KNX
Produktdokumentation

Stand der Dokumentation:
07.04.2022

Gira S1
Bestell-Nr. 2089 00

Gira S1 (Abb. 1:1)

GIRA

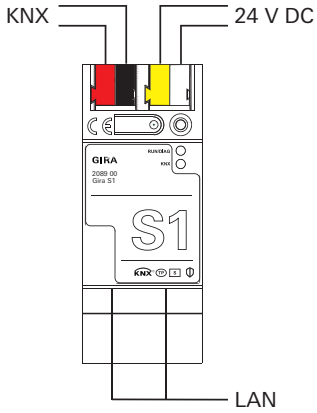
Inhaltsverzeichnis

1. Die Projektierung des Gira S1 auf einen Blick

Diese Seite zeigt den Ablauf der Projektierung auf einen Blick. Die ausführliche Anleitung für die Inbetriebnahme können Sie in den Kapiteln nachlesen, die in den jeweiligen Arbeitsschritten angezeigt werden.

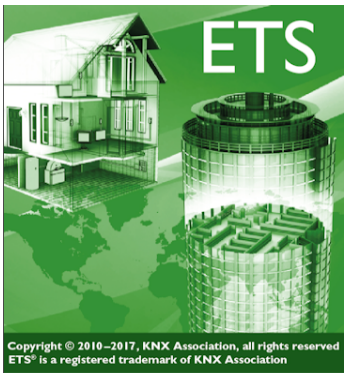
1.1. Montage (siehe Kapitel 7)

- Montieren Sie den Gira S1.
- Schließen Sie die Spannungsversorgung,
- den KNX Anschluss und
- die Verbindung zum Netzwerk an.



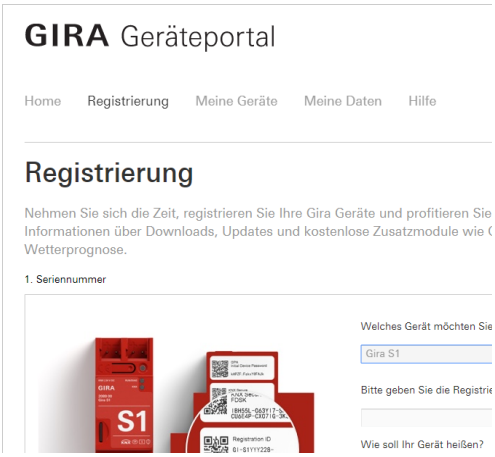
1.2. Projektierung in der ETS (siehe Kapitel 8)

- Legen Sie den Gira S1 als Gerät in der ETS an.
- Vergeben Sie die physikalischen Adressen für den Gira S1.
- Weisen Sie die gewünschten Gruppenadressen zu.
- Übertragen Sie das Applikationsprogramm und die Projektierung.



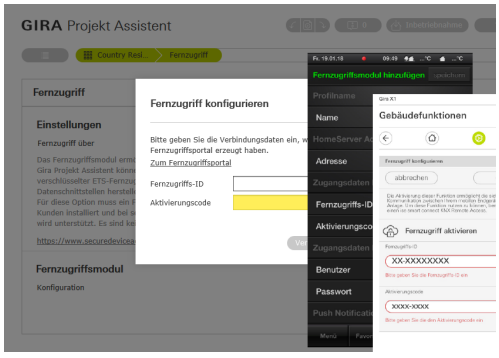
1.3. Projektierung im Gira Geräteportal (siehe Kapitel 10)

- Registrieren Sie den Gira S1.
- Legen Sie die Benutzer an.
- Übertragen Sie ggf. den Gerätebesitz.
- Optional können Sie z. B. noch Benachrichtigungen einrichten.



1.4. Konfiguration der Applikationszugänge (siehe Kapitel 10.7)

- Erzeugen Sie im Gira Geräteportal zunächst die Aktivierungscodes, die Sie anschließend
- in die entsprechende Eingabemaske der jeweiligen Applikation (z. B. Gira Smart Home App, Gira HomeServer App, Gira S1 Windows Client oder Gira Projekt Assistent) eintragen.



2. Produktbeschreibung

2.1. Funktionen

- Sicherer Fernzugriff per Gira HomeServer- und Gira Smart Home App auf das Smart Home mit KNX.
- Sicherer Fernzugriff auf webbasierte Visualisierungen.
- Sichere Fernwartung und Fernprogrammierung vom Gira HomeServer, Gira G1, Gira X1, Gira L1 und Gira KNX IP-Router.
- Sichere Fernprogrammierung über den Gira HomeServer-Experten.
- Sichere Fernprogrammierung über den Gira Projekt Assistent (GPA).
- Sichere Fernwartung und Fernprogrammierung von KNX Projekten mittels ETS4 oder ETS5 in Verbindung mit dem Gira Projekt Assistent oder dem Gira S1 Windows Client. Unterstützt wird die Programmierung und Diagnose über Gruppen- und Busmonitor.
- Sicherer Fernzugriff auf HTML-Seiten (von z.B. Kamera, NAS, Router oder Switch) im Smarthome-Netzwerk (in Abhängigkeit von der technischen Umsetzung der jeweiligen Gerätewebseite).
- Sichere Datenübertragung mittels SSL/TLS-Verschlüsselung.
- Portalserver steht in Deutschland und unterliegt dem deutschen Datenrecht.
- Unabhängigkeit vom Internetprovider und eingesetzten Routern. Sicherer Fernzugriff auch bei IPv6 Dual Stack Lite- (z.B. bei Unitymedia), LTE- oder UMTS-Anschlüssen.
- Zugriffsmanagement der gesicherten Verbindungen über KNX Kommunikationsobjekte, Gira Smart Home App, Gira HomeServer-App und QuadClient.
- Statussignalisierung der gesicherten Verbindungen über KNX Kommunikationsobjekte.
- KNX Statusmeldungen per E-Mail versenden. Der E-Mail kann optional einen Anhang hinzugefügt werden.
- KNX Statusmeldungen per SMS oder Sprachanruf versenden über den kostenpflichtigen Zusatzdienst sms77 oder MessageBird.
- Optimierte KNX IP-Kommunikation, für mobile und sehr langsame Verbindungen.
- Unterstützt die beschleunigte Übertragung von der ETS zu KNXnet/IP-Geräten über eine direkte KNX IP-Verbindung.
- Ein integrierter Ethernet Switch (zwei RJ45 Anschlüsse) vereinfacht die Verbindung mehrerer IP-Geräte. Dadurch können mehrere Gira S1 oder auch andere IP-Geräte in der Verteilung ohne Zuhilfenahme anderer aktiver Komponenten verbunden werden.
- Der Gira S1 kann als Datenlogger eingesetzt werden. Er besitzt einen Kartenleser für microSDHC-Karten bis 32 GB. Auf der Karte können die KNX Telegramme in einem ETS4-konformen Format für Analysen aufgezeichnet werden. Der Kartenspeicher kann als Ringspeicher oder als Festspeicher verwendet werden.
- Als Zeitgeber kann der Gira S1 Zeit und Datum in konfigurierbaren Intervallen auf den Bus senden. Es ist möglich über einen Trigger das Senden der aktuellen Zeit und des aktuellen Datums auszulösen.
- VPN-Netzkopplung ermöglicht u. a. den Zugriff auf KNX Installationen, Visualisierungsoberflächen und Dateien im Heimnetzwerk. Auch für Smartphone-Apps ist ein unkomplizierter Zugang zum KNX System und weiteren Anwendungen gewährleistet. Der VPN-Zugriff lässt sich über KNX Kommunikationsobjekte steuern und überwachen.
- Volle Unterstüzung von KNX Secure.
- Versenden von Push Notifications an die Gira Smart Home App.
- Unterstützung einer Secure-Tunnelingverbindung zwischen Gira HomeServer und Gira S1.

2.2. KNX Secure

Der Gira S1 ist KNX Secure kompatibel. Das notwendige KNX-Secure-Zertifikat bzw. der darin enthaltene FDSK (Factory Default Setup Key, Fabrikschlüssel) befindet sich seitlich als Aufkleber auf dem Gerät und liegt zusätzlich dem Gerät bei.

Für maximale Sicherheit empfehlen wir, die Aufkleber auf dem Gerät zu entfernen.

Den FDSK können Sie selbst nicht wiederherstellen

Bewahren Sie den FDSK sicher auf. Falls Sie den FDSK trotz aller Sorgfalt verlieren sollten, kontaktieren Sie unseren Support.

2.3. Funktionsbeschreibung

Der Gira S1 wird im Heimnetzwerk des Kunden installiert und macht das Heimnetzwerk bereit für den sicheren Zugriff über das Internet.

Der Gira S1 wird per Ethernet an das Heimnetzwerk angeschlossen. Er verbindet sich automatisch über den vorhandenen Internetzugang mit dem Gira Geräteportal. Die Kommunikation zwischen Gira S1 und Gira Geräteportal ist per AES verschlüsselt und mit digitalen Zertifikaten gesichert (Details siehe Kapitel 2.4.1 "HTTPS-Proxy httpaccess.net").

Sie können bereits jetzt auf fast alle mit dem Netzwerk verbundenen Geräte über das Internet zugreifen.

Die Gira Smart Home App und der GPA haben die Möglichkeit, direkt über das Gira Geräteportal mit dem Gira S1 zu kommunizieren. Bei anderen Windows-Anwendungen, wie z.B. ETS oder Gira Experte erfolgt der Zugriff über den Gira S1 Windows Client (siehe Kapitel 2.5 "Clientsoftware (Gira S1 Windows Client)").

Falls eine KNX Installation vorhanden ist, kann diese optional über den KNX Anschluss mit dem Gira S1 verbunden werden. Dadurch kann von überall z.B. mit der ETS auf die KNX Geräte zugegriffen werden.

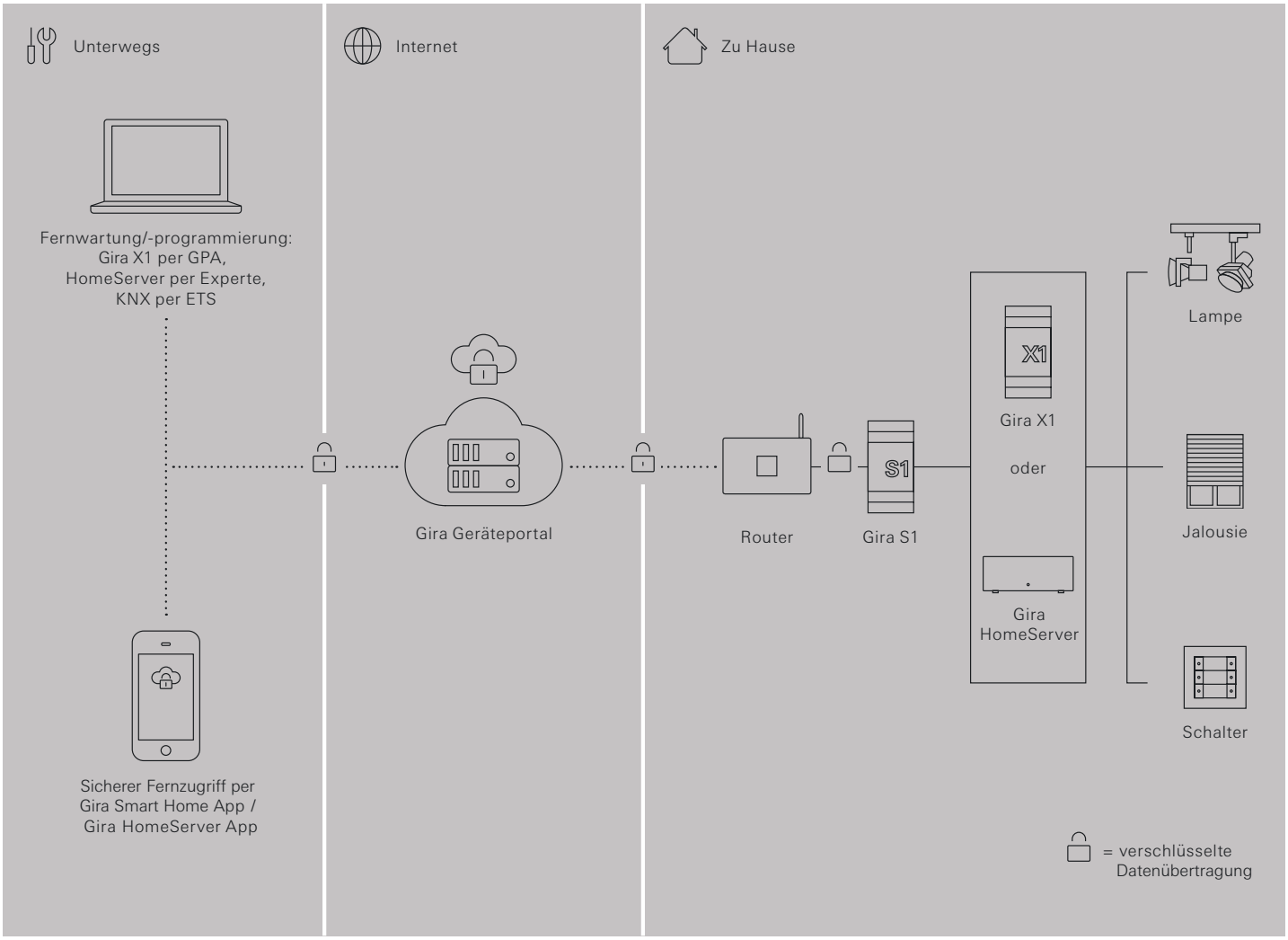


Bild 1: Übersicht über den sicheren Fernzugriff mit dem Gira S1

2.4. Gira Geräteportal

Der Gira S1 wird über das Gira Geräteportal (https://geraeteportal.gira.de) verwaltet. Über das Gira Geräteportal können Sie auch weiteren Benutzern Zugriff auf den Gira S1 und damit auf die im Heimnetzwerk vorhandenen KNX- und Netzwerkgeräte gewähren.

Einem Konto auf dem Gira Geräteportal können beliebig viele Gira S1 zugeordnet werden. Wenn Sie oder von Ihnen autorisierte Personen auf Endgeräte im Heimnetzwerk zugreifen möchten, ist daran immer das Gira Geräteportal als Vermittlungsstelle beteiligt. Das Gira Geräteportal speichert die übertragenen Daten nicht, sondern leitet diese nur weiter.

Der Server für das Gira Geräteportal wird in Deutschland unter Einhaltung der deutschen Datenschutzrichtlinien betrieben.

Hinweis

Die Benutzung des Gira Geräteportals erfordert aus technischen Gründen die Nutzung von Cookies im Internet Browser.

2.4.1. HTTPS-Proxy httpaccess.net

Die meisten Netzwerkgeräte wie z.B. Kameras oder Netzwerkdrucker haben heute einen integrierten Webserver für den Zugriff mit einem Webbrowser. Für diesen Fall ist der Zugriff über das Gira Geräteportal besonders einfach. Jedes über einen Gira S1 erreichbare Netzwerkgerät bekommt automatisch einen eigenen Namen unterhalb der Domain httpaccess.net. Unter diesem Namen können Sie von überall mit einem Webbrowser das entsprechende Netzwerkgerät erreichen.

Auch hier ist die komplette Kommunikation über das Internet verschlüsselt und es erfolgt eine Benutzerauthentifizierung gemäß der für den Gira S1 auf dem Gira Geräteportal eingestellten Zugriffsfreigaben.

Damit Sie sich keine Links merken müssen, verwaltet das Gira Geräteportal eine Linkliste der Endgeräte, die über httpaccess.net erreichbar sind. Wenn das Netzwerkgerät UPnP unterstützt, kann das Gira Geräteportal es automatisch in die Linkliste eintragen. Geräte, die nicht automatisch der Liste hinzugefügt werden, können auch manuell in die Liste eingetragen werden.

2.4.2. Kommunikation – sicher, zuverlässig und einfach zu handhaben

Der Gira S1 verwendet für die Kommunikation mit dem Portalserver die Standardprotokolle HTTPS, TLS/SSL und Websockets. Alle Daten werden per AES verschlüsselt.

Gira S1 und Gira Geräteportal authentifizieren sich gegenseitig mit digitalen Zertifikaten und RSA-Schlüsselpaaren. Die Zertifikate sind von unserer eigenen Zertifizierungsstelle ausgestellt.

Durch den Einsatz von Standardprotokollen und dadurch, dass der Gira S1 sich aktiv mit dem Gira Geräteportal verbindet, erreichen wir größtmögliche Kompatibilität mit der vorhandenen Infrastruktur. Für den Internetrouter unterscheidet sich die Kommunikation des Gira S1 nicht von einer verschlüsselten Verbindung Ihres Webbrowsers z.B. beim Onlinebanking oder bei einer Google-Suche.

Für Sie hat das den Vorteil, dass der Gira S1 ohne komplizierte Konfiguration einfach funktioniert. Das ist ein deutlicher Vorteil gegenüber anderen Ansätzen zum sicheren Fernzugriff, wie z.B. VPN oder SSH-Tunnelling.

Der Fernzugriff funktioniert im Unterschied zu anderen Lösungen sogar über einen Mobilfunk- oder IPv6-Zugang, auch wenn dieser nicht über eine eindeutige von außen erreichbarer IP-Adresse verfügt.

2.4.3. Benachrichtigungen vom Gira S1

KNX Kommunikationsobjekte sowie Systemereignisse wie das An-/Abmelden eines Gira S1 am Portal können genutzt werden, um Benachrichtigungen im Portalserver zu generieren. Diese können neben statischen Texten auch Werte vom KNX enthalten oder auch einen Anhang wie z.B. ein Kamerabild beinhalten.

Diese Benachrichtigungen können konfigurierbar per E-Mail, Push-Nachrichten, Telefon oder SMS weitergeleitet werden. Der Versand von SMS oder Sprachanruf erfolgt über den kostenpflichtigen Zusatzdienst sms77 oder MessageBird. Zusätzlich ist eine Weiterleitung von IFTTT-Auslösern möglich.

2.5. Clientsoftware (Gira S1 Windows Client)

Der Gira S1 Windows Client wird auf einem Windows PC installiert. Über den Gira S1 Windows Client erhalten andere auf dem PC laufende Anwendungen Zugriff auf Ihre Geräte ohne selbst die Fernzugriffs-Funktion unterstützen zu müssen.

Der Gira S1 Windows Client baut über das Gira Geräteportal eine verschlüsselte Verbindung zum Gira S1 auf. Diese Verbindung wird anderen Anwendungen auf dem PC und im lokalen Netzwerk bereitgestellt, damit diese auf Geräte im entfernten Netzwerk zugreifen können. Beispiele:

- Mit der ETS können Sie KNX Geräte konfigurieren.
- Mit dem Gira HomeServer Experten können Sie einen Gira HomeServer konfigurieren.
- Per Remotedesktopverbindung können Sie auf einen Windows-PC zugreifen.
- Per SSH und/oder X-Windows können Sie auf einen Linux-PC oder embedded Linux Geräte zugreifen.
- Über frei konfigurierbare TCP-Portweiterleitungen werden viele weitere Anwendungsfälle unterstützt.

3. Anwendungsszenarien

3.1. Zugriff auf den Gira X1

In Verbindung mit dem Gira X1 können die Gebäudefunktionen über den sicheren Fernzugriff mit der Gira Smart Home App gesteuert werden.

Die Programmierung oder Wartung des Gira X1 über den Gira Projekt Assistent (GPA) kann ebenfalls über den sicheren Fernzugriff erfolgen.

