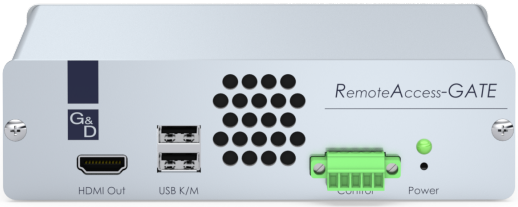
G&D RemoteAccess-GATE

DE Installationsanleitung

EN Installation Guide



A9100375-1.01

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

Version 1.01 – 19.04.2024
Firmware: 4.1.0

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 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.

HINWEIS: 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.

Inhaltsverzeichnis

Sicherheitshinweise

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

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

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

⚠ Trennen Sie alle Spannungsversorgungen

VORSICHT: Risiko elektrischer Schläge!

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

⚠ Disconnect all power sources

CAUTION: Shock hazard!

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

⚠ Débranchez toutes les sources d'alimentation

ATTENTION: Risque de choc électrique!

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

⚠ Vorsicht vor Stromschlägen

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

⚠ Ständigen Zugang zu den Netzsteckern der Geräte sicherstellen

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

⚠ Lüftungsöffnungen nicht verdecken

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

⚠ Korrekte Einbaulage bei Geräten mit Lüftungsöffnungen sicherstellen

Aus Gründen der elektrischen Sicherheit ist bei Geräten mit Lüftungsöffnungen nur eine aufrechte, horizontale Einbauweise zulässig.

⚠ 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 das G&D-Netzteil

Betreiben Sie dieses Gerät nur mit dem mitgelieferten oder in der Bedienungsanleitung aufgeführten Netzteil.

⚠ Betreiben Sie das Gerät ausschließlich im vorgesehenen Einsatzbereich

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

Das G&D-Addon »RemoteAccess-GATE«

RemoteAccess-GATE ist ein Stand-alone-Gerät, das als *Bindeglied* zwischen einem G&D KVM-System und der Netzwerk-Welt eingesetzt wird.

HINWEIS: GATE steht für **G**lobal **A**ccess **T**o **E**nterprise und somit den weltweiten Zugang zu Ihren KVM-Systemen.

Mit *RemoteAccess-GATE* richten Sie einen lokalen Arbeitsplatz ein der über ein Gigabit-Ethernet eine Verbindung zu einem entfernten G&D-Gerät bzw. einem entfernten Computer herstellt.

Über die Software-Clients bzw. den Web-Client bedienen Sie das entfernte G&D-Gerät bzw. den entfernten Computer und konfigurieren *RemoteAccess-GATE* nach Ihren Anforderungen.

HINWEIS: *RemoteAccess-GATE* erlaubt bis zu acht Benutzern den *gleichzeitigen* Zugriff auf das entfernte G&D-Gerät bzw. den entfernten Computer.

Lieferumfang

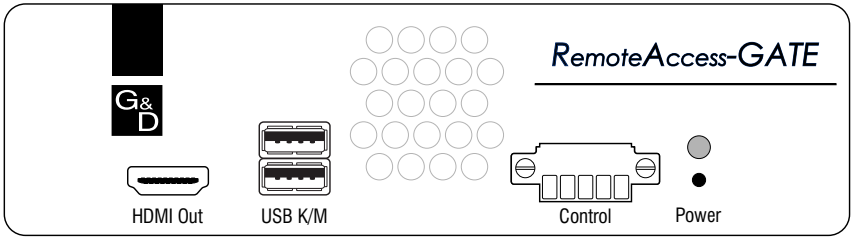
- 1 × *RemoteAccess-GATE*
- 1 × Tischnetzteil
- 1 × Sicherheitshinweise-Flyer

Erforderliches Zubehör

- 1 × Twisted-Pair-Kabel der Kategorie 5e (oder höher) zum Anschluss des Geräts an ein Gigabit-Ethernet

Installation

Schnittstellen an der Frontseite



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.

Control: Schließen Sie optional ein externes Gerät an, das Sie über **RemoteAccess-GATE** ein- bzw. ausschalten möchten.

WICHTIG: Ausschließlich diese Spannungen werden unterstützt: **2A/30VDC**, **0.5A/60VDC** und **0.3A/125VAC**.

HINWEIS: Beachten Sie folgende Hinweise beim Anschluss der Pins:

- **Ausgangsanschluss: Pin 1** bis **Pin3**

  Die drei Pins werden über zwei Relais geführt, die sich eine gemeinsame Leitung teilen. Aus diesem Grund ist **Pin 1** im Normalfall geöffnet und **Pin 3** geschlossen.

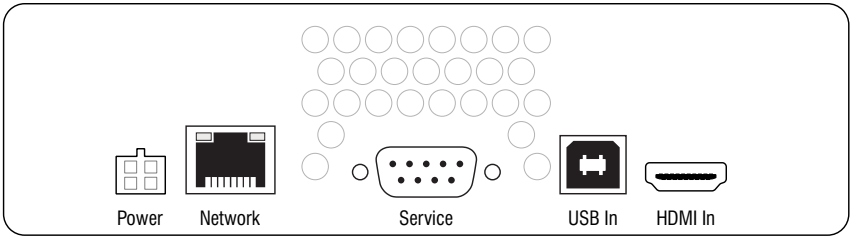
  Achten Sie auf einen korrekten Anschluss, wenn Sie beide Relais zeitgleich verwenden möchten!

