface type:	LC duplex
Cable length (max.)	Singlemode 9/125µm, Class OS1:	10 kilometres (fibres with 500MHz*km)

NOTES

NOTES

NOTES

NOTES

G&D. Control what you see.

Headquarters | Hauptsitz

Guntermann & Drunck GmbH Systementwicklung

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

US Office

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

Middle East Office

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

APAC Office

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