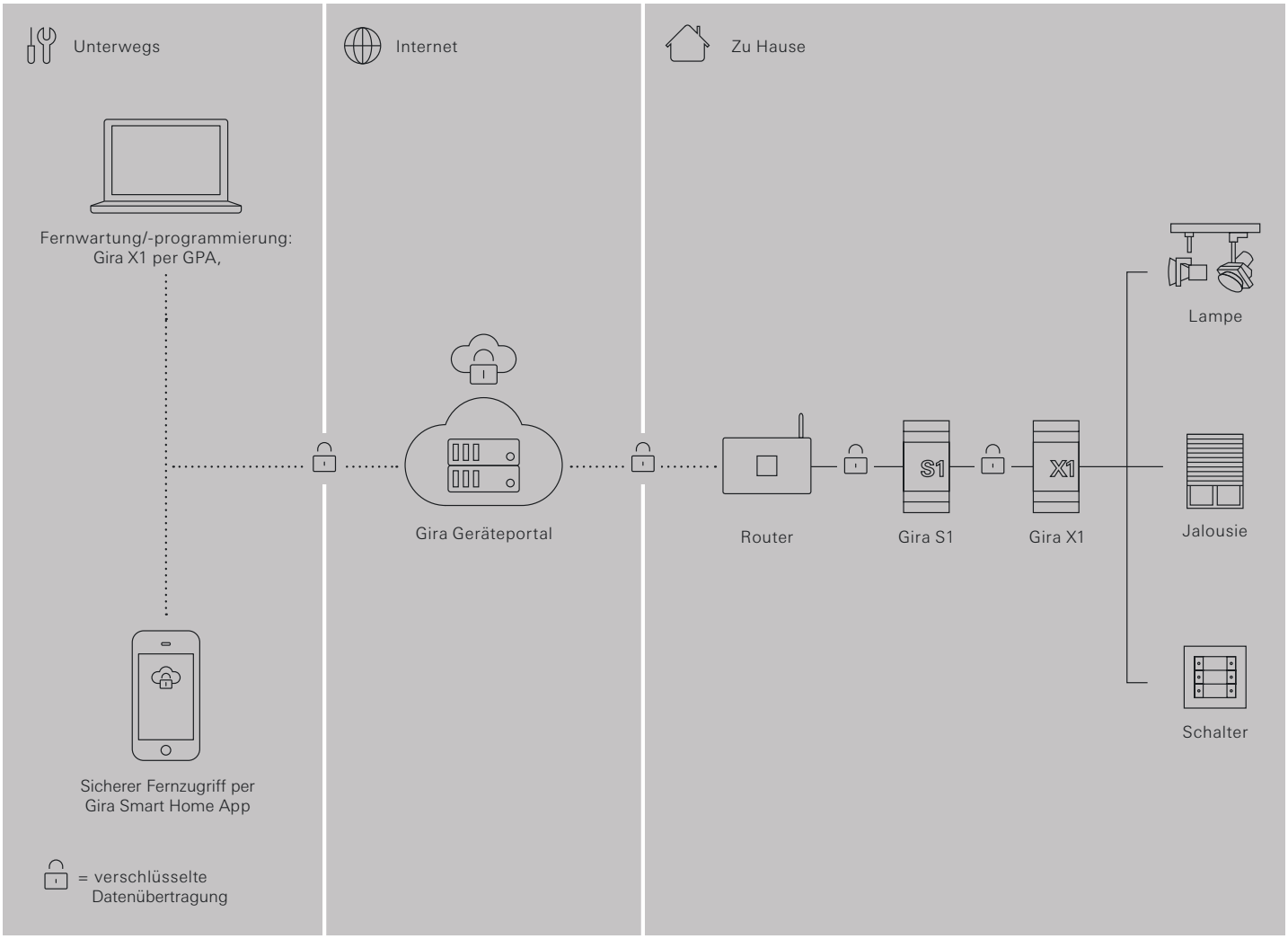


Bild 2: Konfiguration und Bedienung des Gira X1

3.2. Konfiguration und Steuerung des Gira HomeServer

Der Zugriff auf den Gira HomeServer funktioniert sehr ähnlich dem Zugriff auf die KNX Installation. Zum einen wird der Zugriff auf die KNX Installation über den Gira HomeServer über das Eiblib/IP Protokoll, zum anderen die Konfiguration mit dem Experten unterstützt. Darüber hinaus können Sie auch direkt auf die KNX Installation über die Schnittstellenfunktion des Gira S1 zugreifen. Auch hierbei werden alle Daten beim Transport über das Internet verschlüsselt.

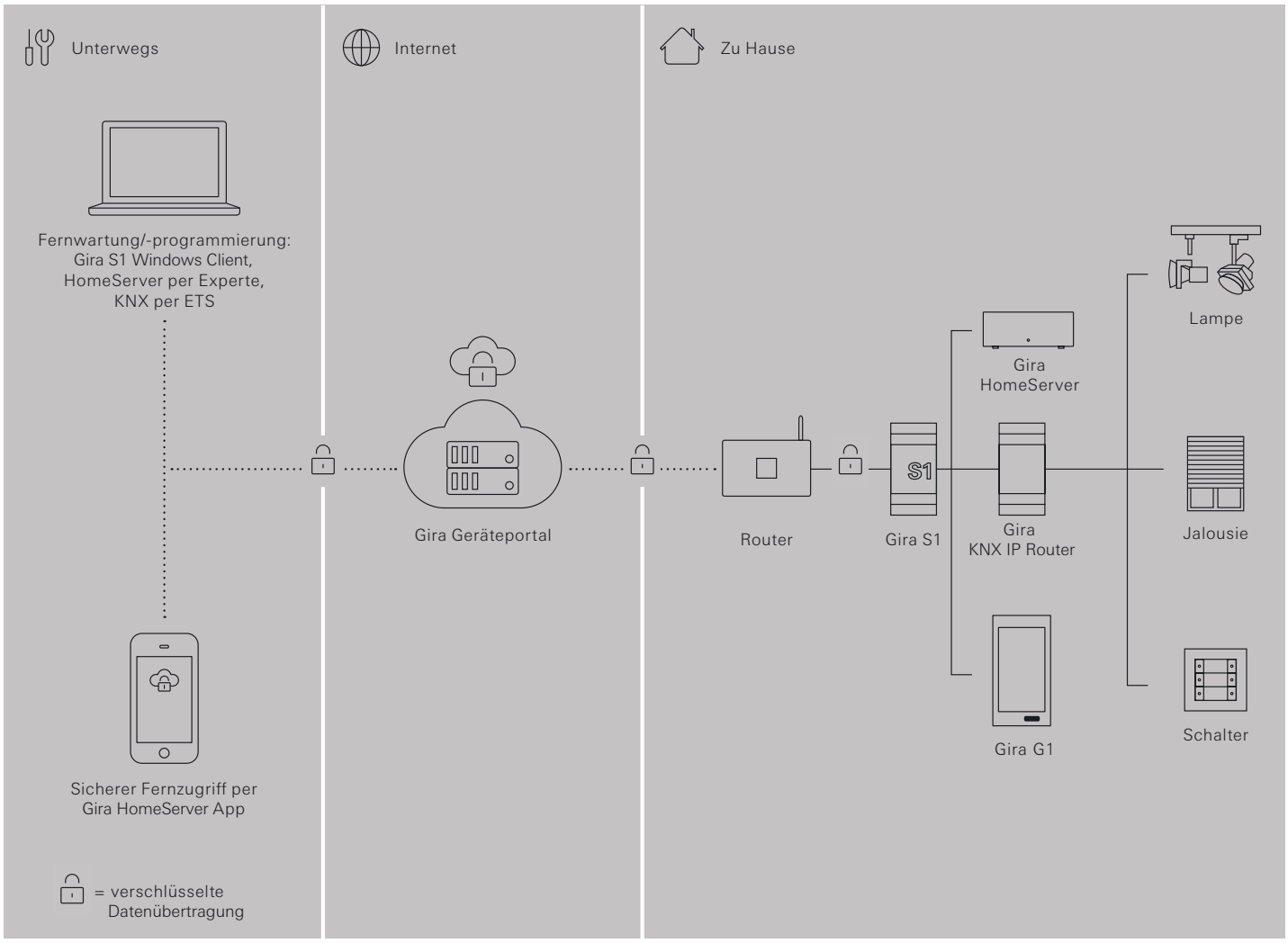


Bild 3: Sichere Konfiguration des Gira HomeServers mit dem Gira S1.

Hinweis

Da für das Eiblib/IP sowie das Gira HomeServer Konfigurationsprotokoll keine automatische Erkennung möglich ist, ist für die Nutzung dieser Protokolle über Fernzugriff folgendes zu beachten: Der Gira S1 Windows Client stellt die Protokollübertragung lokal über die IP Adresse 127.0.0.1 zur Verfügung, d.h. wenn z.B. in der ETS eine Eiblib/IP Verbindung konfiguriert wird, so muss bei der IP Adresse dann bei der Nutzung über Fernzugriff 127.0.0.1 (statt der IP Adresse des Gira HomeServers im entfernten Netzwerk) eingetragen werden. Gleiches gilt für den Download mit dem Experten. Weitere Informationen siehe Kapitel 11.3.2 "Fernkonfiguration Gira HomeServer und Nutzung von Eiblib/IP".

3.3. Verbindung Gira S1 mit Gira HomeServer über KNX Secure Tunneling

Der Gira HomeServer kann direkt über den Gira S1 an den KNX Bus angebunden werden. Dazu gehen Sie wie folgt vor:

3.3.1. Einstellungen in der ETS

- Wählen Sie den Gira S1 aus.
- Aktivieren Sie die sichere Inbetriebnahme.
- Aktivieren Sie das Secure Tunneling.

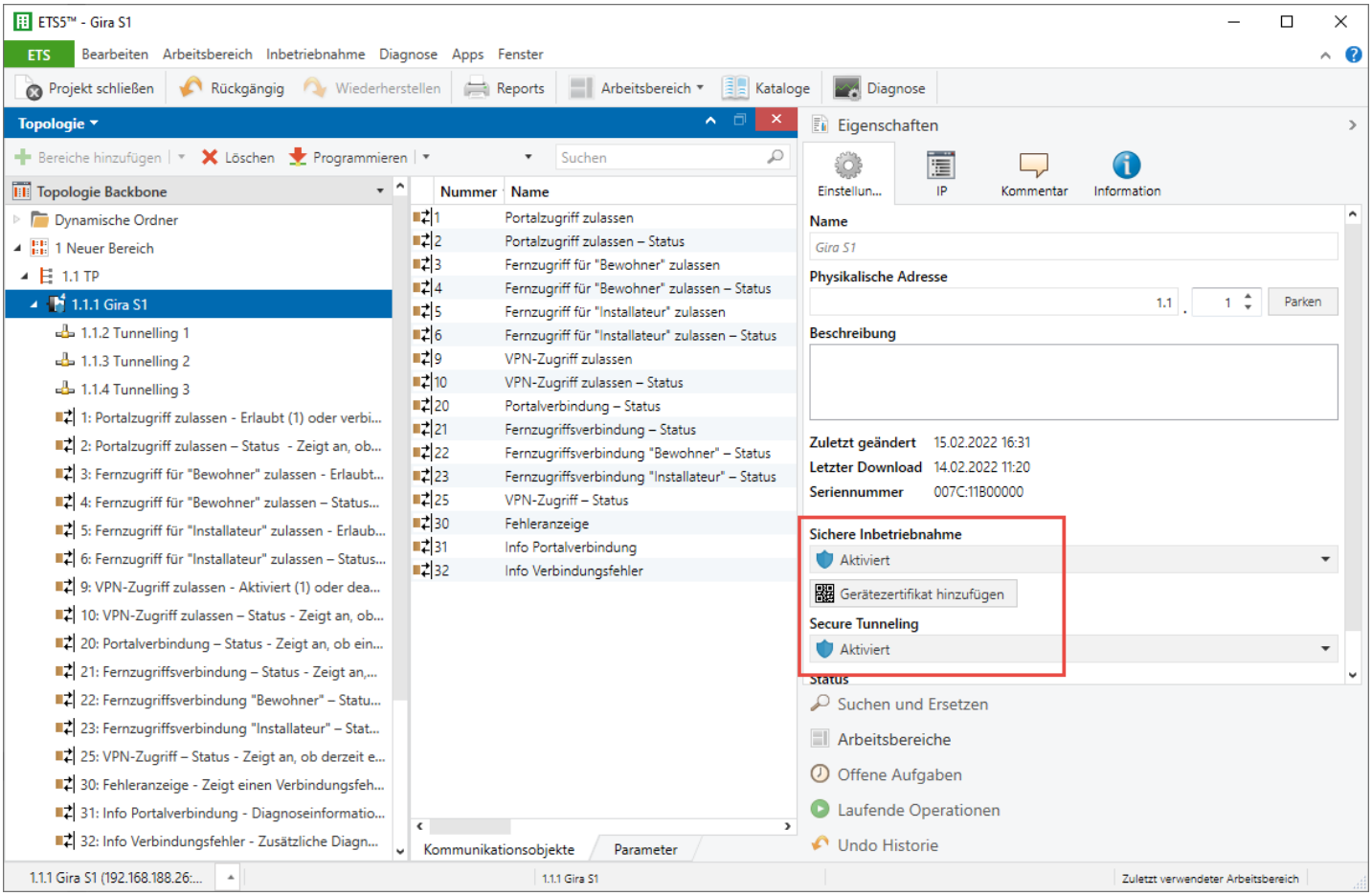


Bild 4: Sichere Inbetriebnahme und Secure Tunneling aktivieren

Eine der vorhandenen Tunneling-Verbindungen wird für den Gira HomeServer benötigt:

- Wählen Sie eine Tunneling-Verbindung aus.
- Notieren Sie die physikalische Adresse dieser Tunneling-Verbindung.

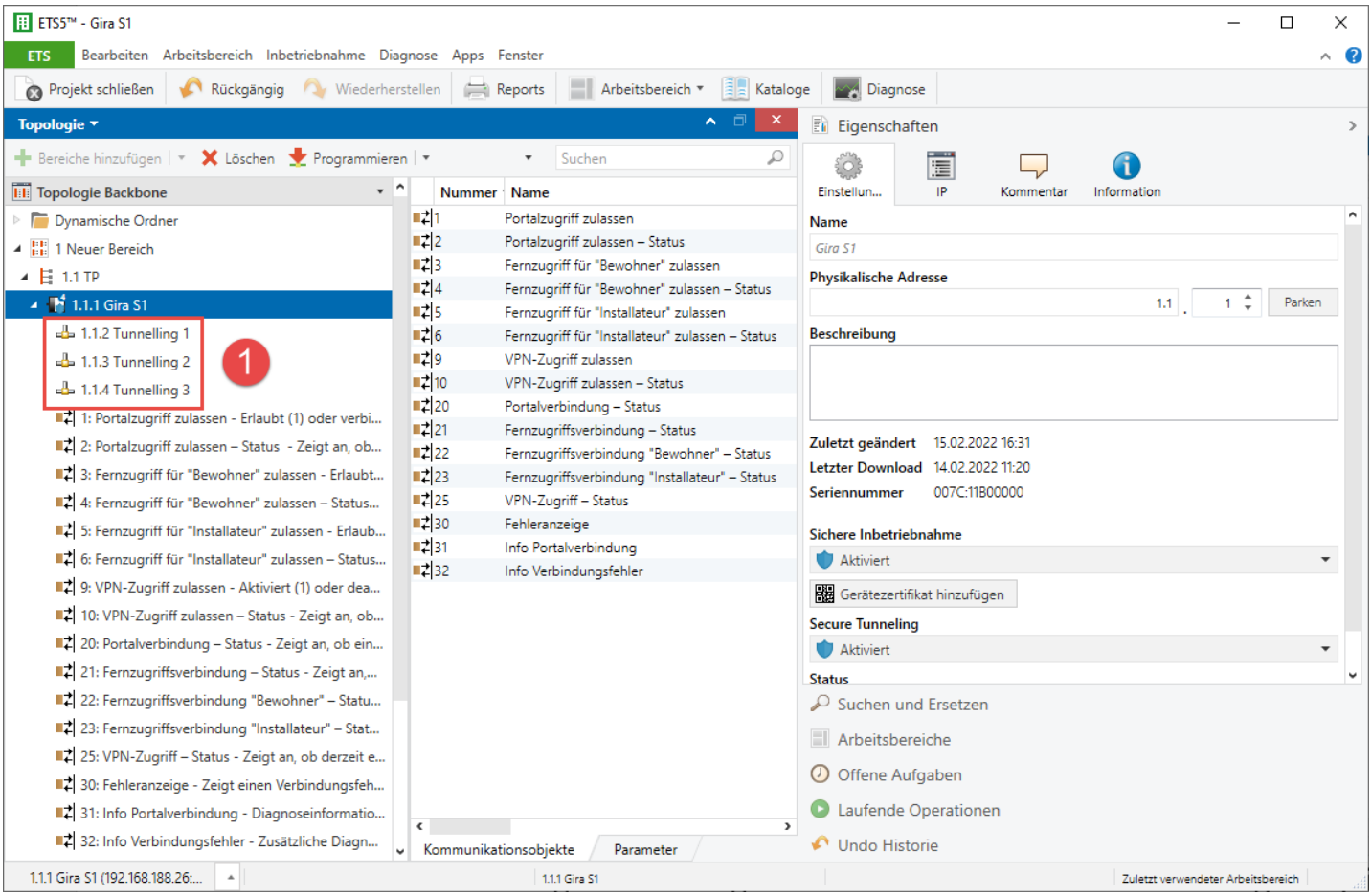


Bild 5: Physikalische Adresse der Tunneling-Verbindung

- Wechseln Sie auf den Reiter „Bus“.
- Notieren Sie die IP-Adresse des Gira S1

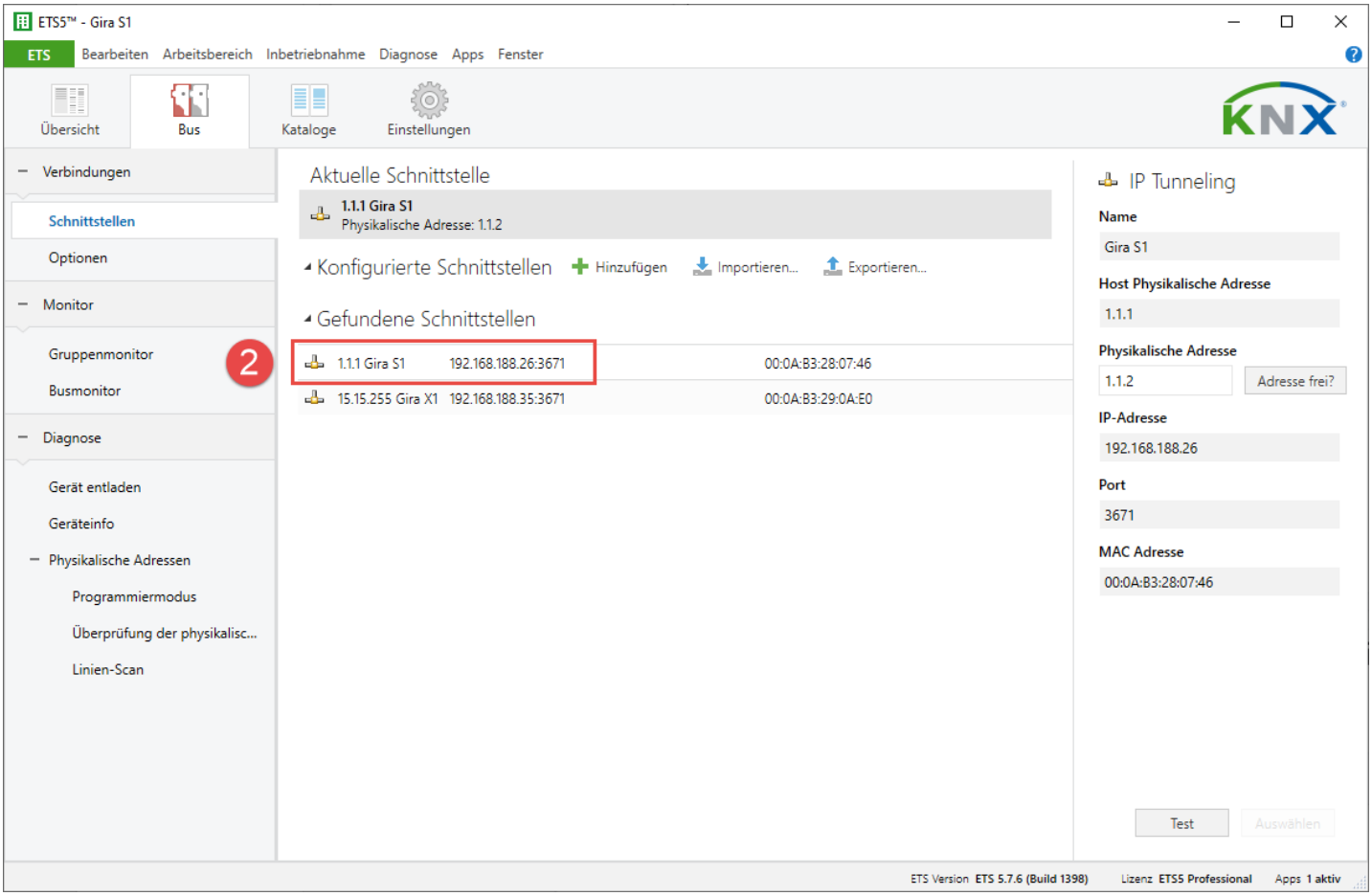


Bild 6: IP-Adresse des Gira S1

- Wählen Sie den Gira S1 aus und wechseln Sie auf den Reiter „IP“.
- Notieren Sie das Inbetriebnahmepasswort und den Authentifizierungscode.