  Unterstützte Geräte: LED, Summer, An-/Aus-Schalter eines Rechners.

- **Eingangsanschluss: Pin 4** und **Pin 5**

  Unterstützte Geräte: externe Drucktaster und/oder binäre Umschalter

Schnittstellen an der Rückseite



Power: Stecken Sie das Anschlusskabel des mitgelieferten Tischnetzteils an. Verbinden Sie das Tischnetzteil mit einer Netzsteckdose.

Network: Stecken Sie ein als Zubehör erhältliches Twisted-Pair-Kabel der Kategorie 5e (oder höher) ein. Das andere Ende des Kabels ist mit einem Gigabit-Netzwerk zu verbinden.

Service: Schließen Sie optional den Rechner an, über dessen Terminalemulationsprogramm (beispielsweise *Tera Term* oder *PuTTY*) Sie CLI-Kommandos ausführen möchten.

USB In: Verbinden Sie einen USB-Port des kompatiblen G&D-Geräts bzw. des Computers mit dieser Schnittstelle.

> **TIPP:** Bei Anschluss eines kompatiblen G&D-Gerätes ist die Einstellung des *Single-Mouse-Mode* im *RemoteAccess-GATE* empfehlenswert.
>
> Ausführliche Informationen zum *Single-Mouse-Mode* finden Sie im Abschnitt des von Ihnen verwendeten Clients (s. Seite 6) des separaten Handbuchs *Configuration and Operation*.

HDMI In: Verbinden Sie den HDMI-Videoausgang des kompatiblen G&D-Geräts bzw. des Computers mit dieser Schnittstelle.

> **HINWEIS:** Für den Anschluss eines G&D-Gerätes mit **DisplayPort**-Anschluss verwenden Sie das als Zubehör erhältliche *DP-HDM-Converter-Cable* (A6300156).
>
> Für den Anschluss eines G&D-Gerätes mit **DVI**-Anschluss verwenden Sie das als Zubehör erhältliche *DVI-HDMI-Adapter-Cable* (A6400049).

Erstkonfiguration

WICHTIG: Die vollständige Konfiguration und Bedienung des Geräts wird im Handbuch *Configuration and Operation* beschrieben.

Das englischsprachige Handbuch wird fortlaufend aktualisiert und ist ausschließlich im Internet veröffentlicht:

https://gdsys.de/A9100284

Bevorzugten Client öffnen

Sie können zwischen drei verschiedenen Clients wählen, um KVM-Sitzungen zu starten oder Ihr Gerät zu konfigurieren.

Die Clients sind für verschiedene Einsatzzwecke und Systeme optimiert:

- **HTML KVM Client (HKC):** Der HKC kann in jedem Browser gestartet und bedient werden.

  Die *Videoperformance* und die *virtuelle Medienfunktionalität* sind bei diesem Client eingeschränkt

  HINWEIS: Zum Start des **HKC** öffnen Sie in Ihrem Browser die folgende URL:

  https://192.168.0.1

- **Active KVM Client (AKC):** Der AKC ist der empfohlene Client für Windows-Anwender mit *Microsoft Edge Legacy*, *Internet Explorer 11* oder einem anderen Browser, der die *ClickOnce*-Technologie unterstützt.

  HINWEIS: Zum Start des **AKC** auf einem Windows-PC öffnen Sie mit *Microsoft Edge Legacy*, *Internet Explorer 11* oder einem anderen Browser mit *ClickOnce*-Technologie die folgende URL:

  https://192.168.0.1/akc

- **Virtual KVM Client Standalone (VKCS):** Der VKCS ist der empfohlene Client für Windows sowie macOS- und Linux-Betriebssysteme mit Java-Support.

  HINWEIS: Zum Start des **VKCS** auf PC mit Java-Support öffnen Sie in Ihrem Browser die folgende URL:

  https://192.168.0.1/vkcs

  Falls Ihr Browser die automatisch heruntergeladene Datei nicht automatisch startet, starten Sie diese mit einem Doppelklick.

Passwort des Admin-Benutzers 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 **4658**.

So ändern Sie das Passwort des Admin-Benutzers:

1. Starten Sie den gewünschten Client (s.o.).
2. Folgen Sie den Anweisungen des Clients, um das Passwort des Admin-Benutzers zu ändern.

Netzwerkeinstellungen konfigurieren

In der Standardeinstellung des Gerätes ist der Netzwerkschnittstelle die statische IPv4-Adresse **192.168.0.1** zugewiesen.

Die Änderung der IP-Adresse sowie die Aktivierung von DHCP ist im Bereich **Device Settings > Network** des Clients möglich.

So ändern Sie die Netzwerkeinstellungen des Gerätes:

1. Klicken Sie im Client auf **Device Settings > Network**.
2. Erfassen Sie im Abschnitt **Ethernet > IPv4** folgende Daten:

Enable IPv4 :	IPv4-Protokoll ein- oder ausschalten
IP Auto Configuration:	Wählen Sie die Methode nach der die IPv4-Einstellungen gesetzt werden: ▪ **Static:** Es wird eine statische IP-Adresse angegeben. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server.
IP Address/ Prefix Length:	Weisen Sie eine statische IPv4-Adresse zu und geben Sie die Präfixlänge an. In der Standardeinstellung ist dies: **192.168.0.1/24**. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn Sie eine statische IP-Adresse (**Static**) verwenden.
Default Gateway	Geben Sie die IP-Adresse des Gateways an. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn Sie eine statische IP-Adresse (**Static**) verwenden.
Preferred Hostname:	Geben Sie den bevorzugten Hostnamen ein. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn die IP-Adresse von einem **DHCP**-Server bezogen wird.