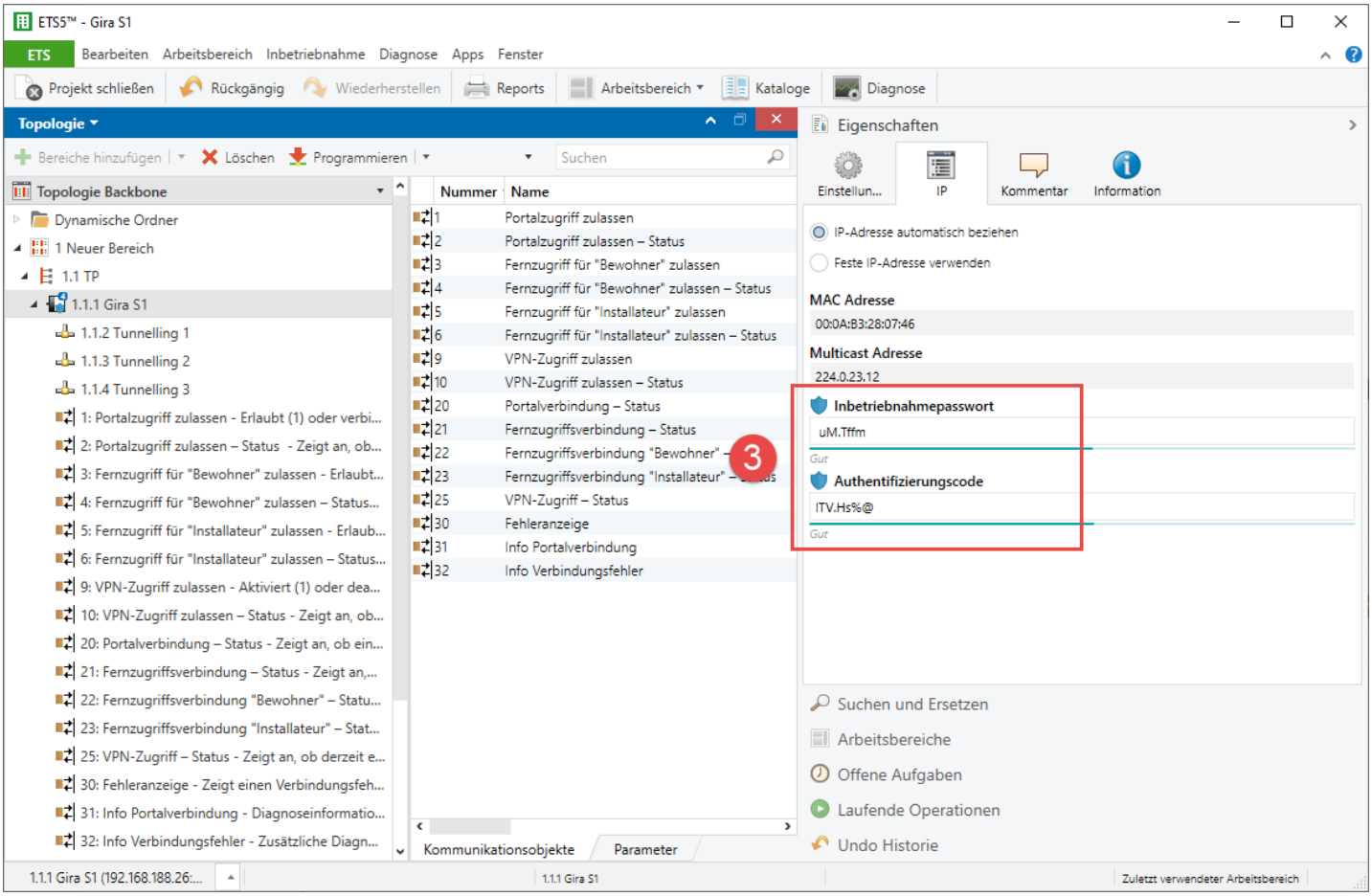


Bild 7: Gira S1 Passwörter

3.3.2. Einstellungen im Gira HomeServer Experten

- Navigieren Sie im Gira HomeServer Experten zu den „Projekteinstellungen“ und öffnen Sie den Reiter „KNX & iETS“.
- Tragen Sie die zuvor notierten Parameter in die entsprechenden Felder ein:

Parameter	Eintrag
Schnittstelle:	KNXnet/IP tunneling mit KNX Secure Unterstützung
Physikalische Adresse:	Physikalische Adresse der gewünschten Tunneling Schnittstelle (1)
IP-Adresse:	IP-Adresse des Gira S1 (2)
Port:	3671
IP-Secure aktivieren:	Ja
Inbetriebnahmepasswort:	Inbetriebnahmepasswort des Gira S1 (3)
Authentifizierungscode:	Authentifizierungscode des Gira S1 (3)

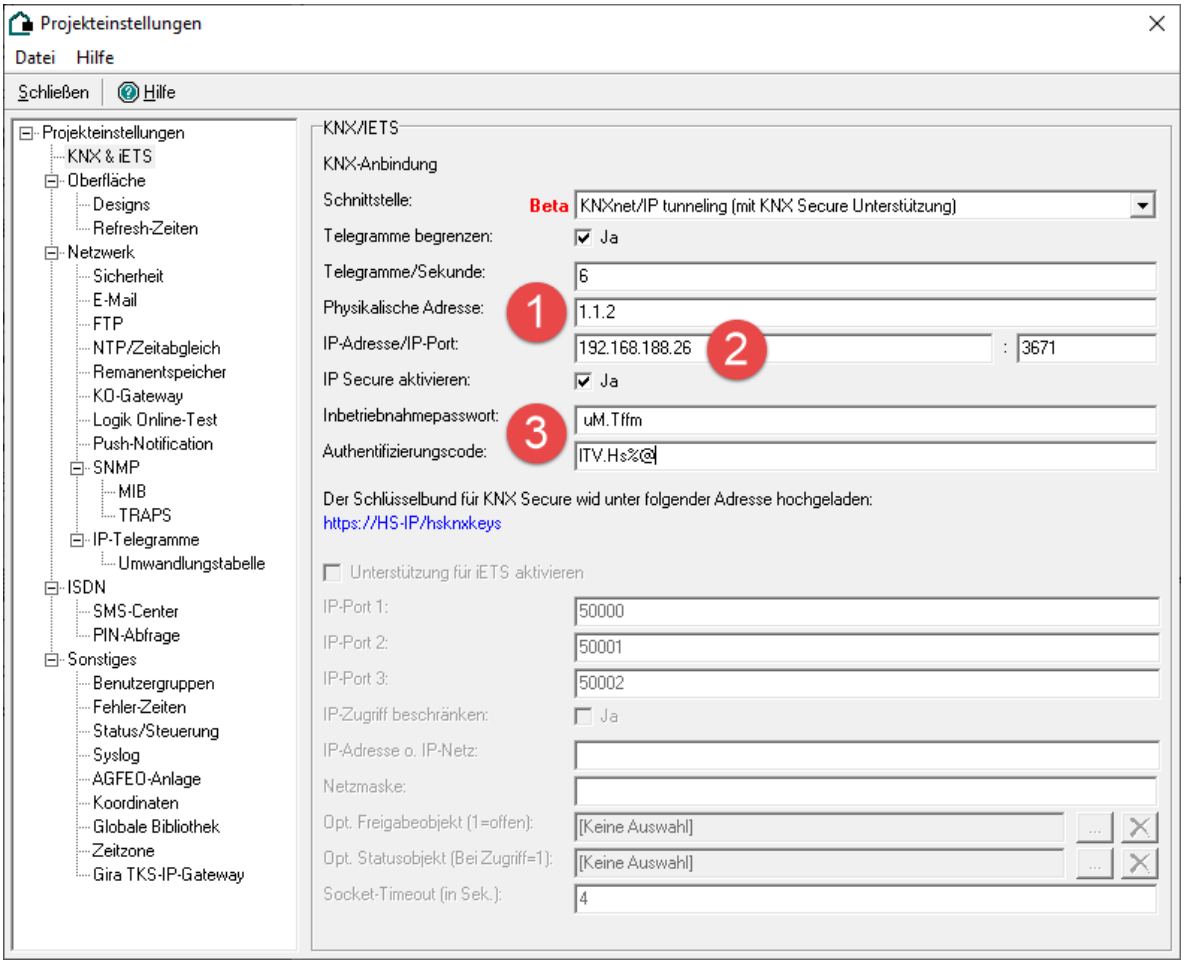


Bild 8: Gira HomeServer Experte – Einstellungen

3.3.3. Gruppenadressen „Data Secure“ übertragen (empfohlen)

Einstellungen in der ETS

- Tragen Sie alle verwendeten Gruppenadressen in die Assoziationstabelle der ausgewählten Tunneling-Verbindung ein.

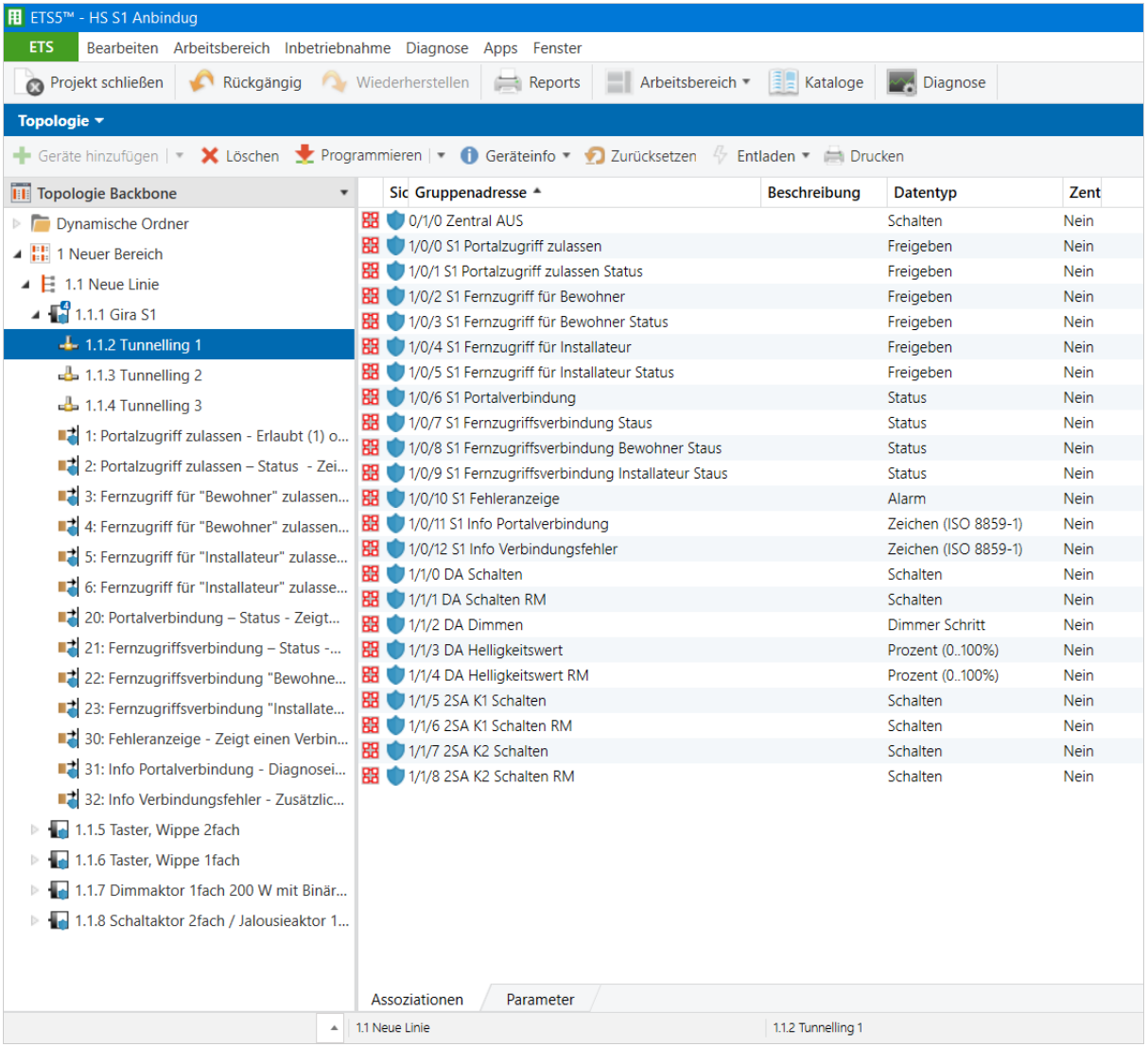


Bild 9: Assoziationen der Tunneling-Verbindung

- Klicken Sie in der ETS unter „Sicherheit“ auf „Schlüsselbund exportieren“.
- Wählen Sie die gewünschte Tunneling-Verbindung aus.

Einstellungen im Gira HomeServer Experten

- Übertragen Sie das Gira HomeServer Projekt mit dem Gira HomeServer Experten.

Einstellungen auf der Startseite des Gira HomeServers (https://HS-IP/)

- Rufen Sie die Webseite zum Hochladen der KNX Schlüsselbunddatei auf.
- Wählen Sie die exportierte Schlüsselbunddatei aus und geben Sie das Passwort ein.
- Authentifizieren Sie den Vorgang und klicken Sie auf „Hochladen“.

3.4. Zugriff auf KNX Installationen

Der Gira S1 Windows Client ermöglicht den sicheren Zugriff auf KNX Installationen über das Internet. Hierzu wird der Gira S1 Windows Client parallel zur ETS auf dem PC installiert und gestartet. Der Gira S1 überträgt alle KNX-relevanten Daten SSL/TLS verschlüsselt an das Gira Geräteportal, während dieses die Daten wiederum SSL/TLS verschlüsselt mit dem Gira S1 Windows Client austauscht. Der Gira S1 Windows Client bereitet die Daten für die ETS auf, so dass diese dann wie gewohnt genutzt werden kann.

Eine Alternative zum Gira S1 Windows Client stellt der Gira Projekt Assistent (GPA) dar. Dazu müssen Sie ein GPA Projekt angelegen, im Projektumfang die Option „Fernwartung“ aktivieren und die Fernzugriffsmethode „Fernzugriffsmodul Gira S1“ auswählen. Anschließend geben Sie die Fernzugriffs-ID und den Authentifizierungsschlüssel im Bereich „Fernzugriff konfigurieren“ ein. Diese Einrichtung müssen Sie nur einmalig durchführen. Klicken Sie nun oben rechts auf „Verbinden“. Der GPA stellt die Verbindung zum Gira S1 her. Nun können Sie die ETS starten und sehen im Bereich „Bus“ die ETS Schnittstellen in der entfernten Anlage. Die gefundenen Schnittstellen besitzen den Prefix „GPA“.

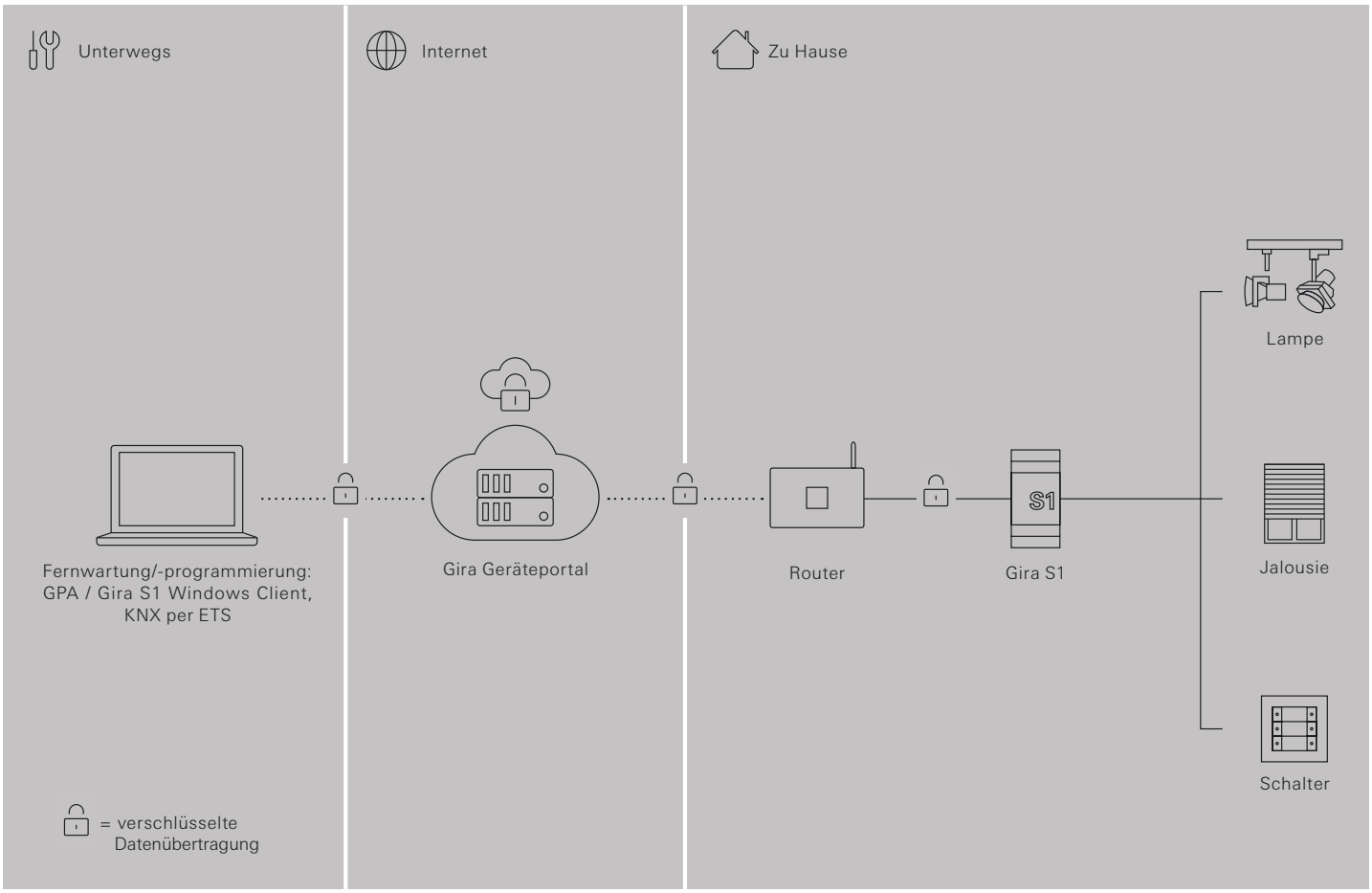


Bild 10: Sicherer Fernzugriff auf die KNX Installation mit dem Gira S1.

Nachdem mit dem Gira S1 Windows Client eine Verbindung zu einem bestimmten Gira S1 hergestellt wurde (siehe Kapitel 11.2 "Verbindung zum Gira Geräteportal herstellen"), erscheinen in der ETS die im entfernten Netzwerk vorhandenen KNX/IP Schnittstellen, so als wäre die ETS selbst im entfernten Netzwerk. Um Verwechslungen mit anderen Geräten im eigenen Netzwerk zu vermeiden, ist es möglich, einen Text dem normalerweise in der ETS angezeigten Gerätenamen voranzustellen. Außerdem ist es der Einfachheit halber auch möglich, nur die KNX/IP Schnittstelle des Gira S1 zur Verfügung zu stellen. Neben den KNX/IP Schnittstellen werden auch alle Geräte, die direkt über IP ladbar sind (siehe Kapitel "Übertragung beschleunigen: Übertragungsweg IP wählen"), der ETS bekannt gemacht, so dass auch diese beschleunigten Downloads über Fernzugriff funktionieren. Weitere Informationen hierzu siehe Kapitel 11.3 "Konfiguration der Zugriffsoptionen eines Gira S1".

3.4.1. Einschränkungen und Freigaben von Zugriffsrechten über KNX Kommunikationsobjekte

Wenn der Gira S1 in einem ETS Projekt eingefügt wird, können über dessen Kommunikationsobjekte auch zur Laufzeit über KNX Zugriffsmöglichkeiten verboten bzw. erlaubt werden. Die über den KNX in der entfernten Installation festgelegten Einschränkungen von Zugriffsrechten wiegen immer stärker als Festlegungen im Portal. So kann über Gruppentelegramme der Fernzugriff unabhängig von Einstellungen im Gira Geräteportal komplett deaktiviert werden.

3.5. Zugriff auf Webseiten im entfernten Netzwerk

Der Fernzugriff über den Gira S1 erlaubt den sicheren Zugriff auf Webseiten im entfernten Netzwerk. Hierfür werden die im entfernten Netzwerk unverschlüsselten (HTTP) Daten (siehe Bild 11) über eine verschlüsselte SSL/TLS Verbindung zum Gira Geräteportal transportiert und wiederum über eine HTTPS Verbindung zum Internet Browser.