3. Erfassen Sie im Abschnitt **Ethernet > IPv6** folgende Daten:

Enable IPv6 :	IPv6-Protokoll ein- oder ausschalten
IP Auto Configuration:	Wählen Sie die Methode nach der die IPv6-Einstellungen gesetzt werden: ▪ **Static:** Es wird eine statische IP-Adresse angegeben. ▪ **DHCP:** Bezug der IP-Adresse von einem DHCP-Server.
IP Address/ Prefix Length:	Weisen Sie eine statische IPv6-Adresse zu und geben Sie die Präfixlänge an. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn Sie eine statische IP-Adresse (**Static**) verwenden.
Default Gateway	Geben Sie die IP-Adresse des Gateways an. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn Sie eine statische IP-Adresse (**Static**) verwenden.
Preferred Hostname:	Geben Sie den bevorzugten Hostnamen ein. **HINWEIS:** Diese Einstellung ist nur verfügbar, wenn die IP-Adresse von einem **DHCP**-Server bezogen wird.

4. Erfassen Sie im Abschnitt **Ethernet > Interface Settings** folgende Daten:

Speed:	Wählen Sie die Geschwindigkeit der LAN-Verbindung: **Auto**, **10 MBit/s**, **100 MBit/s** oder **1 Gbit/s**
Duplex:	Wählen Sie den Duplex-Modus der LAN-Verbindung: **Auto**, **Full** oder **Half**

5. Erfassen Sie folgende Daten im Bereich **Common Network Settings**:

DNS Resolver Preference:	Legen Sie fest, welche IP-Adresse verwendet wird, wenn der DNS-Auflöser sowohl **IPv4**- als auch **IPv6**-Adressen zurückgibt.
DNS Suffixes (optional);	Geben Sie bei Bedarf einen DNS-Suffixnamen an.
First/Second DNS Server:	Geben Sie die IP-Adresse des DNS-Servers an. **HINWEIS:** Wenn **DHCP** oder **Auto** für die IPv4/IPv6-Einstellungen ausgewählt ist und *keine* statischen DNS-Server angegeben sind, verwendet das Gerät die per DHCP zugewiesenen DNS-Server.

6. Klicken Sie auf **Save**.

Interne Uhr des Geräts einstellen

Stellen Sie die interne Uhr des Gerätes manuell ein, oder synchronisieren Sie die interne Uhr mit einem NTP-Server via *Network Time Protocol*.

HINWEIS: Das aktuelle Systemdatum und die Uhrzeit des Gerätes werden in der oberen rechten Ecke der Weboberfläche angezeigt.

So aktivieren Sie die Synchronisierung der internen Uhr mit einem NTP-Server:

1. Klicken Sie im Client auf **Device Settings > Date/Time**.
2. Erfassen Sie im Abschnitt **Common Settings** folgende Daten:

Time Zone:	Wählen Sie die Zeitzone am Standort des Gerätes aus.
Automatic Daylight Saving Time Adjustment:	Aktivieren Sie diese Option, wenn die Umstellung von Sommer- auf Winterzeit (und umgekehrt) automatisch erfolgen soll.
Time Setup Method:	Wählen Sie die Option **Synchronize with NTP Server**.

3. Erfassen Sie im Abschnitt **NTP Settings** folgende Daten:

First/Second NTP Server:	Geben Sie die Adresse eines NTP-Servers ein.

4. Klicken Sie auf **Save**.

So stellen Sie die interne Uhr Gerätes manuell ein:

1. Klicken Sie im Client auf **Device Settings > Date/Time**.
2. Erfassen Sie im Abschnitt **Common Settings** folgende Daten:

Time Zone:	Wählen Sie die Zeitzone am Standort des Gerätes aus.
Automatic Daylight Saving Time Adjustment:	Aktivieren Sie diese Option, wenn die Umstellung von Sommer- auf Winterzeit (und umgekehrt) automatisch erfolgen soll.
Time Setup Method:	Wählen Sie die Option **User Specified Time**.

3. Erfassen Sie im Abschnitt **User Specified Time** folgende Daten:

Date:	Geben Sie das aktuelle Datum im Format **JJJJ-MM-TT** ein oder klicken Sie auf Kalender-Symbol rechts um das Datum in der Kalenderansicht auszuwählen.
Time:	Geben Sie die aktuelle Uhrzeit im Format **hh:mm:ss** ein oder verwenden Sie die Pfeiltasten um die einzelnen Werte zu ändern. **HINWEIS:** Die Zeitangabe erfolgt in 12-Stunden-Zählung. Bei Zeitangaben am Vormittag wählen Sie **am** und bei Zeitangaben am Nachmittag **pm**.