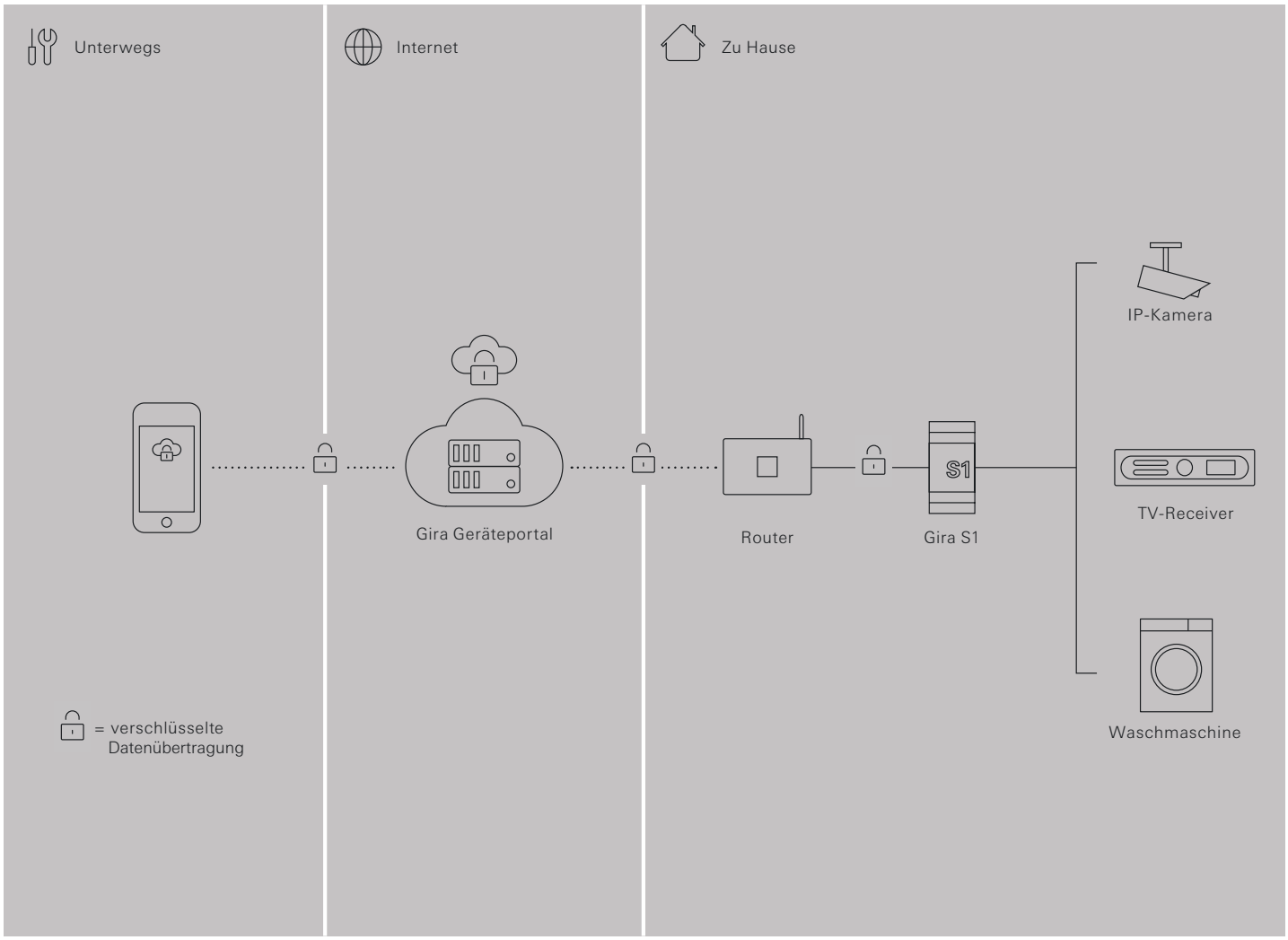


Bild 11: Sicherer Zugriff auf Webseiten über den Fernzugriff.

Der HTTP Zugriff auf Webseiten im entfernten Netzwerk ist am einfachsten über das Gira Geräteportal möglich. Hierbei ist ein Zugriff über das Gira Geräteportal schnell konfiguriert. Eine Beschreibung hierzu siehe Kapitel 10.4 "Links".

3.6. Zugriff über andere TCP Protokolle

Über den Gira S1 ist es grundsätzlich möglich, nahezu alle TCP basierten Protokolle sicher über das Internet zu benutzen.

Weit verbreitet ist u.a. das Remote Desktop Protokoll (RDP), welches Microsoft für den Fernzugriff auf Windows Rechner definiert hat. Zusammen mit dem Gira S1 Windows Client können Sie einfach den Zugriff konfigurieren. Weitere Informationen siehe Kapitel 11.3.3 "Nutzung weitere TCP Protokolle über Fernzugriff".

3.7. Benutzerrechte und Benutzergruppen

Unabhängig von der Art des Zugriffs (z. B. auf Webseiten, KNX, Gira HomeServer, Remotedesktopverbindung) können Zugriffsrechte für die vordefinierten Benutzergruppen „Bewohner“ und „Installateur“ pro Beziehung zwischen Gira S1 und Portalbenutzer konfiguriert werden und über KNX Kommunikationsobjekte dynamisch gesteuert werden.

Ein typisches Szenario nach der Schlüsselübergabe könnte so aussehen:

- Mit dem Gira S1 sind ein oder mehrere Portalbenutzer des Elektrohandwerkbetriebs/Systemintegrators in der Rolle des „Installateurs“ verbunden, z. B. für Wartungszwecke.
- Mit dem Gira S1 sind ein oder mehrere Portalbenutzer in der Rolle des „Bewohner“ verbunden, typischerweise alle Familienmitglieder, für Visualisierungen auf dem Smartphone und Webseitenzugriffe.
- Der Gira S1 wird in der ETS über die Parameter so konfiguriert, dass die Benutzer mit der Benutzergruppe „Bewohner“ grundsätzlich Zugriff haben; außerdem haben die Benutzer der Benutzergruppe „Installateur“ standardmäßig Zugriff.
- Wenn der Installateur zu einem Wartungstermin oder auf Grund eines Anrufs des Hausherrn auf die Anlage zugreifen will, meldet er sich beim Hausherrn. Dieser gibt ihm dann Zugriff, indem er über eine Option in seiner Visualisierung o. ä. über das entsprechende Kommunikationsobjekt den Zugriff freischaltet. Mit Einsatz einer Logik oder einer Zeitschaltuhr ist auch ein automatisches Abschalten des Zugriffs nach einer gewissen Zeit problemlos realisierbar.
- Für sicherheitssensible Bewohner ist es auch möglich, über einen Taster oder Visualisierung den Fernzugriff komplett zu deaktivieren. Der Gira S1 meldet sich dann gar nicht mehr beim Portal an, ein Fernzugriff ist unmöglich.
- Der Gira S1 signalisiert einen Verbindungsaufbau über Fernzugriff über KNX Kommunikationsobjekte, so dass eine entsprechende Verarbeitung in einer Visualisierung/Logik (z. B. E-Mail Information wenn sich jemand verbindet) einfach möglich ist.

Darüber hinaus kann der Zugriff von Software wie z. B. Visualisierungen über den Einsatz von Aktivierungscodes gesteuert werden. Von diesen kann jeder Benutzer an jedem Gira S1, auf den er Zugriff hat, beliebig viele Codes anlegen, z.B. für die Visualisierung (siehe Kapitel 10.7 "Applikationszugänge").

4. Zeitgeber

Als Zeitgeber kann der Gira S1 die aktuelle Uhrzeit in konfigurierbaren Intervallen auf den KNX Bus senden. Diese Funktion wird über die ETS eingerichtet. Aktivieren Sie in den ETS-Parametern des Gira S1 in der Ansicht „Allgemein“ den Parameter „Zeitgeber“, damit die Parameterseite „Zeitgeber“ sichtbar wird (siehe Kapitel 8.5 "Parameter").

Mit den Parametern „Uhrzeit senden“ und „Datum senden“ konfigurieren Sie das jeweils gewünschte Intervall. Die gesendete Zeit wird aus der Systemzeit bezogen. Diese wird mit einem über die Gerätewebseite konfigurierbaren NTP Server synchronisiert.

Über die Parameter „Uhrzeit senden“ (Kommunikationsobjekt 50) und „Datum senden“ (Kommunikationsobjekt 51) wird das Intervall für das Senden des Kommunikationsobjektes 52 „Datum und Uhrzeit“ festgelegt. Sofern sich die Parameterwerte unterscheiden, wird das kürzere Intervall verwendet.

Das Gerät kann für verschiedene UTC Zeitzonen konfiguriert werden. Der dafür verwendete Parameter „Zeitzone“ befindet sich in der Parameteransicht „Allgemein“.

Die Berücksichtigung der Zeitumstellungen erfolgt je nach eingestellter Zeitzone automatisch oder gar nicht. Um keine automatischen Zeitumstellungen vorzunehmen, muss eine „Generic Time Zone w/o DST“ parametriert werden.

Der Zeitgeber wird nur dann Datum und Uhrzeit aussenden, wenn seit dem Gerätestart mindestens eine erfolgreiche NTP Synchronisation durchgeführt wurde. Dies geschieht um zu verhindern, dass eine eventuell falsche Systemzeit versendet wird.

Bei der Funktion Zeitgeber wird ein Kommunikationsobjekt zur Verfügung gestellt, mit dem das Senden der Zeit/des Datums ausgelöst werden kann (Trigger). Genaueres siehe Kapitel 8.6 "Objekttabelle".

Bei der Auslieferung ist die Zeitgeberfunktion deaktiviert.

5. Datenlogger

Der Gira S1 kann als Datenlogger genutzt werden. Die Datenloggerfunktionalität wird über den Parameter „Datenlogger“ in der Parameteransicht „Allgemein“ gesteuert (siehe Kapitel 8.5 "Parameter"). Ist er auf „Ja“ eingestellt, ist die Datenloggerfunktionalität grundsätzlich aktiviert. Wird eine microSD-Karte in das Gerät gesteckt oder befindet sich bereits eine microSD-Karte im Gerät, so startet das Loggen automatisch, sofern es nicht über das Kommunikationsobjekt „Aktiviere Datenlogger“ deaktiviert ist.

Der Datenlogger-Zustand wird über das Kommunikationsobjekt „Datenlogger Status“ gesendet. Der Datenlogger-Zustand kann aber auch direkt abgefragt werden. Solange der Datenlogger aktiv ist, hat das Kommunikationsobjekt den Wert 1. Das Kommunikationsobjekt „Datenlogger Status“ übernimmt den Wert 0 und sendet diesen, wenn:

- die microSD-Karte entfernt wird,
- kein Speicherplatz auf der microSD-Karte vorhanden ist oder
- der Datenlogger über das Kommunikationsobjekt „Aktiviere Datenlogger“ deaktiviert wurde.

Der Datenlogger unterstützt zwei Arten der Speicherverwaltung. Der microSD-Kartenspeicher kann als Festspeicher oder als Ringspeicher verwendet werden.

Bei der Verwendung als Ringspeicher wird der verbleibende Speicher überwacht. Beim Unterschreiten einer Restspeichermenge von 2,5 Mbyte wird die älteste Logdatei gelöscht, um Platz für neue Daten zu schaffen. Bei der Verwendung als Festspeicher wird, sobald die microSD-Karte voll ist, das Loggen automatisch beendet, bis eine microSD-Karte mit ausreichend Platz eingelegt wird.

Über den Parameter „Datenloggingformat“ in derselben Parameteransicht kann konfiguriert werden, ob ein ETS 3 (.trx) oder ETS 4/ETS 5 (.xml) konformes Dateiformat verwendet werden soll. Der Datenlogger kann über das Kommunikationsobjekt „Aktiviere Datenlogger“ aktiviert und deaktiviert werden.

Die Benennung und Ablage der Logdateien auf der microSD-Karte erfolgt nach folgendem Schema:
2010_01_06_TP1.trx (Jahr_Monat_Tag)

Sollte es zu einem Spannungsverlust und einem daraus resultierenden Zeit-/Datumsverlust kommen, könnte sich ein Dateiname wiederholen. In diesem Fall wird eine Tilde (~) an das Ende des Dateinamens gehängt, bei weiteren Wiederholungen eine Tilde mit fortlaufender Nummer (~1).

Der Gira S1 unterstützt SDHC-Karten bis maximal 32 GByte. Die Karten müssen mit FAT32 formatiert werden.

Hinweis

Um eine Beschädigung der microSD-Karte zu vermeiden, deaktivieren Sie vor der Entnahme der microSD-Karte das Loggen.

Zur Überwachung des Speicherstatus stehen verschiedene Kommunikationsobjekte zur Verfügung. Über diese Kommunikationsobjekte kann der aktuelle Kartenstatus und der Füllstand abgefragt werden. Genaueres siehe Kapitel 8.6 "Objekttabelle".

Wichtiger Hinweis: Ist der NTP-Server nicht erreichbar, wird bei Spannungsausfall eine Default-Zeit eingesetzt. Das weitere Loggen erfolgt auf Basis dieser Zeit, bis der NTP-Server wieder verfügbar ist.

5.1. Zugriff auf das Datenlogger-Archiv

Über die Gerätewebseite kann auf das Datenlogger Archiv zugegriffen werden. Der Menüpunkt ist auch bei deaktiviertem Datenlogger vorhanden, um ggf. alte Dateien herunterzuladen. Neben den gespeicherten Dateien wird auch der Status der microSD-Karte angezeigt.

Bei eingelegter microSD-Karte werden unter dem Punkt „Inhalt“ die auf der microSD-Karte gespeicherten Logdateien aufgelistet. Diese sind nach Jahr und Monat gruppiert. Standardmäßig sind die Jahre und Monate minimiert und können durch das Pluszeichen neben dem Jahr/Monat erweitert werden.

Bild 12: Datenlogger-Archiv

Die Dateigröße in Byte(s) wird jeweils neben einem Monat, bzw. einer einzelnen Datei angezeigt. Den Download einer xml-Datei starten Sie mit einem Klick auf das nebenstehende Downloadsymbol.

6. VPN

Um per VPN auf Ihr Heimnetzwerk zugreifen zu können, benötigen Sie einen OpenVPN-Client.

Laden Sie unter https://openvpn.net/community-downloads/ die Software OpenVPN herunter und installieren Sie diese auf Ihrem PC. Die Kompatibilität der Version 2.5.0 mit der VPN-Funktion des Gira S1 wurde sichergestellt.

Beabsichtigen Sie VPN auf Ihrem Smartphone zu nutzen, laden Sie die App „OpenVPN Connect“ aus dem Apple App Store bzw. dem Google Play Store herunter und installieren Sie sie auf Ihrem Smartphone.

6.1. Voraussetzung für die VPN-Einrichtung

- Unter https://geraeteportal.gira.de wurde ein Benutzerkonto angelegt.
- Der Gira S1 ist mit dem Internet verbunden.
- Der Gira S1 ist im Gira Geräteportal registriert.
- Eine veröffentlichte Version (released) des OpenVPN-Clients wurde heruntergeladen und auf dem PC oder Smartphone installiert.

6.2. VPN-Einrichtung

1. Melden Sie sich im Gira Geräteportal an.
2. Klicken Sie in der Funktionsübersicht auf „VPN-Zugang“.
3. Klicken Sie auf die Schaltfläche „VPN-Zugang einrichten“.
4. Warten Sie, bis die Konfigurationsdatei erstellt wurde und laden Sie die Datei herunter.
5. Öffnen Sie den OpenVPN-Client und importieren Sie die Konfigurationsdatei.
6. Aktivieren Sie im OpenVPN-Client die VPN-Verbindung.

Möchten Sie den VPN-Zugang für mehrere Benutzer anlegen, benötigt jeder dieser Benutzer ein eigenes Benutzerkonto im Gira Geräteportal. Die Schritte 4 bis 6 sind für jeden Benutzer zu wiederholen.

Hinweis

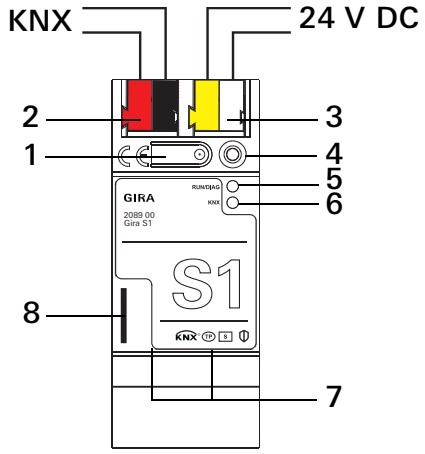
Testen Sie zunächst, ob die vorgenommene Konfiguration funktioniert, bevor Sie den VPN-Zugang für weitere Benutzer einrichten.

7. Montage

Sicherheitshinweis

Anschluss und Montage elektrischer Geräte dürfen nur durch Elektrofachkräfte erfolgen.
Bei Nichtbeachtung der Anleitung können Schäden am Gerät, Brand oder andere Gefahren entstehen.

7.1. Geräteaufbau



1. Programmier-Taste
2. Anschluss KNX
3. Anschluss Externe Spannungsversorgung
4. Programmier-LED (rot):
   ein = Programmiermodus aktiv
5. Betriebs-LED (grün):
   ein = Gira S1 betriebsbereit
   blinkt langsam = Gira S1 noch nicht bzw. falsch parametriert
   blinkt schnell = Interner Gerätefehler
6. KNX LED (gelb)
   ein = Verbindung zum KNX System
   aus = keine Verbindung zum KNX System
   blinkt = KNX Datenübertragung
7. Netzwerkanschluss mit LED (grün/orange)
   grün ein = Datenübertragungsrate 100 Mbit/s
   grün aus = Datenübertragungsrate 10 Mbit/s
   orange ein = Verbindung zum IP-Netz
   orange blinkt = keine Verbindung zum IP-Netz, kein Datenempfang vom IP-Netz
8. microSD-Karte (bis 32 GB (SDHC))
   Fromatierung: FAT32
   Damit der Datenlogger Telegramme aufzeichnen kann, muss eine microSD-Karte eingelegt werden.

7.2. Montage und elektrischer Anschluss

Gefahr

Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung.
Elektrischer Schlag kann zum Tod führen.
Vor Arbeiten am Gerät freischalten und spannungsführende Teile in der Umgebung abdecken!

7.2.1. Gerät montieren

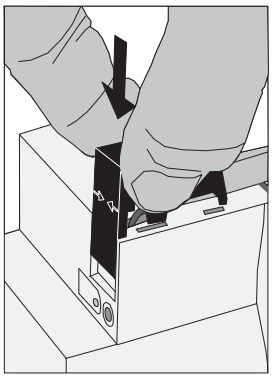
Temperaturbereich beachten. Für ausreichende Kühlung sorgen.

- Das Gerät auf Hutschiene nach DIN EN 60715 aufschnappen. Einbaulage siehe Bild 1.
- Externe Spannungsversorgung an Anschlussklemme (3) anschließen.
  Empfehlung: weiß-gelbe Anschlussklemme verwenden.
- KNX Linie mit rot-schwarzer Busklemme (2) anschließen.
- Abdeckkappe über den Anschluss KNX/Externe Spannungsversorgung stecken.
- Netzwerkanschluss mit RJ45-Stecker an RJ-Buchse (7) anschließen.

7.2.2. Abdeckkappe aufstecken

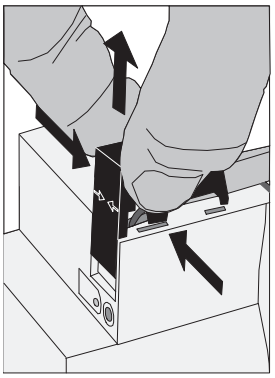
Um den Busanschluss vor gefährlichen Spannungen im Anschlussbereich zu schützen, muss eine Abdeckkappe aufgesteckt werden.

- Busleitung nach hinten führen.
- Abdeckkappe über die Busklemme stecken, bis sie einrastet.



7.2.3. Abdeckkappe entfernen

- Abdeckkappe seitlich drücken und abziehen.



8. Projektierung in der ETS

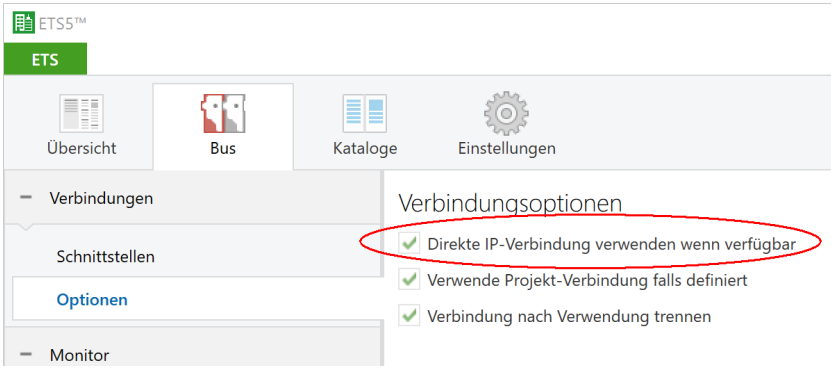
Die Projektierung des Gira S1 in der ETS gliedert sich in folgende Schritte:

1. Gira S1 als Gerät in der ETS anlegen (Kapitel 8.1).
2. Physikalische Adresse des Geräts sowie die bis zu drei physikalischen Adressen des Interfaces zuordnen (Kapitel 8.2).
3. IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse des Gira S1 einstellen oder die Auswahl „IP-Adresse automatisch (von einem DHCP-Server) beziehen“ treffen (Kapitel 8.3).
4. Allgemeine Parameter inklusive ggf. DNS Server zum Gira S1 einstellen (Parameter, siehe Kapitel 8.5)
5. Gruppenadressen an Kommunikationsobjekte anbinden (Objekttabelle, siehe Kapitel 8.6).
6. Physikalische Adressen programmieren (Kapitel 8.3.1).
7. Applikationsprogramm und Projektierung übertragen (Kapitel 8.4).