4. Klicken Sie auf **Save**.

Zertifikate installieren

RemoteAccess-GATE verwendet TLS 1.3 für den verschlüsselten Netzwerkverkehr mit verbundenen Clients. Beim Verbindungsaufbau authentifizert sich das Gerät gegenüber dem Client mit einem kryptografischen Zertifikat.

WICHTIG: Das Gerät wird mit einem Standardzertifikat ausgeliefert. Das Ersetzen des Standardzertifikats durch ein eigenes Zertifikat wird dringend empfohlen!

Das Gerät kann selbständig ein **selbstsigniertes Zertifikat** oder einen **Certificate Signing Request** (CSR) erzeugen. Alternativ können Sie ein eigenes Zertifikat in das Gerät laden.

TIPP: Die Details des aktiven Zertifikats können Sie im Client unter **Security > TLS Certificate** einsehen und das Zertfikat sowie den Key downloaden.

Variante 1: Selbstsigniertes Zertifikat erstellen und aktivieren

WICHTIG: Stellen Sie vor der Erstellung eines Zertifikates sicher, dass die interne Uhr des Gerätes korrekt eingestellt ist (s. Seite 9).

Ein selbstsigniertes Zertifikat ist die einfachste und schnellste Art und Weise den Netzwerkverkehr des Gerätes mit einem *eigenen* Zertifikat abzusichern.

Ihr Browser und die Clients werden der Verbindung aufgrund des *selbstsignierten* Zertifikats standardmäßig *nicht* vertrauen, da der Herausgeber des Zertifikats nicht bekannt ist. Sobald Sie im Browser bzw. Client eine Ausnahme für den Herausgeber speichern, kann die verschlüsselte Verbindung aufgebaut werden.

HINWEIS: Falls Sie ein Zertifikat nutzen möchten, dass ohne Ausnahmen vom Browser und Client akzeptiert wird, erstellen Sie einen *Certificate Signing Request* (s. unten) und fordern damit die Zertifikatserstellung bei einer bekannten Zertifizierungsstelle an.

So erstellen und aktivieren Sie ein selbstsigniertes Zertifikat:

1. Klicken Sie im Client auf **Security > TLS Certificate**.
2. Scrollen Sie zum **New TLS Certificate**.
3. Geben Sie in der linken Spalte **(Subject)** des Fensters mindestens die im Client als erforderlich (**required**) gekennzeichneten Daten ein.

   Nachfolgend werden die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country (ISO Code)	DE
State or province	NRW
Locality	Siegen
Organization	Guntermann & Drunck GmbH
Organizational unit	
Common name	Guntermann & Drunck GmbH
Email address	

4. Geben Sie in der rechten Spalte im Abschnitt **Subject Alternative Names** bis zu zehn IP-Adressen oder Hostnamen ein, für die das Zertifikat gültig sein wird.
5. Aktivieren Sie die **Self-sign**-Option im Abschnitt **Key Creation Paramaters**.
6. Geben Sie im Feld **Validity in days** die Anzahl der Tage ein, die das Zertifikat gültig sein wird.
7. Klicken Sie auf **Create New TLS Key**.
8. Vergewissern Sie sich anhand der Anzeige der Zertifikatsdetails, dass Sie die korrekten Dateien ausgewählt haben und klicken Sie auf **Install Key and Certificate**.

Variante 2: Certificate Signing Request für Zertifizierungsstelle erstellen

WICHTIG: Stellen Sie vor der Erstellung eines Zertifikates sicher, dass die interne Uhr des Gerätes korrekt eingestellt ist (s. Seite 9).

1. Klicken Sie im Client auf **Security > TLS Certificate**.
2. Scrollen Sie zum **New TLS Certificate**.
3. Geben Sie in der linken Spalte **(Subject)** des Fensters mindestens die im Client als erforderlich (**required**) gekennzeichneten Daten ein.

   Nachfolgend werden die verschiedenen Felder und eine exemplarische Eingabe aufgeführt:

Feld	Beispiel
Country (ISO Code)	DE
State or province	NRW
Locality	Siegen
Organization	Guntermann & Drunck GmbH
Organizational unit	
Common name	Guntermann & Drunck GmbH
Email address	

4. Geben Sie in der rechten Spalte im Abschnitt **Subject Alternative Names** bis zu zehn IP-Adressen oder Hostnamen ein, für die das Zertifikat gültig sein wird.

   WICHTIG: Stellen Sie sicher, dass die **Self-sign**-Option im Abschnitt **Key Creation Paramaters** deaktiviert ist!

5. Geben Sie in den Feldern **Challenge** und **Confirm challenge** im Abschnitt **Key Creation** ein Challenge-Passwort ein.
6. Klicken Sie auf **Create New TLS Key**.
7. Klicken Sie auf **Download Certificate Signing Request** und übergeben Sie die heruntergeladene Datei einer Zertifizierungsstelle zur Erstellung des Zertifikates.
8. Öffnen Sie das von der Zertifizierungsstelle erhaltene Zertfikat im Abschnitt **Upload Certificate** und klicken Sie auf **Upload**.