Übertragung beschleunigen: Übertragungsweg IP wählen

Die Programmierung (Übertragung von der ETS zum Gerät) erfolgt in der ETS. Für die Übertragung wird keine zusätzliche KNX Datenschnittstelle benötigt (Busanschluss via Busanschlussklemme). Die ETS kann das Gerät sowohl über die IP- als auch über die KNX TP-Seite erreichen.

Wegen deutlich kürzerer Übertragungszeiten wird der Download über die IP-Seite des Geräts empfohlen.
Diese Option können Sie auf der ETS-Startseite in der Ansicht „Bus“ - „Verbindungen“ - „Optionen“ auswählen:
Für die Übertragung der ETS über die IP-Seite wählen Sie die Einstellung „Direkte KNX-IP-Verbindung verwenden wenn verfügbar“.



8.1. Gira S1 als Gerät in der ETS anlegen

Wenn noch nicht geschehen, importieren Sie die ETS-Geräteapplikation zum Gira S1 einmalig in den Gerätekatalog ihrer ETS.
Die ETS-Applikation können Sie unter www.downloads.gira.de kostenlos herunterladen.

Produktkatalog
Produktname: Gira S1
Bauform: REG (Reiheneinbau)
Best.-Nr.: 2089 00

Auslieferungszustand

Der Gira S1 ist im Auslieferungszustand bzw. nach einem Werksreset, bevor er das erste Mal mit einer ETS geladen wird, folgendermaßen konfiguriert:

- Der Fernzugriff ist für die Benutzergruppe „Bewohner“ aktiviert
- Die physikalische Adresse ist 15.15.255, die drei zusätzlichen physikalischen Adressen für den Tunneling Server haben alle die Adresse 15.15.254.

Sollten Sie bereits ein ETS-Projekt mit einem vorherigen Datenbankeintrag haben, so können Sie auch das Applikationsprogramm aktualisieren. Dazu ziehen Sie den neuen Datenbankeintrag in das Projekt und wählen danach das Gerät mit dem alten Datenbankeintrag an. Nun wählen Sie unter den „Eigenschaften“ des Geräts „Information“ aus und dort den Reiter „Applikation“ (ETS4.2) bzw. „Applikationsprogramm“ (ETS5). Dort können Sie nun mit der Schaltfläche „Applikationsprogramm aktualisieren“ (ETS4.2) bzw. „Aktualisieren“ (ETS5) den alten Datenbankeintrag ersetzen. Hierbei gehen bestehende Verknüpfungen mit Gruppenadressen nicht verloren. Das neu hinzugefügte Gerät kann nun wieder gelöscht werden. In der ETS4.2 benötigen Sie hierfür eine spezielle Lizenz, ab der ETS5 ist dies mit jeder Lizenz möglich.

Hinweis: „Applikationsprogramm ändern“ nicht nutzen

Bitte nutzen Sie **nicht** das Dropdown-Menü „Applikationsprogramm ändern“, da bei der Benutzung dieser Funktion die komplette Konfiguration des Gira S1 verloren geht.

8.2. Physikalische Adressen zuordnen

Der Gira S1 verfügt über drei Tunneling Server (KNX/IP Interfaces). Diese Interfaces können für den Download als auch im Gruppen- und Busmonitor-Modus genutzt werden. Neben der physikalischen Adresse des Geräts besitzt das Gerät daher noch (bis zu) drei weitere physikalische Schnittstellen. Diese können wie bei vielen Produkten heute üblich nach Öffnen der KNX/IP Verbindung in der ETS über die Einstellungen der Schnittstelle konfiguriert werden. In diesem Fall muss man selbst genau darauf achten, dass die Adressen nicht bereits anderweitig benutzt sind.
Ab der ETS4 ist es möglich, bei Produkten die Anzahl der zusätzlichen Adressen anzugeben, so dass diese in der ETS konfigurierbar sind. Hierzu erscheint unter dem Eingabefenster für die physikalische Adresse bei den Geräteeigenschaften in der ETS eine Liste mit den zusätzlichen Adressen. In diesem Fall stellt die ETS die Eindeutigkeit der Adressen im Projekt sicher und lädt drei Adressen beim Programmieren der physikalischen Adresse automatisch mit in das Gerät.
Wenn Sie nicht alle drei Schnittstellen benötigen, können Sie über die „Parken“ Funktion auch Adressen freigeben. Beim Einfügen eines Geräts besetzt die ETS in der Regel die zusätzlichen Adressen automatisch vor.

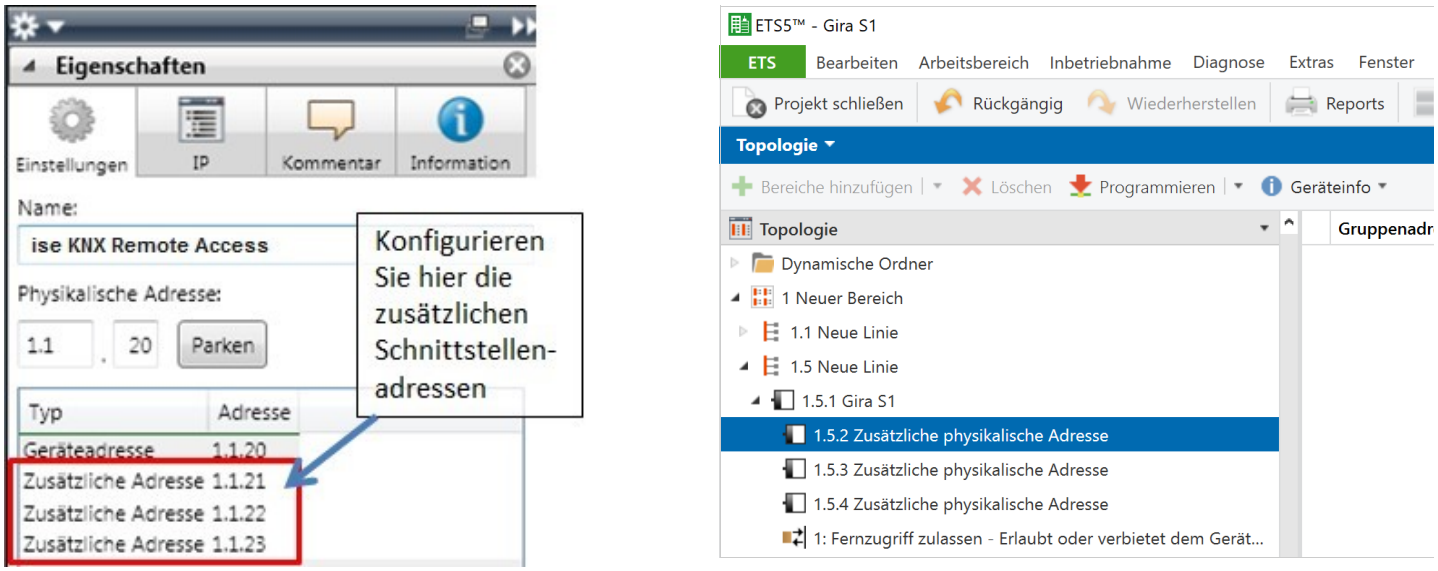


Bild 13: Zusätzliche physikalischen Adressen in der ETS4 (links) und der ETS5 (rechts)

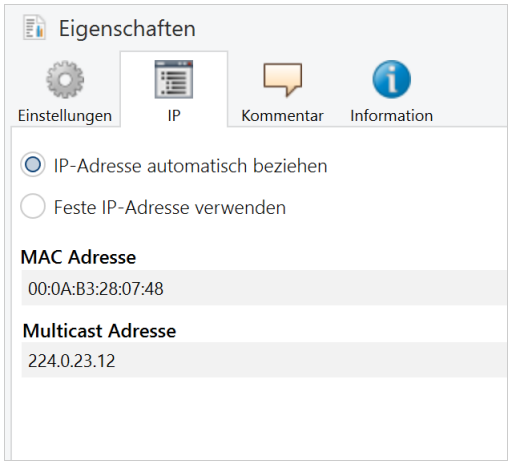
8.3. IP-Adresse, Subnetzmaske und Adresse des Standardgateways einstellen

Neben der physikalischen Adresse im KNX Netzwerk muss dem Gira S1 eine Adressierung im IP-Datennetzwerk zugewiesen werden. Dazu gehören folgende Informationen:

- IP-Adresse
- Subnetz-Maske
- Adresse des Standardgateways
- DNS Server

Gehen Sie wie folgt vor:

1. Wählen Sie den Gira S1 in der ETS aus.
2. Zeigen Sie die Eigenschaften des Gira S1 in der Eigenschaftsspalte der ETS an.
3. Wählen Sie den Reiter „IP“.
   Wählen Sie nun entweder
   - „IP-Adresse automatisch beziehen“ (Standard)
     Die Adressdaten werden automatisch von einem DHCP-Server im Datennetzwerk bezogen.



oder

- „Folgende IP-Adresse verwenden“
  und tragen Sie die Daten manuell ein.
  Den zulässigen IP-Adressbereich, sowie Subnetzmaske und Standardgateway können Sie üblicherweise der Oberfläche der Router Konfiguration entnehmen.

Wichtig: Wenn das Gerät nicht mit DHCP genutzt wird, muss in den Parametern des Geräts der DNS Eintrag korrekt gesetzt werden (siehe Kapitel 8.5 "Parameter")!

Bei der Einstellung „IP-Adresse automatisch beziehen“ muss ein DHCP-Server dem Gira S1 eine gültige IP-Adresse zuteilen. Steht bei dieser Einstellung kein DHCP-Server zur Verfügung, so startet das Gerät nach einer Wartezeit mit einer Auto IP-Adresse (Adressbereich von 169.254.1.0 bis 169.254.254.255). Sobald ein DHCP Server zur Verfügung steht, wird dem Gerät automatisch eine neue IP-Adresse zugewiesen.

8.3.1. Physikalische Adresse des Geräts programmieren

1. Stellen Sie sicher, dass Gerät und Busspannung eingeschaltet sind.
2. Sellen Sie sicher, dass die Programmier-LED (4) nicht leuchtet.
3. Programmiertaste (1) kurz drücken – Programmier-LED (4) leuchtet rot.
4. Physikalische Adresse mit Hilfe der ETS programmieren.

Nach einem erfolgreichen Programmier-Vorgang

- erlischt die LED (4).
- zeigt die ETS die abgeschlossene Übertragung mit grüner Markierung unter Historie in der Eigenschaftsspalte (normalerweise am rechten Fensterrand) an.
- setzt die ETS die Inbetriebnahme-Häkchen am Gerät für „Adr“ und „Cfg“.

Nun können Sie die physikalische Adresse auf dem Gerät notieren.

Hinweis

Die zusätzlichen Adressen des Tunneling Servers, den der Gira S1 mitbringt und der bis zu drei Verbindungen unterstützt, werden ebenfalls über die ETS bei den Eigenschaften des Geräts konfiguriert.

8.4. Applikationsprogramme und Projektierungsdaten übertragen

Im Anschluss an die Programmierung der physikalischen Adresse können Applikationsprogramm, Parameter-Einstellungen und Gruppenadress-Anbindungen in das Gerät übertragen werden. Die Verbindung zum Gerät kann dafür weiter über IP oder über KNX erfolgen.

- Wählen Sie dazu „Programmieren Applikationsprogramm“. Der Download dauert ca. 15 Sekunden bei einer IP-Direktverbindung bzw. ca. 2 Minuten bei der Nutzung von TP.
- Nach dem Download bitte ca. 15 Sekunden warten, während das Gerät die Daten übernimmt und die Applikation initialisiert.
- Die Inbetriebnahme ist abgeschlossen.

8.5. Parameter

Der Standardwert jedes Parameters ist **fett** markiert.

8.5.1. Allgemein

Parameter	Eintrag / Auswahl	Bemerkungen
DNS Server (falls kein DHCP)	**Standard Gateway**	Die IP-Adresse des Standardgateways wird verwendet (siehe Kapitel 8.3 "IP-Adresse, Subnetzmaske und Adresse des Standardgateways einstellen").
	Individuelle DNS-Server IP-Adresse	Mit diesem Parameter entsteht die Möglichkeit, eine individuelle IP-Adresse des DNS-Servers einzurichten.
	0.0.0.0	Die individuelle DNS Server IP-Adresse. Bei Verwendung von 0.0.0.0 wird das Default Gateway verwendet.
VPN-Zugriff über KNX steuern	**Nein** Ja	Dieser Parameter stellt bei Aktivierung die Kommunikationsobjekte für den VPN-Zugriff und dessen Status zur Verfügung.
Zeitgeber	**Nein** Ja	Das Gerät arbeitet als Zeitgeber und sendet in konfigurierbaren Intervallen die aktuelle Zeit und das Datum auf den KNX Bus.
Datenlogger	**Nein** Ja	Dieser Parameter legt fest, ob die Datenloggerfunktion aktiviert ist. Nur wenn sie aktiviert ist, stehen die entsprechenden Kommunikationsobjekte zur Verfügung.
Zeitzone	**(UTC+01:00) Europe/ Berlin** Weitere UTC Zeitzonen	Hier wird die zu benutzende Zeitzone ausgewählt. Es existieren mehrere Zeitzonen mit identischen UTC Abweichungen. In einigen dieser Zeitzonen erfolgt die Sommer-/Winterzeitumstellung zu einem anderen Zeitpunkt. Damit keine automatische Zeitumstellung erfolgt, muss eine der „Generic Time Zone w/o DST“ Zeitzonen ausgewählt werden. Hinweis: Wird diese Einstellung geändert, erfolgt nach der Programmierung der Applikation ein sofortiger Neustart des Gira S1. Hinweis: Die Option NTP über die Gerätewebseite zu deaktivieren, wurde ab Firmware-Version 5.0 entfernt. Wenn Sie NTP deaktiviert haben, wird als Standard-NTP-Server automatisch ein NTP-Server von ntp.org verwendet.

Parameter	Eintrag / Auswahl	Bemerkungen
Fernzugriff generell nach Neustart	**wie vor Neustart**	Der generelle Fernzugriffstatus wird nach einem Neustart auf den letzten bekannten Wert vorm Neustart eingestellt, ist z.B. der generelle Fernzugriffstatus vor Neustart aktiviert, wird der Fernzugriffstatus nach Neustart auch aktiviert.
	aktiviert	Erlaubt dem Gerät eine Verbindung zum Portalserver aufzubauen nach jedem Neustart.
	deaktiviert	Verbietet dem Gerät eine Verbindung zum Portalserver aufzubauen nach jedem Neustart.
Fernzugriff für die Gruppe „Bewohner“, oder die Gruppe „Installateure“ nach Neustart	**wie vor Neustart**	Der Fernzugriffstatus der jeweiligen Gruppe wird nach einem Neustart auf den letzten bekannten Wert vorm Neustart eingestellt, ist z.B. der Fernzugriffstatus vor Neustart aktiviert, wird der Fernzugriffstatus nach Neustart auch aktiviert.
	aktiviert	Erlaubt den Fernzugriff für die jeweilige Gruppe nach jedem Neustart.
	deaktiviert	Verbietet den Fernzugriff für die jeweilige Gruppe bei jedem Neustart.
Anzahl der Benachrichtigungsobjekte	**0**...50	Hier wird die Anzahl der Benachrichtigungsobjekte festgelegt (max. 50). Entsprechend der Auswahl werden die Kommunikationsobjekte „101 ff.“ sichtbar.
Trennzeichen für Fließkommazahlen	. ,	

8.5.2. Zeitgeber

Die Parameterseite „Zeitgeber“ ist nur sichtbar, wenn der Zeitgeber auf der Parameterseite Allgemein aktiviert ist.

Parameter	Eintrag / Auswahl	Bemerkungen
Uhrzeit senden	**Jede Minute** Jede Stunde Jeden Tag	Mit diesem Parameter wird das Intervall konfiguriert, im dem die Uhrzeit auf den Bus gesendet wird.
Datum senden	**Jede Minute** Jede Stunde Jeden Tag	Mit diesem Parameter wird das Intervall konfiguriert, im dem das Datum auf den Bus gesendet wird.

8.5.3. Datenlogger

Die Parameterseite „Datenlogger“ ist nur sichtbar, wenn der Datenlogger auf der Parameterseite Allgemein aktiviert ist.

Parameter	Eintrag / Auswahl	Bemerkungen
Format		Dieser Parameter legt fest, in welchem Format die Daten auf die microSD-Karte geloggt werden sollen.
	ETS4/ETS5	Die Daten werden in einem ETS 4-konformen Format abgelegt (.xml), welches mit der ETS 5 ebenfalls lesbar ist.
	ETS3	Die Daten werden in einem ETS 3-konformen Format abgelegt (.trx).
Speichertyp	Ringspeicher **Festspeicher**	Dieser Parameter legt fest, wie der microSD-Kartenspeicher verwendet werden soll.
Speicherstatustyp		Nur sichtbar, wenn „Speichertyp“ auf „Festspeicher“ eingestellt ist. Dieser Parameter legt fest, welchen Typ das Statusobjekt des Kartenfüllstands entsprechen soll.
	Binär	Es wird ein 1 Bit Objekt verwendet. Der Wert „1“ bedeutet, dass die microSD-Karte voll ist, eine „0“ bedeutet, dass auf der microSD-Karte noch Platz zum Loggen ist.
	Wert (0-255)	Es wird ein 1 Byte Objekt verwendet. Der Wertebereich liegt zwischen 0 – 255. Dabei entspricht der Wert „255“ einem Kartenfüllstand von 100%.

8.5.4. Benachrichtigungen

Entsprechend der oben gewählten Anzahl der Benachrichtigungen können nun die DP-Typen und weitere Parameter der jeweiligen Benachrichtigung (Benachrichtigung Nr. 1 = Kommunikationsobjekt 101, Benachrichtigung Nr. 2 = Kommunikationsobjekt 102…) festgelegt werden.

Parameter	Eintrag / Auswahl	Bemerkungen
Datentyp	**Bool (1 Bit, DPT 1.001)** Prozent (1 Byte, DPT 5.001) Zähler (1 Byte, DPT 5.010) Fließkomma (2 Byte, DPT 9.*) Text (14 Byte, DPT 16.001)	Der gewünschte Datentyp der jeweiligen Benachrichtigung kann ausgewählt werden.
Benachrichtigung nur bei Wertänderung	Checkbox **(inaktiv)**	

Parameter	Eintrag / Auswahl	Bemerkungen
Schwellwert	0-1000 Angabe als Ganzzahl	Benachrichtigungen unterdrücken. Erst wieder eine Benachrichtigung senden, wenn der Schwellwert überschritten wird. Der Schwellwert ist die Abweichung vom letzten Wert (als absolute Zahl), der eine Benachrichtigung erzeugt hat. 0: Kein Schwellwert. Sie erhalten bei jeder Änderung eine Benachrichtigung.
Schwellwert Basis	Wert gemäß Auswahlliste	Faktor mit dem der Schwellwert bei Bedarf multipliziert wird. 1: Kein Faktor.
Filter	**Benachrichtigung immer erzeugen** Benachrichtigung nur für 1 (true) erzeugen Benachrichtigung nur für 0 (false) erzeugen	Beim Datentyp Bool (DPT 1.001) ist der Filter über eine Auswahlliste möglich.
	Text	Bei allen anderen Datentypen kann der Filter aus einem festen Wert oder bis zu zwei Bedingungen bestehen. Beschreibung siehe Parameterdialog.
Priorität	**Niedrig** Hoch Alarm	
Kategorie	Text	Kann zum Filtern der Benachrichtigungen und deren Weiterleitungen auf dem Portal genutzt werden.
Betreff	Text	Beschreibung siehe Parameterdialog. Wird beim Versand von E-Mails als „Betreff“ genutzt.
Text	Text	Beschreibung siehe Parameterdialog. Wird beim Versand von E-Mails als „Text“ genutzt.
Anhang hinzufügen	Checkbox **(inaktiv)**	
URL des Anhangs	Text	Nur http Anfragen werden unterstützt. Beachten Sie die maximal zulässige Dateigröße von 250 kByte.

8.6. Objekttabelle

Hinweis für alle Kommunikationsobjekte, die eine laufende Verbindung signalisieren

Bei der Nutzung des HTTP Zugriffs, also ohne Gira S1 Windows Client, wird die Verbindung zum Gerät (wenn sie gestattet war) nicht sofort nach Laden der Seiten bzw. Schließen des Browsers beendet. Dies hängt mit einer technischen Optimierung des HTTP Zugriffs im Gira Geräteportal zusammen. HTTP Verbindungen können bis zu fünf Minuten benötigen, bis sie geschlossen werden. Das heißt, dass die entsprechenden Kommunikationsobjekte, die eine aktive Verbindung signalisieren, das Schließen auch erst zu diesem Zeitpunkt signalisieren. Bei der Nutzung des Gira S1 Windows Clients hingegen erfolgt der Verbindungsabbau synchron.

Am Gira S1 stehen die folgenden Kommunikationsobjekte zur Anbindung von Gruppenadressen bereit:

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
1	Portalzugriff zulassen	Schreiben	1 Bit	1.003	K-S--
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Erlaubt oder verbietet dem Gerät, eine Verbindung zum Portalserver aufzubauen. Ist der Verbindungsaufbau verboten, so ist das Gerät niemals von außen zu erreichen.				
Beschreibung:	1 = Erlauben, 0= Verbieten				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
2	Portalzugriff zulassen – Status	Lesen	1 Bit	1.003	KL-Ü-
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Zeigt an, ob das Gerät eine Verbindung zum Portalserver aufbauen darf.				
Beschreibung:	1 = Erlaubt, 0= Verboten				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
3 (Bewohner) 5 (Installateur)	Fernzugriff zulassen	Schreiben	1 Bit	1.003	K-S--
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Erlaubt oder verbietet den Fernzugriff jeweils für Mitglieder der Gruppe				
Beschreibung:	1 = Erlauben, 0= Verbieten				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
4 (Bewohner) 6 (Installateur)	Fernzugriff zulassen – Status	Lesen	1 Bit	1.003	KL-Ü-
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Zeigt an, ob Fernzugriff für jeweils für Mitglieder der Gruppe zugelassen ist.				
Beschreibung:	1 = Erlaubt, 0= Verboten				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
9	VPN-Zugriff zulassen	Schreiben	1 Bit	1.003	K-S--
Rubrik:	VPN-Zugriff	Datentyp:	Freigeben		
Funktion:	Aktiviert oder deaktiviert den VPN-Zugriff aller Benutzer, für die VPN im Gira Geräteportal freigeben wurde.				
Beschreibung:	1=Aktivieren, 0=Deaktivieren				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
10	VPN-Zugriff zulassen - Status	Lesen	1 Bit	1.011	KL-Ü--
Rubrik:	VPN-Zugriff	Datentyp:	Status		
Funktion:	Zeigt an, ob VPN-Zugriff zugelassen ist.				
Beschreibung:	1=Erlaubt, 0=Nicht erlaubt				

20	Portalverbindung - Status	Lesen	1 Bit	1.011	KL-Ü-
Rubrik:	Fernzugriff	Datentyp:	Status		
Funktion:	Zeigt an, ob eine Portalverbindung aufgebaut ist. Genauere Informationen stellt Kommunikationsobjekt 31 zu Verfügung.				
Beschreibung:	1 = Verbunden, 0= Getrennt				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
21	Fernzugriffsverbindung - Status	Lesen	1 Bit	1.011	KL-Ü-
Rubrik:	Fernzugriffsverbindung	Datentyp:	Status		
Funktion:	Zeigt an, ob mindestens eine Fernzugriffsverbindung, unabhängig von der Art der Verbindung, derzeit aktiv ist.				
Beschreibung:	1 = Aktiv, 0= Nicht aktiv				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
22 (Bewohner) 23 (Installateur)	Fernzugriffsverbindung - Status	Lesen	1 Bit	1.011	KL-Ü-
Rubrik:	Fernzugriffsverbindung	Datentyp:	Status		
Funktion:	Zeigt an, ob eine Fernzugriffsverbindung jeweils für die Gruppe derzeit aktiv ist. Eine aktive Verbindung wird ggf. auch für eine andere Gruppe signalisiert, wenn einem Mitglied dieser Gruppe aufgrund der Mitgliedschaft in einer anderen Gruppe der Zugriff gestattet wurde.				
Beschreibung:	1 = Aktiv, 0= Nicht aktiv				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
25	VPN-Zugriff - Status	Lesen	1 Bit	1.011	KL-Ü-
Rubrik:	VPN-Zugriff	Datentyp:	Status		
Funktion:	Zeigt an, ob derzeit eine aktive VPN-Verbindung besteht.				
Beschreibung:	1 = Aktiv, 0= Nicht aktiv				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
30	Fehleranzeige	Lesen	1 Bit	1.005	KL-Ü-

Rubrik:	Verbindungsfehler	Datentyp:	Alarm
Funktion:	Zeigt einen Verbindungsfehler an, der durch Kommunikationsobjekt 32 beschrieben wird. Weitere Details auf der Gerätewebseite des Gira S1.		
Beschreibung:	1 = Alarm, 0= Kein Alarm		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
31	Info Portalverbindung	Lesen	14 Byte	16.001	KL-Ü-

Rubrik:	Verbindungsfehler	Datentyp:	Zeichen (ISO 8859-1)
Funktion:	Diagnoseinformationen zur Portalverbindung		
Beschreibung:	Liefert genauere Informationen zum Portalverbindungsstatus, der durch Kommunikationsobjekt 20 angezeigt wird.		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
32	Info Verbindungsfehler	Lesen	14 Byte	16.001	KL-Ü-

Rubrik:	Verbindungsfehler	Datentyp:	Zeichen (ISO 8859-1)
Funktion:	Zusätzliche Diagnoseinformation im Falle eines Fehlers der Portalverbindung.		
Beschreibung:	Liefert genauere Informationen zum Verbindungsfehler, der durch Kommunikationsobjekt 30 angezeigt wird.		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
50	Uhrzeit	Lesen	3 Byte	10.001	KL-Ü-

Rubrik:	Zeitgeber	Datentyp:	Tageszeit
Funktion:	Sendet zyklisch und auf Anfrage die aktuelle Uhrzeit.		
Beschreibung:	3 Byte Objekt zum Senden der aktuellen Uhrzeit. Das Intervall ist parametrierbar (siehe Kapitel 8.5.2 "Zeitgeber"). Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie die derzeitige Systemzeit, die von der korrekten Zeit abweichen kann.		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
51	Datum	Lesen	3 Byte	11.001	KL-Ü-

Rubrik:	Zeitgeber	Datentyp:	Datum
Funktion:	Sendet zyklisch und auf Anfrage das aktuelle Datum.		
Beschreibung:	3 Byte Objekt zum Senden des aktuellen Datums. Das Intervall ist parametrierbar (siehe Kapitel 8.5.2 "Zeitgeber"). Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie das derzeitige Systemdatum, das vom korrekten Datum abweichen kann.		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
52	Datum und Uhrzeit	Lesen	8 Byte	19.001	KL-Ü-
Rubrik:	Zeitgeber	Datentyp:	Datum/Zeit		
Funktion:	Sendet zyklisch und auf Anfrage aktuelles Datum und Uhrzeit.				
Beschreibung:	8 Byte Objekt zum Senden des aktuellen Datums und Uhrzeit. Das Intervall wird aus dem geringeren Intervall der Parametern für die Kommunikationsobjekte 50 „Uhrzeit“ und 51 „Datum“ bestimmt (siehe Kapitel 8.5.2 "Zeitgeber"). Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie die derzeitige Systemzeit und -datum, welche vom der korrekten Zeit und Datum abweichen können.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
53	Auslöser Datum/Uhrzeit senden	Schreiben	1 Bit	1.007	K-S--
Rubrik:	Zeitgeber	Datentyp:	Auslöser		
Funktion:	Löst das Senden von Datum und Uhrzeit aus.				
Beschreibung:	1 Bit Objekt zum Auslösen des Sendens der aktuellen Zeit/Datum, wenn dem Objekt ein beliebiger Wert zugewiesen wird. Wenn noch keine NTP Abfrage erfolgreich war, werden keine Werte gesendet.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
54	NTP-Abfrage - Status	Lesen	1 Bit	1.002	KL-Ü-
Rubrik:	Zeitgeber	Datentyp:	Boolesch		
Funktion:	Zeigt an, ob eine gültige Uhrzeit vom NTP-Server abgefragt werden konnte.				
Beschreibung:	1 Bit Objekt zur Anzeige des Status der letzten NTP Abfrage. Wenn die NTP Abfrage erfolgreich war und die Systemzeit daraufhin neu gestellt wurde oder es bei der vorherigen Abfrage einen Fehler gab, wird dem Objekt eine „1“ zugewiesen. Wenn die letzte NTP Abfrage nicht erfolgreich war, wird dem Objekt eine „0“ zugewiesen.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
55	SD-Kartenfehler	Lesen	1 Bit	1.002	KL-Ü-
Rubrik:	Datenlogger	Datentyp:	Boolesch		
Funktion:	Zeigt an, ob derzeit ein microSD-Kartenfehler vorhanden ist.				
Beschreibung:	1 Bit Objekt zur Signalisierung eines microSD-Kartenfehlers. Wenn dem Objekt eine „1“ zugewiesen ist, liegt ein microSD-Kartenfehler vor.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
56	SD-Fehlercode	Lesen	1 Byte	20.*	KL-Ü-
Rubrik:	Datenlogger	Datentyp:	-		
Funktion:	Zeigt den derzeitigen Fehlercode an (0 = kein Fehler).				
Beschreibung:	1 Byte Objekt zur Signalisierung eines microSD-Kartenfehlers. 0 = microSD-Karte OK 1 = microSD-Karte voll 2 = microSD-Karte nicht gesteckt 4 = microSD-Karte hat einen Fehler (z.B. falsch formatiert)				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
57	Aktiviere Datenlogger	Schreiben	1 Bit	1.001	KLS--
Rubrik:	Datenlogger	Datentyp:	Schalten		
Funktion:	Aktiviert (1 = default) oder deaktiviert (0) das Logging und zeigt auf Abfrage den Status an.				
Beschreibung:	1 Bit Objekt zur Aktivierung des Datenloggers. Wenn dem Objekt eine „1“ zugewiesen wird, ist der Datenlogger aktiv. Wird ihm eine „0“ zugewiesen, ist er deaktiviert.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
58	Datenlogger - Status	Lesen	1 Bit	1.002	KL-Ü-
Rubrik:	Datenlogger	Datentyp:	Boolesch		
Funktion:	Zeigt an, ob der Datenlogger derzeit Daten aufzeichnet.				
Beschreibung:	1 Bit Objekt, welches den Zustand des Datenloggers wiedergibt. Wenn das Objekt den Wert „1“ hat, ist der Datenlogger aktiv. Eine „0“ bedeutet, dass der Datenlogger inaktiv ist.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
59	SD-Karten - Speicherzustand	Lesen	1 Bit	1.002	KL-Ü-
Rubrik:	Datenlogger	Datentyp:	Boolesch		
Funktion:	Zeigt an, ob der microSD-Kartenspeicher erschöpft ist (1 = voll).				
Beschreibung:	1 Bit Objekt zur Anzeige des Füllstandes der microSD-Karte. Wenn dem Objekt eine „1“ zugewiesen wird, ist die microSD-Karte voll. Wird ihm eine „0“ zugewiesen, ist auf der microSD-Karte noch Platz zum Loggen.				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
60	SD-Karte - Speicherfüllstand	Lesen	1 Byte	5.001	KL-Ü-
Rubrik:	Datenlogger	Datentyp:	Prozent (0..100%)		
Funktion:	Zeigt an, wieviel Prozent des microSD-Kartenspeichers belegt sind.				
Beschreibung:	1 Byte Objekt zur Anzeige des Füllstandes der microSD-Karte. Der Wertebereich ist 0-255 (entspricht 0-100%).				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	Benachrichtigung	Schreiben	1 Bit	1.001	K-S--
Rubrik:	Schalten	Datentyp:	Ein/Aus		
Funktion:	Sendet eine Benachrichtigung zum Portalserver.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Kommunikationsobjekte „101 bis 150“. Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Kapitel 8.5 "Parameter").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	Benachrichtigung	Schreiben	1 Byte	5.001	K-S--
Rubrik:	Prozent	Datentyp:	Prozent (0..100%)		
Funktion:	Sendet eine Benachrichtigung zum Portalserver.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Kommunikationsobjekte „101 bis 150“. Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Kapitel 8.5 "Parameter").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	Benachrichtigung	Schreiben	1 Byte	5.010	K-S--
Rubrik:	Zähler	Datentyp:			
Funktion:	Sendet eine Benachrichtigung zum Portalserver.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Kommunikationsobjekte „101 bis 150“. Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Kapitel 8.5 "Parameter").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	Benachrichtigung	Schreiben	2 Byte	9.*	K-S--
Rubrik:	Fließkomma	Datentyp:	KNX-Fließkomma (floating point)		
Funktion:	Sendet eine Benachrichtigung zum Portalserver.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Kommunikationsobjekte „101 bis 150“. Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Kapitel 8.5 "Parameter").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	Benachrichtigung	Schreiben	14 Byte	16.001	K-S--
Rubrik:	Text	Datentyp:	Zeichen (ISO 8859-1)		
Funktion:	Sendet eine Benachrichtigung zum Portalserver.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Kommunikationsobjekte „101 bis 150“. Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Kapitel 8.5 "Parameter").				

9. Anzeigen und Bedienung

9.1. LED-Statusanzeigen

Das Gerät verfügt über drei Status-LEDs auf der Gehäuseoberseite und über vier Status-LEDs an den Netzwerkanschlüssen.

Die LED-Anzeigen haben unterschiedliche Bedeutungen

- während Gerätestart und
- im Betrieb.

9.1.1. LED-Statusanzeige beim Gerätestart

Nach Einschalten der Spannungsversorgung (DC 24 V an der weiß-gelben Anschlussklemme) bzw. nach Spannungsrückkehr zeigt das Gerät den Status mit folgenden LED-Kombinationen an:

LED „RUN/DIAG“ (grün)	LED „KNX“ (gelb)	Bedeutung
aus	aus	Fehler: Keine Versorgungsspannung. Bitte Anschlüsse und Spannungsversorgung prüfen.
aus	ein	Gerät startet
blinkt langsam	ein	Das Gerät ist komplett hochgefahren, aber noch unparametriert. Ein ETS Download ist notwendig
blinkt schnell	aus	Fehler: Bitte kontaktieren Sie den Support. Die Firmware kann nicht gestartet werden.
Beide LED blinken langsam im Wechsel		Fehler: Bitte kontaktieren Sie den Support. Die neu geladene Firmware kann nicht gestartet werden. Das System versucht, die bisherige Firmware zu aktivieren (Ungültige Firmware)

9.1.2. LED-Statusanzeige im Betrieb

Ist der Gerätestart abgeschlossen, ist die Bedeutung der LEDs wie folgt:

LED „RUN/DIAG“ (grün)	Bedeutung
ein	Normalbetrieb: Der Fernzugriff ist generell erlaubt, das Gerät verbindet sich mit dem Portalserver, allerdings ist kein Fernzugriff derzeit aktiv.
aus	Gerät im Startvorgang oder außer Betrieb. Warten Sie bis Startvorgang abgeschlossen ist bzw. prüfen Sie die Spannungsversorgung
blinkt langsam mit 2 s Pause	Hinweis: Kein Fernzugriff erlaubt. Das Gerät verbindet sich nicht mit dem Gira Geräteportal, ein Fernzugriff ist technisch unmöglich.
blinkt dreimal langsam mit 2 s Pause	Hinweis: Der Fernzugriff ist für mindestens eine Gruppe erlaubt und es gibt mindestens eine aktive Verbindung. Der Fernzugriff ist also in Benutzung.

LED „KNX“ (gelb)	Bedeutung
ein	Normalbetrieb: KNX Verbindung ist hergestellt, kein KNX Telegrammverkehr.
blinkt schnell	Normalbetrieb: KNX Verbindung ist hergestellt, KNX Telegrammverkehr.
aus	Fehler: Verbindung zu KNX ist unterbrochen. Prüfen Sie die Busverbindung.

9.2. Werksreset

Nach einem Werksreset verhält sich das Gerät wie im Auslieferzustand. Das Gerät ist unprojektiert. Dies ist nach dem Hochfahren des Gerätes an der langsam blinkenden grünen LED (5) zu erkennen.
Werksseitig voreingestellt ist folgende physikalische KNX Adresse:15.15.255

Hinweis

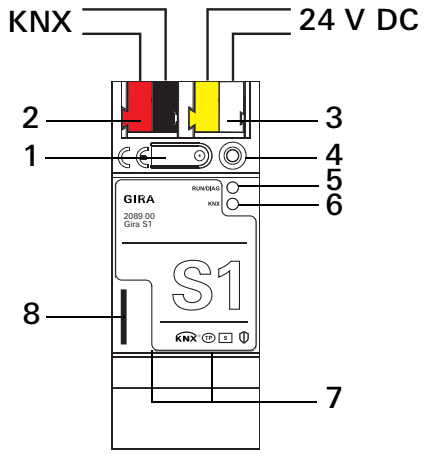
Ein Werksreset führt zu einer vollständigen Deaktivierung des VPN-Zugriffs.
Nach einem Werksreset ist die Neueinrichtung des VPN-Zugangs über das Gira Geräteportal erforderlich (siehe Kapitel 6 "VPN").

9.2.1. Werksreset über den Gira Projekt Assistent

Der Werksreset kann wie folgt über den Gira Projekt Assistent ausgeführt werden:

- Starten Sie den Gira Projekt Assistent und klicken Sie auf die Kachel „Wartung und Update“.
- In der sich öffnenden Ansicht werden alle Geräte aufgelistet, die sich in Ihrem Netzwerk befinden.
- Markieren Sie den Gira S1, den Sie auf die Werkseinstellungen zurücksetzen möchten.
- Klicken Sie in der markierten Zeile auf das Zahnradsymbol und wählen Sie in dem sich öffnenden Menü den Eintrag “Werksreset“.
- Geben Sie in dem sich öffnenden Dialog das Gerätepasswort des Gira S1 ein. Das Passwort befindet sich auf einem Aufkleber am Gerät.
- Der Werksreset wird durchgeführt.

9.2.2. Werksreset über die Programmiertaste am Gerät



Das Gerät kann über eine Sequenz beim Starten auf Werkseinstellungen zurückgesetzt werden:

- Sicherstellen, dass das Gerät ausgeschaltet ist (weiß-gelbe Anschlussklemme abziehen).
- Programmiertaste (1) drücken, gedrückt halten und das Gerät einschalten (weiß-gelbe Anschlussklemme aufstecken).
- Programmiertaste gedrückt halten bis die Programmier-LED (4), die Betriebsanzeige LED (5) und die KNX Led (6) gleichzeitig langsam blinken.
- Programmiertaste (1) kurz loslassen, erneut drücken und gedrückt halten bis die Programmier-LED (4),die Betriebsanzeige LED (5) und die KNX Led (6) gleichzeitig schnell blinken
- Der Werksreset wird durchgeführt.
- Programmiertaste loslassen.
- Das Gerät muss nach einem Werksreset nicht neu gestartet werden.

Der Werksreset kann zu jederzeit durch unterbrechen der Sequenz abgebrochen werden.

9.2.3. Werksreset über die Gerätewebseite

Der Werksreset kann auch über die Gerätewebseite ausgelöst werden.

- Rufen Sie die Gerätewebseite auf:
  Öffnen Sie dazu den Windows Explorer und klicken Sie dort auf „Netzwerk“.
  Im Bereich „Andere Geräte“ wird der Gira S1 angezeigt.
  Führen Sie einen Doppelklick auf das Symbol des Gira S1 aus.
  Alternativ können Sie auch die IP-Adresse des Gerätes in Ihrem Browser eingeben.
- Auf der sich öffnenden Webseite geben Sie bitte als Passwort die Registrierungs-ID des Gira S1 ein.
  Die Registrierungs-ID befindet sich auf einem Aufkleber am Gerät.
- Klicken Sie in der oberen Menüleiste auf Werksreset.
- Bestätigen Sie die Sicherheitsabfrage.
- Die nachfolgend angezeigte Seite zeigt die Durchführung des Werksresets an. Sobald dieser abgeschlossen ist, wird wieder die Startseite geladen.

9.3. Firmwareupdate des Gerätes

9.3.1. Firmwareupdate über den Gira Projekt Assistent

Ein Firmwareupdate kann wie folgt über den Gira Projekt Assistent ausgeführt werden:

- Starten Sie den Gira Projekt Assistent und klicken Sie auf die Kachel „Wartung und Update“.
- In der sich öffnenden Ansicht werden alle Geräte aufgelistet, die sich in Ihrem Netzwerk befinden.
- Markieren Sie den Gira S1, den Sie aktualisieren möchten.
- Klicken Sie in der markierten Zeile auf das Zahnradsymbol und wählen Sie in dem sich öffnenden Menü den Eintrag „Firmware auswählen“.
- Markieren Sie die gewünschte Firmware und klicken Sie auf „Aktualisierung starten“.
- Geben Sie in dem sich öffnenden Dialog das Gerätepasswort des Gira S1 ein.
- Die Firmware wird aktualisiert. Dies kann mehrere Minuten dauern. Trennen Sie das Gerät während dieser Zeit nicht vom Netz.

9.3.2. Firmwareupdate über die Gerätewebseite

Der Gira S1 bietet die Möglichkeit, Firmwareupdates über die Gerätewebseite zu installieren. Klicken Sie hierzu auf der Gerätewebseite auf „Firmware aktualisieren“. Nun sucht der Gira S1 automatisch auf dem Updateserver nach einer neueren Version und zeigt die aktuelle Firmwareversion sowie ggf. die Version eines verfügbaren Updates an.