Variante 3: Eigenes Zertifikat in das Gerät laden und aktivieren

So laden Sie ein extern erstelltes Zertifikat in das Gerät und aktivieren es:

1. Klicken Sie im Client auf **Security > TLS Certificate**.
2. Klicken Sie im Abschnitt **New TLS Certificate** auf **Upload Key and certificate**.
3. Klicken Sie auf **Key File** und öffnen Sie die vorhandene Schlüsseldatei.
4. Klicken Sie auf **Certificate File** und öffnen Sie die vorhandene Zertifikatsdatei.
5. Klicken Sie auf **Upload**.
6. Vergewissern Sie sich anhand der Anzeige der Zertifikatsdetails, dass Sie die korrekten Dateien ausgewählt haben und klicken Sie auf **Install Key and Certificate**.

Statusanzeigen

LED an der Frontseite

Bezeichnung	Farbe	Status	Bedeutung
Power	**grün**	an	Das Gerät wird mit Spannung versorgt.
		blinkt	Das Gerät wird mit Spannung versorgt. Fernzugriff Zielverbindung besteht.
		aus	Das Gerät wird nicht mit Spannung versorgt.

LEDs an der Rückseite

Die in die Network-Buchse integrierten LEDs signalisieren die Netzwerkgeschwindigkeit und -aktivität der Buchse:

Gelb (links)	Grün (rechts)	Bedeutung
aus	aus	Verbindung inaktiv
an	aus	1000 MBps Link; keine Aktivität
blinkt	aus	1000 MBps Link; Aktivität (RX, TX)
aus	ein	100 MBps Link; keine Aktivität
aus	blinkt	100 MBps Link; Aktivität (RX, TX)
an	an	10 MBps Link; keine Aktivität
blinkt	blinkt	10 MBps Link; Aktivität (RX, TX)

Technische Daten

REMOTEACCESS-GATE		
Schnittstellen zum lokalen Arbeitsplatz	Video:	1 × HDMI (HDMI Out)
	Tastatur- und Maussignale:	2 × USB-A (USB K/M)
Schnittstellen zum G&D-Gerät bzw. Computer	Video:	1 × HDMI (HDMI In)
	Tastatur- und Maussignale:	1 × USB-B (USB In)
Sonstige Schnittstellen:	Netzwerk:	1 × RJ45-Buchse (Network)
	Service:	1 × D-Sub 9-Stecker
	Control:	5-poliger Klemmblock
Video	Format:	HDMI 1.4b
	Farbtiefe:	24 Bit
	Videobandbreite:	25 bis zu 297 MP/s
	max. Auflösung:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Auflösungsbeispiele:	▪ 3840 × 2160 (24, 25 oder 30 Hz) ▪ 2560 × 1440 (60 Hz) ▪ 1920 × 1200 (60 Hz) ▪ 1920 × 1080 (24, 30 oder 60 Hz) ‣ Weitere standardisierte Auflösungen im Rahmen der max. Videobandbreite möglich.
	Vertikalfrequenz:	24 Hz bis 85 Hz
	Horizontalfrequenz:	20 kHz bis 99 kHz
Audio ‣ Embedded Audio	Übertragungsart:	2-Kanal-LPCM, stereo
	Auflösungen:	16 bit
	Abtastraten:	bis 48 kHz
Stromversorgung	Typ:	Tischnetzteil
	Anschluss:	1 × 4-poliger Steckverbinder
	Stromaufnahme:	5 VDC; max. 4 A
Gehäuse	Material:	Aluminium eloxiert
	Maße (B × H × T):	160 × 44,5 × 144 mm
	Gewicht:	ca. 720 g
Einsatzumgebung	Temperatur:	+0 °C bis +40 °C
	Luftfeuchte:	20% bis 80%, nicht kondensierend
Lagerumgebung	Temperatur:	-20 °C bis +60 °C
	Luftfeuchte:	15% bis 80%, nicht kondensierend
Konformität		CE, EAC, FCC Klasse A, RoHs

About this manual

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

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

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

Caveat Emptor

G&D will not provide warranty for devices that:

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

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

Proof of trademark

All product and company names mentioned in this manual, and other documents you have received alongside your G&D product, are trademarks or registered trademarks of the holder of rights.

Version 1.01 – 19/04/2024
Firmware: 4.1.0

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.

Contents

Safety instructions

Please read the following safety instructions carefully before you start operating the G&D product. The instructions will help in avoiding damages to the product and in preventing possible injuries.

Keep this manual handy for all persons who will be using this product.

Follow all warnings or operating instructions which are on the device or stated in this user 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.

⚠ Beware of electric shocks

To avoid the risk of electric shock, do not open the device or remove the covers.
If service is required, please contact our technicians.

⚠ Ensure constant access to the power plugs

During the installation of the devices, ensure that the power plugs remain accessible.

⚠ Do not cover the ventilation openings

Ventilation openings prevent the device from overheating. Do not cover them.

⚠ Ensure proper installation position

For reasons of electric safety, the device has to be installed upright and horizontally.

⚠ Avoid tripping hazards

Avoid tripping hazards while laying cables.

⚠ Only use a grounded voltage source

Operate this device by using a grounded voltage source.

⚠ Use only the provided G&D power pack

Operate this device with the provided G&D power pack or with the power pack listed in the manual.

⚠ Operate the device only in designated areas.

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

G&D add-on »RemoteAccess-GATE«

The *RemoteAccess-GATE* is a stand-alone device serving as a *link* between a G&D KVM system and the network world.

NOTE: GATE is short for **G**lobal **A**ccess **T**o **E**nterprise, thus meaning the worldwide access to your KVM system.