Wenn die neue Firmware inkompatibel zur Konfiguration der vorherigen Firmware ist, so wird eine entsprechende Meldung angezeigt. Hierbei werden zwischen den folgenden Fällen unterschieden:

1. Die neue Version stellt neue Funktionalität zur Verfügung. Das Gerät funktioniert nach dem Update mit dem unveränderten Funktionsumfang. Neue Funktionen können aber erst nach einem ETS-Download von einem neueren Katalogeintrag genutzt werden.
2. Die neue Version ist vollständig inkompatibel zur Parametrierung der aktuell verwendeten Version. Ein ETS-Download ist zwingend erforderlich. Es wird empfohlen, das ETS-Applikationsprogramm vor dem Update zu entladen und das Gerät nach dem Update mit dem neuen Katalogeintrag zu projektieren.

Das Update kann über die Schaltfläche „Firmware aktualisieren“ gestartet werden. Im Falle einer möglichen Inkompatibilität muss das Update zur Sicherheit nochmals bestätigt werden.

9.3.3. Lokales Firmwareupdate ohne Internetzugang

Zusätzlich zu einem Online-Update ist ein lokales Update ohne Internetzugang möglich. Die Firmwaredatei kann über die Schaltfläche „Datei auswählen“ ausgewählt werden und anschließend über die Schaltfläche „Firmware aktualisieren“ gestartet werden. In diesem Fall ist der Anwender dafür verantwortlich sicherzustellen, dass das Update kompatibel ist (siehe Kapitel 9.3.4 "Kompatibilität zwischen ETS Katalogeintrag und Firmware"). Ein Downgrade auf eine ältere Version ist mit diesem Verfahren nicht möglich.

9.3.4. Kompatibilität zwischen ETS Katalogeintrag und Firmware

Die Versionsnummern des ETS Katalogeintrags und der Firmware sind nach dem Schema X.Y aufgebaut. Die Hauptnummer X der jeweiligen Version gibt an, ob Katalogeintrag und Firmware kompatibel sind. Dies ist der Fall, wenn beide Hauptnummern identisch sind. Der zweite Teil der Versionsnummer Y hat keine Bedeutung für die Kompatibilität. Sie signalisiert lediglich Updates innerhalb der Version.

Wenn eine neue Firmware eine höhere Hauptnummer hat, ist nicht garantiert, dass diese Version mit einem alten ETS Katalogeintrag kompatibel ist. Daher wird empfohlen, das Applikationsprogramm vom Gerät immer vor dem Update zu entladen und danach nur noch den neuen Katalogeintrag zu verwenden.

Wenn die Hauptnummern gleich sind, kann es nötig sein, einen neuen ETS Katalogeintrag zu verwenden, um die volle Funktionalität zu erlangen. Dies ist aber nicht zwingend notwendig, wenn die neuen Funktionen nicht in Ihrem Projekt verwendet werden.

10. Nutzung des Gira Geräteportals

Für die Fernzugriffsfunktionen muss der Gira S1 im Gira Geräteportal registriert werden.
Das Gira Geräteportal ist unter der gesicherten Adresse https://geraeteportal.gira.de erreichbar.

10.1. Startseite

Auf der Startseite des Gira Geräteportals müssen Sie sich zunächst mit Ihren Benutzerdaten anmelden, um entsprechenden Zugriff auf die Konfigurationseinstellungen zu erhalten.
Vor der ersten Verwendung des Gira Geräteportal müssen Sie sich als Benutzer registrieren. Klicken sie dazu auf „Registrieren“.
Die Registrierung erfolgt nach dem heute üblichen Standard zur Verifikation der E-Mail-Adresse. Geben Sie bei der Registrierung Ihre E-Mail-Adresse an. An diese E-Mail-Adresse wird automatisch eine E-Mail zur Verifikation geschickt. Die Bestätigung des Links in dieser E-Mail ist zwingend erforderlich. Damit ist sichergestellt, dass eine Anmeldung unter einer fremden E-Mail-Adresse nicht möglich ist.

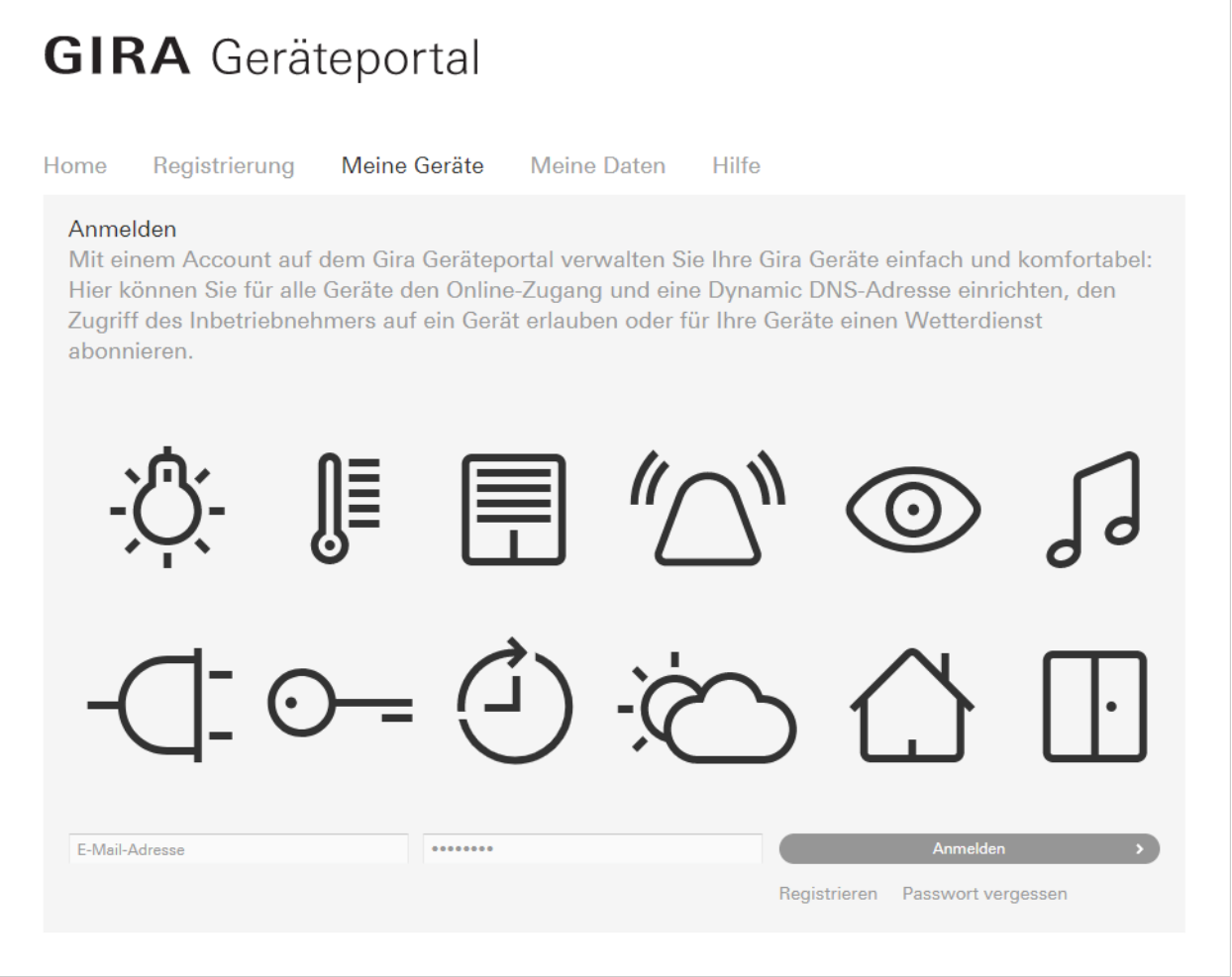


Bild 14: Gira Geräteportal – Startseite

10.2. Geräteübersicht

Nachdem Sie sich am Gira Geräteportal angemeldet haben, sehen Sie die Liste aller mit Ihrem Benutzerkonto verbundenen Geräte. Bei der ersten Anmeldung ist sie typischerweise leer.

Sie können über folgende Wege mit einem Gerät verbunden werden:

1. Sie fügen der Liste Ihrer Geräte einen neuen Gira S1 hinzu, indem Sie das Gerät registrieren und werden damit der Eigentümer (siehe Kapitel 10.3 "Gira S1 registrieren").
2. Ein anderer Benutzer gibt Ihnen Zugriffsrechte auf einen Gira S1, der von dem anderen Benutzer administriert wird.
3. Ein anderer Benutzer überträgt Ihnen die Eigentümerschaft (siehe Kapitel 10.9.3 "Gerätebesitz übertragen - Schlüsselübergabe").

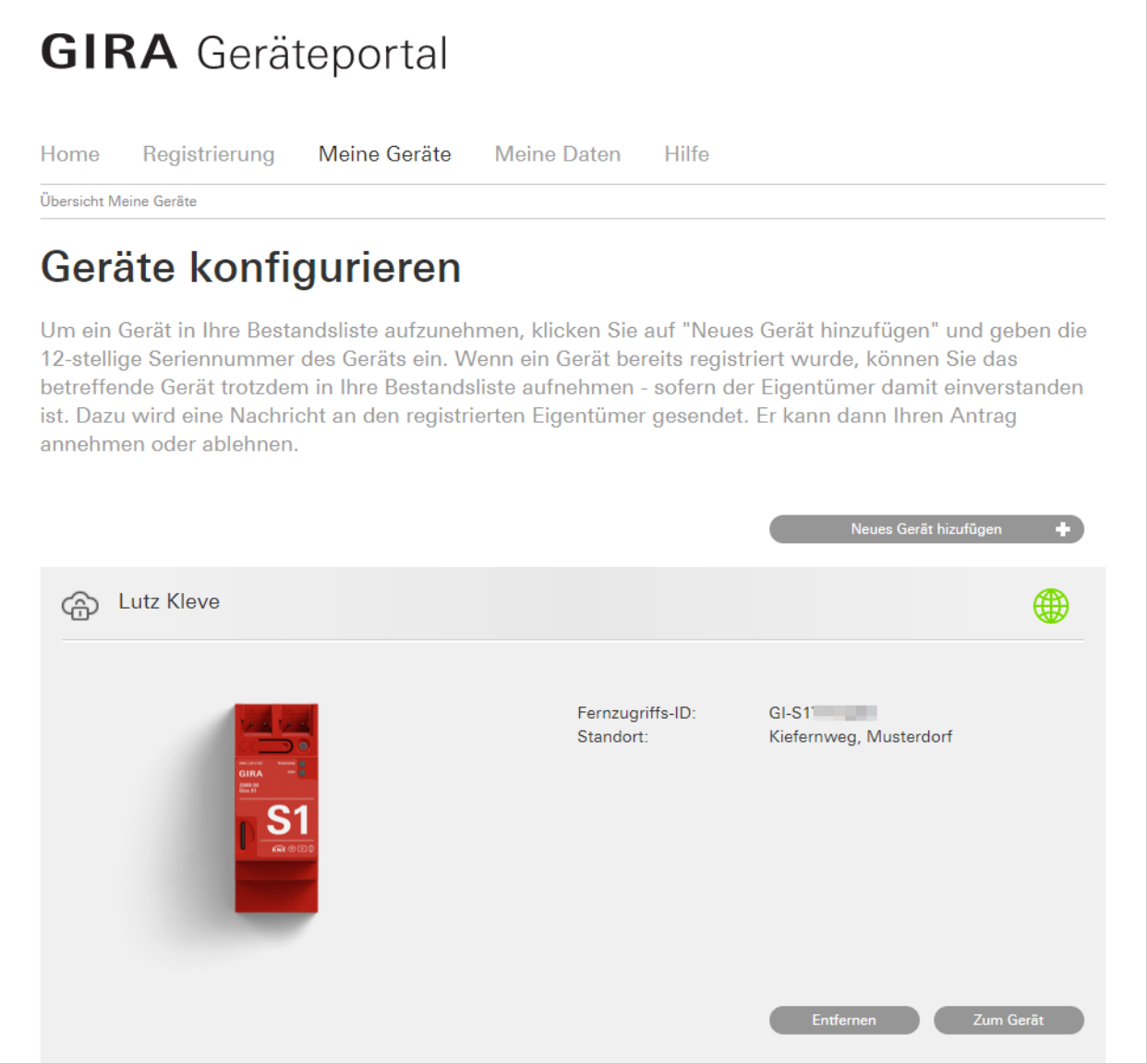


Bild 15: Gira Geräteportal – Geräte des angemeldeten Benutzers

10.3. Gira S1 registrieren

Um einen Gira S1 zu registrieren, gehen Sie wie folgt vor:

1. Melden Sie sich mit Ihrer Benutzerkennung am Gira Geräteportal an.
2. Klicken Sie im Geräteportal auf „Registrierung“.
3. Wählen Sie als Gerät den Gira S1 aus.
4. Geben Sie die Registrierungs-ID ein.
   Die Registrierungs-ID finden Sie auf einem Aufkleber am Gerät.
5. Vergeben Sie einen Namen für das Gerät und tragen Sie einen Standort ein.
6. Klicken Sie auf „Weiter“ und akzeptieren Sie die Nutzungsbedingungen.
7. Nachdem Sie den Gira S1 erfolgreich registriert haben, öffnet sich die Übersichtsseite für den Gira S1. Hier stehen Ihnen die folgenden Optionen zur Verfügung:
   - Links (siehe Kapitel 10.4)
   - Nachrichten (siehe Kapitel 10.5)
   - Gerätedaten (siehe Kapitel 10.6)
   - Applikationszugänge (siehe Kapitel 10.7)
   - Weiterleitungen (siehe Kapitel 10.8)
   - Portalbenutzer (siehe Kapitel 10.9)
   - VPN-Zugang (siehe Kapitel 10.10)
   - FAQs (siehe Kapitel 10.11)

10.4. Links

Die Ansicht „Links“ listet die Webseiten der im Netzwerk befindlichen Geräte auf. Diese Seite speichert die bereits in der Vergangenheit genutzten Links zu Geräten. Darüber hinaus kann über die Schaltfläche „Geräte suchen“ auch im entfernten Netzwerk nach Geräten gesucht werden. Dabei wird für jedes gefundene Gerät ein Link automatisch erzeugt. Die meisten Geräte wie z.B. Drucker, DSL-Router oder IP-Kameras werden dabei erfasst. Technisch wird hier das Simple Service Discovery Protocol (kurz SSDP) benutzt.

Über den Dialog „Link manuell hinzufügen“ können Links von Geräten die nicht automatisch gefunden werden, manuell eingegeben und in der Liste gespeichert werden.

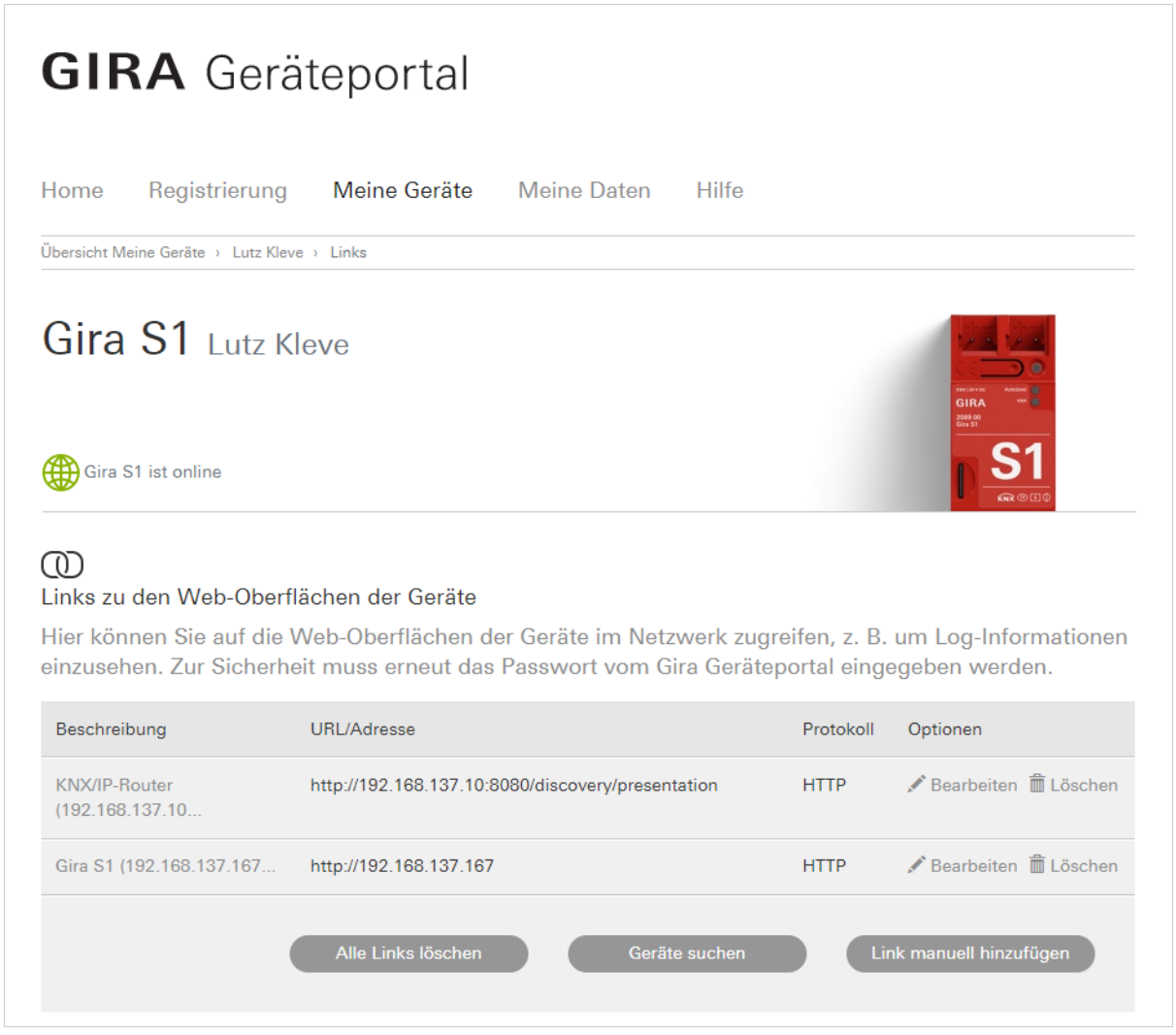


Bild 16: Gira Geräteportal – Zugriff auf HTTP-Webseiten

10.5. Nachrichten

Im Bereich „Nachrichten“ werden alle Nachrichten eines Gira S1 chronologisch sortiert angezeigt. Eventuelle Anhänge wie z.B. Kamerabilder können per Link direkt geöffnet werden.

Diese Nachrichten können auch nach konfigurierbaren Regeln weitergeleitet werden (siehe Kapitel 10.8 "Nachrichten konfigurieren").

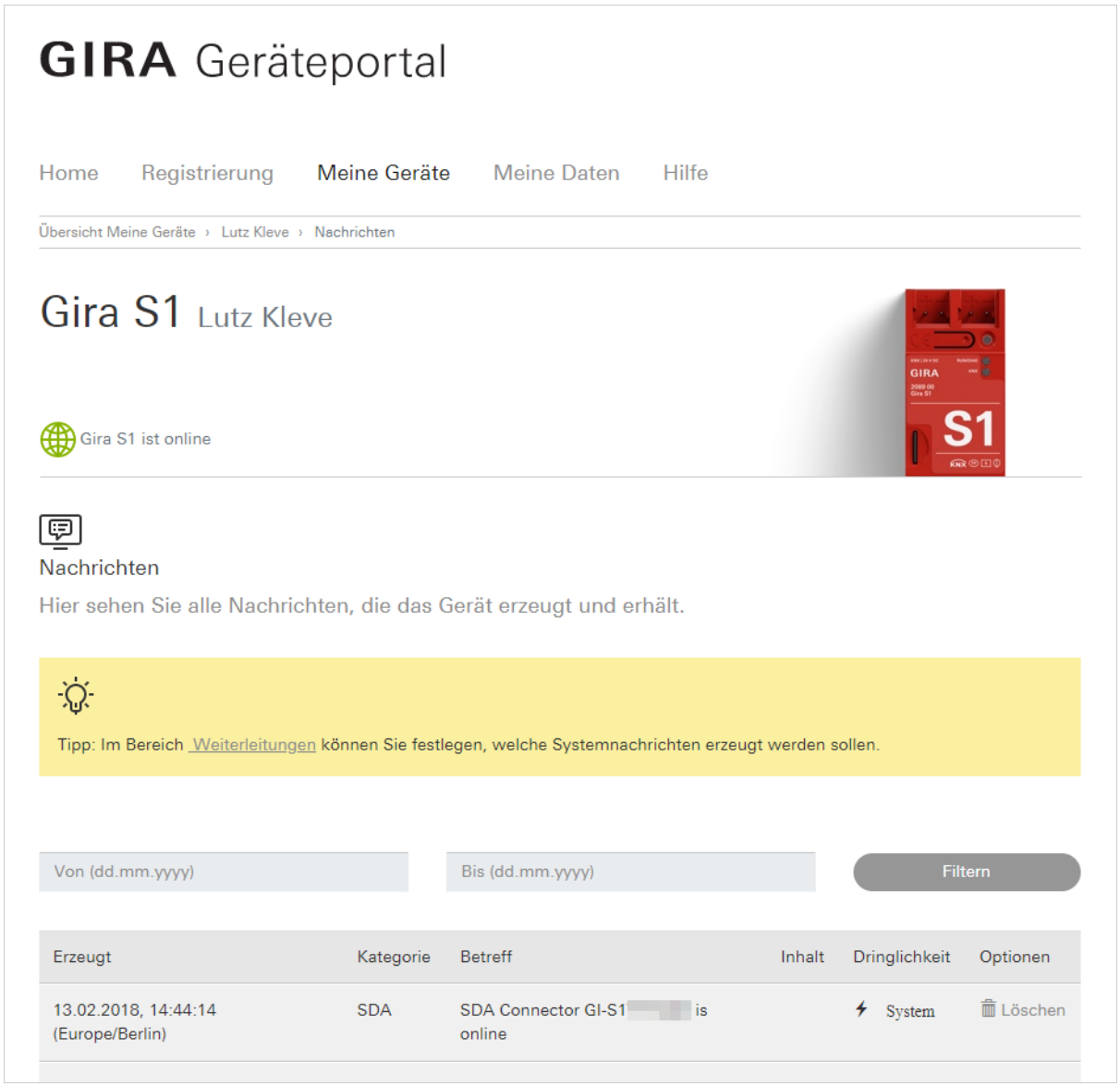


Bild 17: Gira Geräteportal – Nachrichten

10.6. Gerätedaten

Die Seite zeigt detaillierte Informationen zum Gira S1 an. Über die Schaltfläche „Anzeigen“ kann die vollständige Registrierungs-ID sichtbar gemacht werden, die Sie dann mit der Schaltfläche „Kopieren“ in die Zwischenablage kopieren können.