The *RemoteAccess-GATE* helps you to set up a local console establishing a connection to a remote G&D device or a remote computer using a Gigabit Ethernet.

Using software clients or a web client, you can operate a remote G&D device or a remote computer and configure the *RemoteAccess-GATE* according to your requirements.

NOTE: The *RemoteAccess-GATE* lets up to eight users *simultaneously* operate a remote G&D device or a remote computer.

Scope of delivery

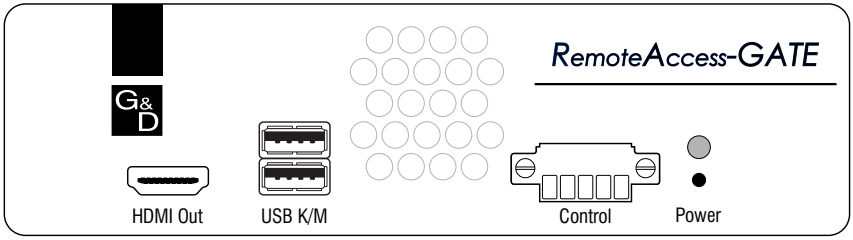
- 1 × *RemoteAccess-GATE*
- 1 × table power pack
- 1 × »Safety instructions« flyer

Required accessories

- 1 × category 5e (or higher) twisted-pair cable to connect the device to a Gigabit Ethernet

Installation

Interfaces on the front panel



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.

Control: Optionally, connect an external device that you want to switch on or off using the **RemoteAccess-GATE**.

IMPORTANT: Only the following voltages are supported: **2A/30VDC**, **0.5A/60VDC** and **0.3A/125VAC**.

NOTE: Mind the following instructions when connecting the pins:

- **Output connection: Pin 1** to **Pin 3**

  The three pins are routed via two relays sharing a line. For this reason, **Pin 1** is usually open and **Pin 3** is closed.

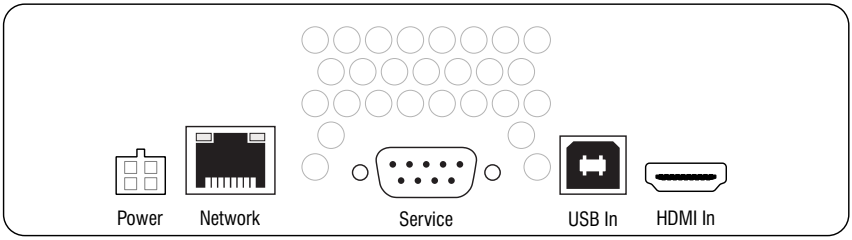
  Ensure proper connection if you want to use both relays at the same time.

  Supported devices: LED, buzzer, on/off button of a computer

- **Input connection: Pin 4** and **Pin 5**

  Supported devices: external push buttons and/or binary switches

Interfaces on the back panel



Power: Plug the connection cable of the supplied table power pack into this interface. Connect the table power pack to a mains socket.

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 gigabit network.

Service: Optionally, connect the computer whose terminal emulator (e.g. *Tera Term* or *PuTTY*) you want to use to execute CLI commands.

USB In: Connect a USB port of a compatible G&D device or a computer to this interface.

ADVICE: When connecting a compatible G&D device, it is recommended to set the *single mouse mode* in the *RemoteAccess-GATE*.

For detailed information about the *single mouse mode*, refer to the section of the separate *Configuration and Operation* manual for the client you are using (see page 6).

HDMI In: Connect the HDMI video output of a compatible G&D device or computer to this interface.

NOTE: To connect a G&D device including a **DisplayPort** connector, use the *DP-HDM-Converter-Cable* (A6300156), which is available as accessory.

To connect a G&D device including a **DVI** connector, use the *DVI-HDMI-Adapter-Cable* (A6400049), which is available as accessory.

Initial configuration

IMPORTANT: The complete configuration and operation of the device is described in the *Configuration and Operation* manual.

The manual is continuously updated and only available online:

https://gdsys.de/A9100284

Opening a preferred client

You can choose between three different clients to start KVM sessions or configure your device.

The clients are optimized for different purposes and systems:

- **HTML KVM Client (HKC):** You can start and operate the HKC in any browser. With this client, both the *video performance* and the *virtual media functionality* are limited.

  NOTE: To start the **HKC**, open the following URL in your browser:

  https://192.168.0.1

- **Active KVM Client (AKC):** The AKC is the recommended client for Windows users with *Microsoft Edge Legacy*, *Internet Explorer 11* or another browser supporting the *click-once* technology.

  NOTE: To start the **AKC** on a Windows computer, use *Microsoft Edge Legacy*, *Internet Explorer 11* or another browser supporting the *click-once* technology to open the following URL:

  https://192.168.0.1/akc

- **Virtual KVM Client Standalone (VKCS):** The VKCS is the recommended client for Windows as well as macOS and Linux operating systems supporting Java.

  NOTE: To start the **VKCS** on a computer supporting Java, open the following URL in your browser:

  https://192.168.0.1/vkcs

  If your browser does not automatically launch the downloaded file, double-click it to start it.

Changing the admin password

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 **4658**.

How to change the admin password:

1. Start the desired client (see above).
2. Follow the instructions of the client to change the Admin password.

Configuring network settings

In the default setting of the device, the static IPv4 address **192.168.0.1** is assigned to the network interface.

You can change the IP address and activate DHCP in the client under **Device Settings > Network**.

How to change the device network settings:

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

Enable IPv4:	Enable or disable IPv4 protocol
IP Auto Configuration:	Select the method by which the IPv4 settings are set: ▪ **Static:** Enter a static IP address. ▪ **DHCP:** Obtain IP address from a DHCP server.
IP Address/ Prefix Length:	Assign a static IPv4 address and specify the prefix length. The default IPv4 address is **192.168.0.1/24**. **NOTE:** This setting is only available when using a static IP address (**Static**).
Default Gateway	Enter the IP address of the gateway. **NOTE:** This setting is only available when using a static IP address (**Static**).
Preferred Hostname:	Enter a preferred hostname. **NOTE:** This setting is only available if the IP address is obtained by a **DHCP** server.

3. Enter the following values under **Ethernet > IPv6** :

Enable IPv6:	Enable or disable IPv6 protocol
IP Auto Configuration:	Select the method by which the IPv6 settings are set: ▪ **Static:** Enter a static IP address. ▪ **DHCP:** Obtain IP address from a DHCP server.
IP Address/ Prefix Length:	Assign a static IPv6 address and specify the prefix length. **NOTE:** This setting is only available when using a static IP address (**Static**).
Default Gateway	Enter the IP address of the gateway. **NOTE:** This setting is only available when using a static IP address (**Static**).
Preferred Hostname:	Enter a preferred hostname. **NOTE:** This setting is only available if the IP address is obtained by a **DHCP** server.

4. Enter the following values under **Ethernet > Interface Settings**:

Speed:	Select the speed of the LAN connection: **Auto**, **10 MBit/s**, **100 MBit/s** or **1 Gbit/s**
Duplex:	Select the duplex mode of the LAN connection. **Auto**, **Full** or **Half**

5. Enter the following values under **Common Network Settings**:

DNS Resolver Preference:	Define which IP address is used when the DNS resolver returns both **Ipv4** and **Ipv6** addresses.
DNS Suffixes (optional)	If necessary, enter a DNS suffix.
First/Second DNS Server:	Enter the IP address of the DNS server. **NOTE:** If **DHCP** or **Auto** is selected for the IPv4/IPv6 settings *without* the definition of static DNS servers, the device uses the DNS servers assigned by DHCP.

6. Click on **Save**.

Setting the internal clock of the device

Set the internal clock of the device manually, or synchronize it with an NTP server via *Network Time Protocol*.

NOTE: The current system date and time of the device are displayed in the upper right corner of the web interface.

How to activate the synchronisation of the internal clock with an NTP server:

1. In the client, click on **Device Settings > Date/Time**.
2. Enter the following values under **Common Settings**:

Time Zone:	Select the time zone at the location of the device.
Automatic Daylight Saving Time Adjustment:	Activate this option if you want the time to change automatically from summer to winter time (and vice versa).
Time Setup Method:	Select the option **Synchronize with NTP Server**.

3. Enter the following values under **NTP Settings**:

First/Second NTP Server:	Enter the address of an NTP server.

4. Click on **Save**.

How to manually set the internal clock of the device:

1. In the client, click on **Device Settings > Date/Time**.
2. Enter the following values under **Common Settings**:

Time Zone:	Select the time zone at the location of the device.
Automatic Daylight Saving Time Adjustment:	Activate this option if the time change from summer to winter time (and vice versa) should be done automatically.
Time Setup Method:	Select the option **User Specified Time**.

3. Enter the following values under**User Specified Time**:

Date:	Enter the current date in **YYYY-MM-DD** format or click the calendar icon on the right to select the date in the calendar.
Time:	Enter the current time in the format **hh:mm:ss** or use the arrow keys to change the individual values. **NOTE:** The time is displayed in a 12-hour count. For time entries in the morning, select the option **am**, for time entries in the afternoon **pm**.

4. Click on **Save**.

Installing certificates

The *RemoteAccess-GATE* uses TLS 1.3 for encrypted network traffic with connected clients. When establishing a connection, the device authenticates itself to the client with a cryptographic certificate.

IMPORTANT: The device is shipped with a standard certificate. We strongly recommend replacing the standard certificate with your own certificate!

The device can independently generate a **self-signed certificates** or a **Certificate Signing Request** (CSR). Alternatively, you can load your own certificate into the device.

ADVICE: You can view the details of the active certificate under **Security > TLS Certificate**. Here, you can also download the certificate and the key.

Version 1: Creating and activating a self-signed certificate

IMPORTANT: Before creating a certificate, make sure that the internal clock of the device is set correctly (see page 9).

A self-signed certificate is the easiest and fastest way to secure the device's network traffic with an *individual* certificate.

Due to using a *self-signed* certificate, your browser and the clients will *not* trust the connection by default, because the issuer of the certificate is unknown. After you save an exception for the publisher in the browser or client, the encrypted connection can be established.

NOTE: If you want to use a certificate that is accepted by the browser and client without requiring any exceptions, create a *Certificate Signing Request* (see below) and use it to request the certificate creation from a known certificate authority.

How to create and activate a self-signed certificate:

1. In the client, click on **Security > TLS Certificate**.
2. Scroll down to **New TLS Certificate**.
3. In the **Subject** column, enter at least the data that the client has marked as required.

   The following table lists the different fields including exemplary entries:

Field	Example
Country (ISO Code)	DE
State or province	NRW
Locality	Siegen
Organization	Guntermann & Drunck GmbH
Organizational unit	
Common name	Guntermann & Drunck GmbH
E-mail address	

4. In the right column, under **Subject Alternative Names** , enter up to ten IP addresses or hostnames for which the certificate will be valid.
5. Activate the **Self-sign** option under**Key Creation Paramaters**.
6. In the **Validity in days** field, enter the number of days the certificate will be valid.
7. Click on **Create New TLS Key**.
8. Check the certificate details display to make sure you have selected the correct files and click on **Install Key and Certificate**.

Version 2: Creating a Certificate Signing Request for a certificate authority

IMPORTANT: Before creating a certificate, make sure that the internal clock of the device is set correctly (see page 9).

1. In the client, click on **Security > TLS Certificate**.
2. Scroll down to **New TLS Certificate**.
3. In the **Subject** column, enter at least the data that the client has marked as required.

   The following table lists the different fields including exemplary entries:

Field	Example
Country (ISO Code)	DE
State or province	NRW
Locality	Siegen
Organization	Guntermann & Drunck GmbH
Organizational unit	
Common name	Guntermann & Drunck GmbH
E-mail address	

4. In the right column, under **Subject Alternative Names** , enter up to ten IP addresses or hostnames for which the certificate will be valid.

   IMPORTANT: Make sure that the **Self-sign** option under**Key Creation Paramaters** is disabled.

5. Under **Key Creation**, enter a challenge password in the fields **Challenge** and **Confirm challenge**.
6. Click on **Create New TLS Key**.
7. Click on **Download Certificate Signing Request** and submit the downloaded file to a certification authority to create the certificate.
8. Open the certificate you received from the certification authority under **Upload Certificate**, and click on **Upload**.

Version 3: Loading your own certificate into the device and activating it

How to load an externally created certificate into the device and activate it:

1. In the client, click on **Security > TLS Certificate**.
2. Under **New TLS Certificate** , click on **Upload Key and Certificate**.
3. Click on **Key File** and open the existing key file.
4. Click on **Certificate File** and open the existing certificate file.
5. Click on **Upload**.
6. Check the certificate details display to make sure you have selected the correct files and click on **Install Key and Certificate**.

Status displays

LEDs on the front panel

Description	Colour	Status	Meaning
Power	**Green**	On	The device is supplied with power.
		Blinking	The device is supplied with power. Remote target connection
		Off	The device is not supplied with power.

LEDs on the back panel

The LEDs integrated into the network socket indicate the network speed and activity of the socket:

Yellow (left)	Green (right)	Meaning
Off	Off	Inactive connection
On	Off	1000 MBps link; no activity
Blinking	Off	1000 MBps link; activity (RX, TX)
Off	On	100 MBps link; no activity
Off	Blinking	100 MBps link; Active (RX, TX)
On	On	10 MBps link; no activity
Blinking	Blinking	10 MBps link; activity (RX, TX)

Technical data

REMOTEACCESS-GATE		
Interfaces to local console	Video:	1 × HDMI (HDMI Out)
	Keyboard and mouse signals:	2 × USB-A (USB K/M)
Interfaces to G&D device or computer	Video:	1 × HDMI (HDMI In)
	Keyboard and mouse signals:	1 × USB-B (USB In)
Other interfaces	Network:	1 × RJ45 socket (Network)
	Service:	1 × D-Sub 9 plug
	Control:	5-pole terminal block
Video	Format:	HDMI 1.4b
	Colour depth:	24 bits
	Video bandwidth:	25 to 297 MP/s
	Max. resolution:	▪ 2560 × 1600 (60 Hz) ▪ 4096 × 2160 (30 Hz)
	Exemplary resolutions:	▪ 3840 × 2160 (24, 25 or 30 Hz) ▪ 2560 × 1440 (60 Hz) ▪ 1920 × 1200 (60 Hz) ▪ 1920 × 1080 (24, 30 or 60 Hz) ‣ Further standard resolutions within the framework of the max. video bandwidth possible.
	Vertical frequency:	24 Hz to 85 Hz
	Horizontal frequency:	20 kHz to 99 kHz
Audio ‣ Embedded audio	Transmission type:	2-channel LPCM, stereo
	Resolutions:	16 bits
	Refresh rates:	Up to 48 kHz
Power supply	Type:	Table power pack
	Connection:	1 × 4-pole connector
	Power consumption:	5 VDC; max. 4 A
Housing	Material:	Anodised aluminium
	Dimensions (W × H × D):	160 × 44.5 × 144 mm
	Weight:	Approx. 720 g
Operating environment	Temperature:	+0°C to +40°C
	Air humidity:	20 % to 80 %, non-condensing
Storage environment	Temperature:	-20°C to +60°C
	Air humidity:	15 % to 80 %, non-condensing
Conformity		CE, EAC, FCC Class A, RoHS

NOTES

NOTES

G&D. FEELS RIGHT.

Hauptsitz | Headquarter
Guntermann & Drunck GmbH Systementwicklung
Obere Leimbach 9 | D-57074 Siegen | Germany
Phone +49 271 23872-0
sales@gdsys.com | www.gdsys.com

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