Die Zeile „Standort“ erhält ein Textfeld, welches vom Anwender frei vergeben werden kann. Der Standort ist eine Eigenschaft am Gira S1 und damit für alle Benutzer gleich, der Beschreibungstext kann von jedem mit dem Gira S1 verbundenen Benutzer frei vergeben werden. Das ermöglicht z. B. einem Installateur nach der Übergabe die Adresse zu hinterlegen, während der Bauherr als Standort „Zu Hause“ einträgt.

Über „Gerät vom Portal löschen“ können Sie den Gira S1 aus dem Geräteportal löschen. Diese Funktion ist nur sinnvoll, wenn der Gira S1 verkauft wird, da alle Benutzerberechtigungen u.ä. irreversibel entfernt werden.

Weiterhin werden die Benutzer für dieses Gerät angezeigt. Über die Schaltfläche „Benutzer verwalten“ wird die Seite „Portalbenutzer verwalten“ aufgerufen, auf der Sie Benutzer z. B. hinzufügen oder löschen können.

Im Bereich „Datenverbrauch“ erhalten Sie Informationen über den aktuellen Verbindungsstatus des Gira S1. Die Uhrzeitangaben werden entsprechend der Zeitzoneneinstellung Ihres Benutzers dargestellt. Zusätzlich wird das bisher verbrauchte Datenvolumen für den aktuellen sowie den Vormonat angezeigt. Hinsichtlich des zur Verfügung stehenden Datenvolumens und der Nutzungsbedingungen siehe Kapitel 16 "Lizenzvereinbarung".

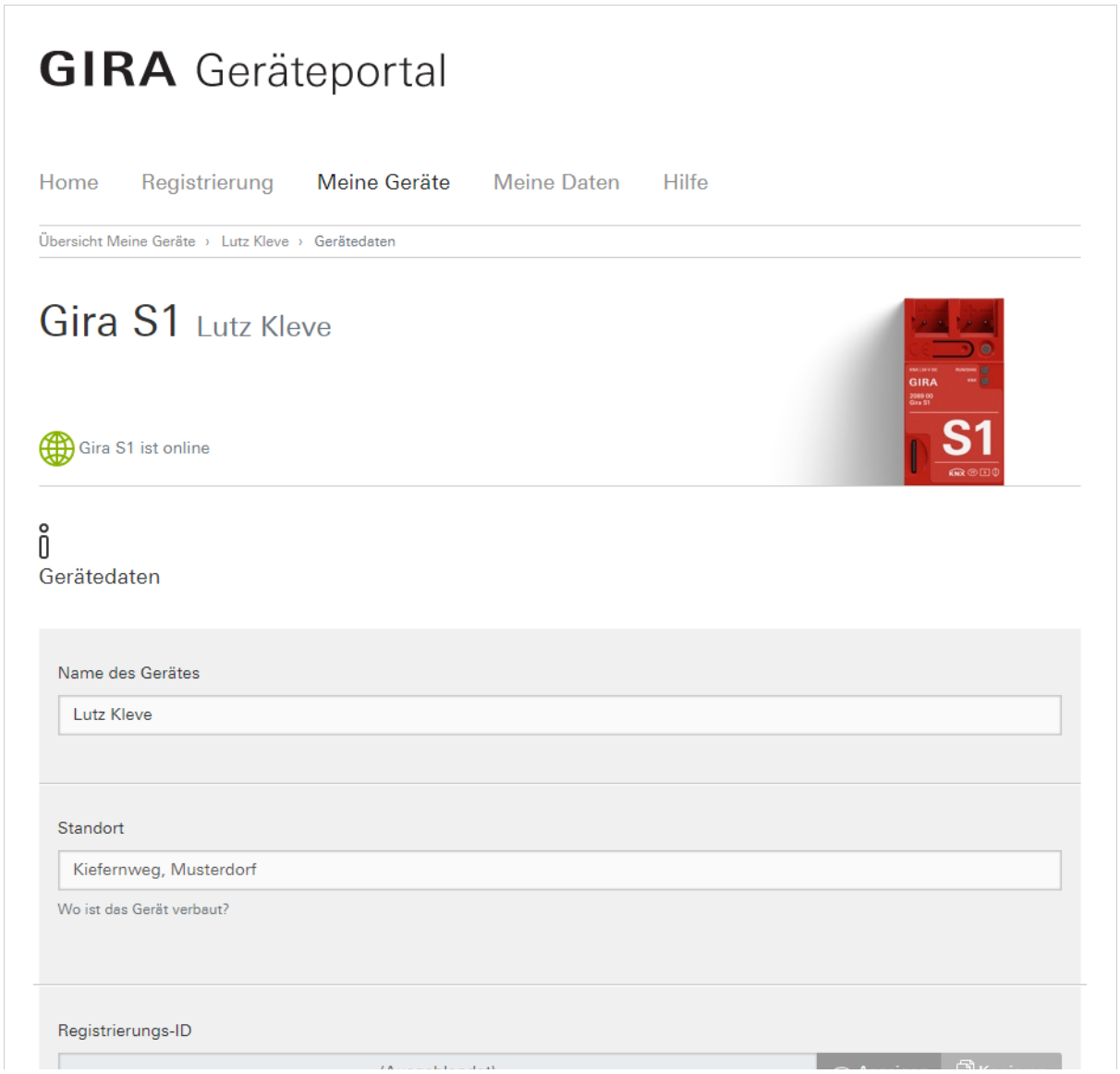


Bild 18: Gira Geräteportal – Gerätedaten

10.7. Applikationszugänge

Der Zugriff von Software wie z. B. Visualisierungen wird über den Einsatz von Aktivierungscodes gesteuert. Von diesen kann jeder Benutzer an jedem Gira S1, auf den er Zugriff hat, beliebig viele Codes anlegen, z. B. für die Visualisierung.

Zu jedem erzeugten Aktivierungscode steht ein Textfeld zur Verfügung, dass die Nutzung des Codes beschreibt. Die Aktivierungscodes können jederzeit wieder gelöscht werden (z. B. wenn ein Smart-Phone verloren geht). Es wird niemals ein gleicher Aktivierungscode nochmals erzeugt, so dass ein verloren gegangener Code durch das Löschen unwiderruflich unbrauchbar wird.

Um einen neuen Aktivierungscode zur erstellen, klicken Sie auf „Neuen App-Zugang erstellen“.

Für erstellte Aktivierungscodes stehen folgende Aktionen zur Verfügung:

- Kopieren in die Zwischenablage
- Löschen des Aktivierungscodes

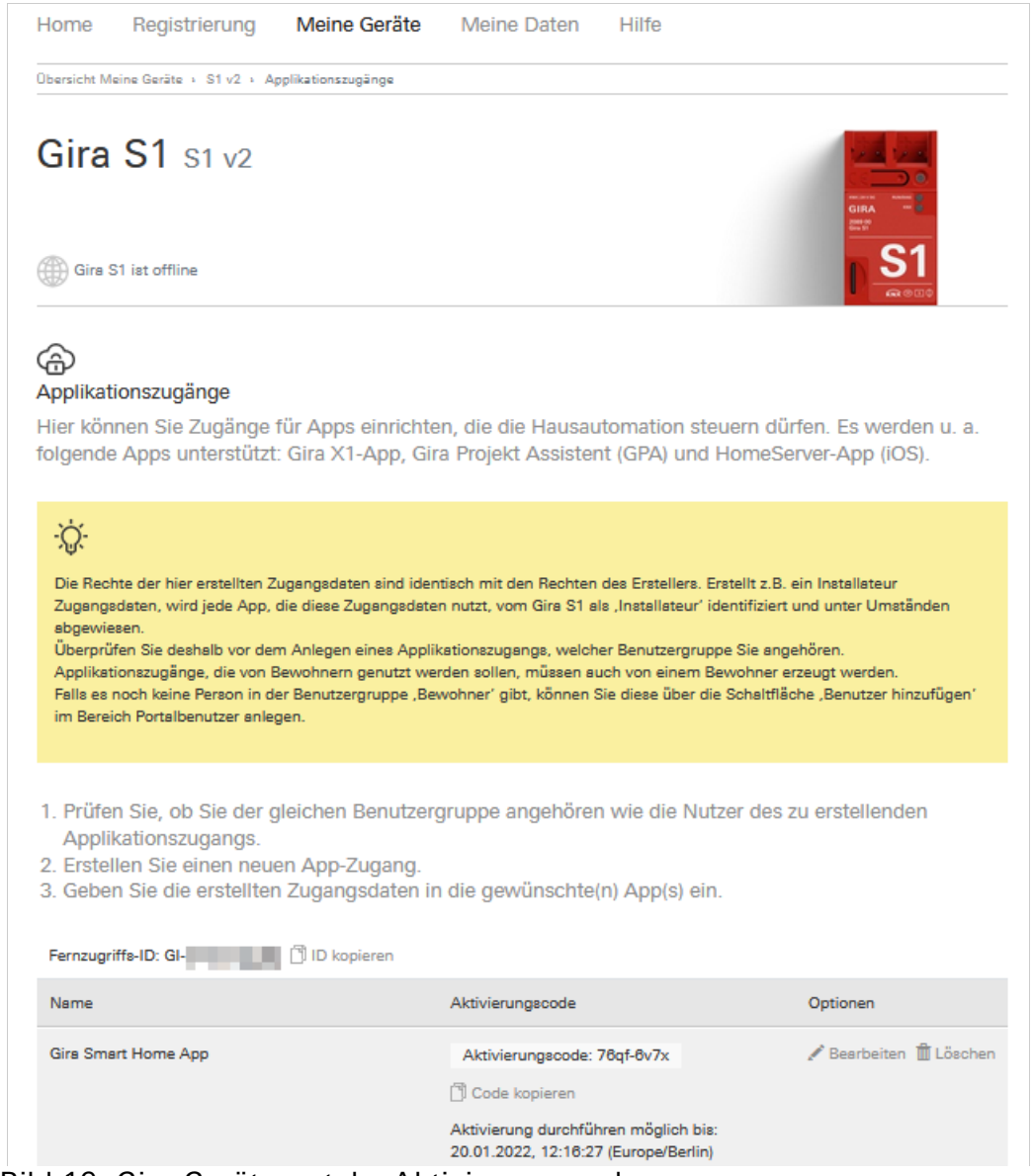


Bild 19: Gira Geräteportal – Aktivierungscodes

Geben Sie anschließend die erstellten Zugangsdaten in die gewünschte Applikation ein.

10.7.1. Zugangsdaten im Gira Projekt Assistent (GPA) eingeben

1. Öffnen Sie das Projekt im GPA.
2. Im Projektumfang muss die Option „Fernzugriff“ aktiviert sein.
3. Klicken Sie im Projekt auf die Kachel „Fernzugriff“.
4. Wählen Sie in der sich öffnenden Ansicht die Option „Fernzugriff über Gira S1“.
5. Kicken Sie auf die Schaltfläche „Fernzugriff konfigurieren“.
6. Geben Sie die Fernzugriffs-ID und den Aktivierungscode ein und klicken Sie auf „Verbinden“.

Hinweis

Die über den Gira Projekt Assistent zur Verfügung gestellte Verbindung steht allen Teilnehmern zur Verfügung, die sich im selben Netzwerk befinden, wie der PC mit dem Gira Projekt Assistent.
Bitte nutzen Sie diese Funktion daher nicht in öffentlichen Netzwerken.

10.7.2. Zugangsdaten in die Gira Smart Home App eingeben

1. Öffnen Sie die Gira Smart Home App auf dem Smartphone.
2. Öffnen Sie in der App das Systemmenü, indem Sie auf das Zahnradsymbol in der Navigationsleiste tippen.
3. Tippen Sie im Systemmenü auf die Schaltfläche „System“.
4. Tippen Sie auf „Verbindung zum Gira Gerät“.
5. Tippen Sie auf „Fernzugriff konfigurieren“.
6. Aktivieren Sie den Fernzugriff, indem Sie den Schiebeschalter nach rechts bewegen.
7. Geben Sie die Fernzugriffs-ID und den Aktivierungscode ein und klicken Sie auf „OK“.

10.7.3. Zugangsdaten in die Gira HomeServer App eingeben

1. Öffnen Sie die Gira HomeServer App auf dem Smartphone.
2. Legen Sie ein neues Profil an.
3. Wählen Sie in dem sich öffnenden Dialog die Option „Profil mit Fernzugriffsmodul“.
4. Geben Sie neben den anderen notwendigen Eingaben für das Profil die Fernzugriffs-ID und den Aktivierungscode ein und klicken Sie auf „speichern“.

10.8. Nachrichten konfigurieren

In diesem Bereich können Sie festlegen, welche Nachrichten generiert werden sollen und Weiterleitungsregeln erstellen.

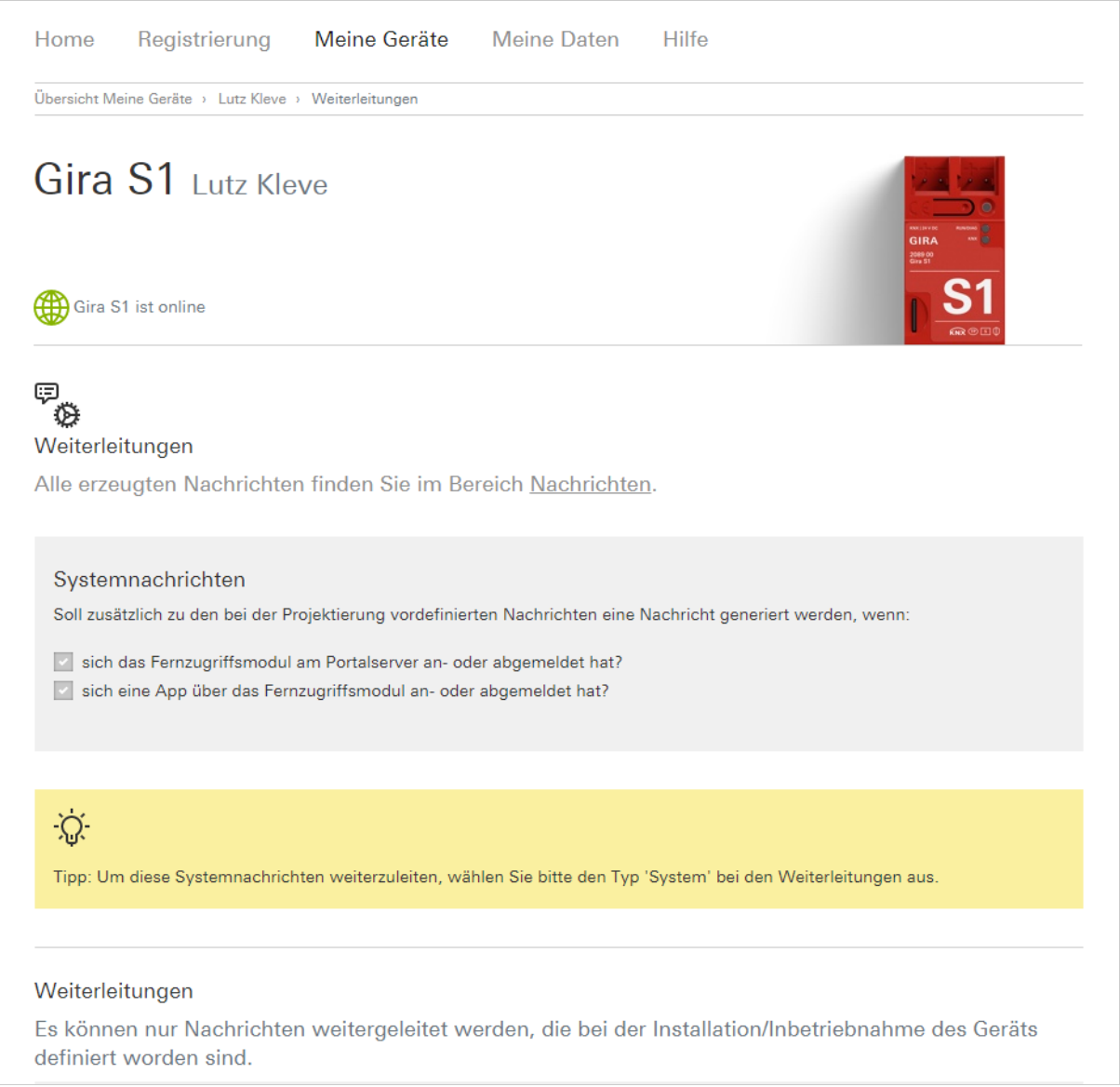


Bild 20: Gira Geräteportal – Nachrichtenempfang

10.8.1. Systemnachrichten

Als Systemereignisse können das An- und Abmelden des Gira S1 am Portal und der Zugriff auf das entfernte Netzwerk über eine App erfasst werden.

10.8.2. Benachrichtigungen über KNX

Die Benachrichtigungen sind dafür gedacht, aus der Installation, z. B. über KNX Kommunikationsobjekte, Informationen auf dem Portal in einer Nachrichtendatenbank zu speichern. Es stehen 50 KNX Kommunikationsobjekte zur Verfügung, um Werte vom KNX zu empfangen und Nachrichten daraus zu erzeugen.

Folgende Datentypen werden unterstützt:

- Bool (1 Bit)
- Zähler (1 Byte), z. B. Anzahl offene Fenster
- Prozent (1 Byte), z. B. Helligkeit oder Jalousieposition
- Fließkommazahl (2 Byte), z.B. Raum- oder Außentemperatur
- Texte (14 Byte), z. B. Alarmtext

Neben der Auswahl des Datentyps können Filter angegeben werden, z.B. Grenzwerte oder Wertebereiche, in denen Nachrichten erzeugt werden sollen.

Benachrichtigungen unterdrücken: Falls Sie nicht über jede Änderung benachrichtigt werden möchten, können Sie einen Schwellwert angeben (als absoluten Wert). Änderungen werden dann erst gemeldet, wenn dieser Schwellwert überschritten wird.

Die beiden Texteigenschaften „Betreff“ und „Text“ können aus statischen Texten bestehen, in denen per Platzhalter der vom KNX empfangene Wert eingesetzt werden kann. Außerdem kann optional eine Webadresse angegeben werden, um von einem Webserver (z. B. IP Kamera) einen Anhang zu laden und diesen an eine Nachricht anzuhängen.

Die konkreten Beschreibungen dieser Funktionen finden sich im Parameterdialog in der ETS.

Hinweis

Es können maximal 120 Benachrichtigungen in zwei Minuten und 1000 Benachrichtigungen innerhalb von 24 Stunden versendet werden. Bei Überschreitung einer dieser Grenzen wird der Nachrichtenversand gesperrt. Eine Benachrichtigung mit dem Titel „Drop notification“ und dem Inhalt „Dropped excess notification(s)“ wird versendet. Die Sperre wird aufgehoben, sobald die Nachrichtengrenzen unterschritten werden.

10.8.3. Weiterleitungen

Die Benachrichtigungen werden zunächst nur im Geräteportal in der Ansicht „Nachrichten“ angezeigt. Als Administrator können Sie Weiterleitungsregeln für Benachrichtigungen festlegen.

Die Benachrichtigungen können bei der Erzeugung auf verschiedene Arten weitergeleitet werden:

- E-Mail (Standard ist die Benutzerkennung des Portals, Angabe mehrerer Adressen möglich)
- Push-Nachrichten (wahlweise an die Gira Smart Home App oder die MySDA-App)
- SMS-Dienst (nutzt sms77.de oder Messagebird als Provider, Angabe mehrerer Adressen möglich)
- Text-to-Speech-Dienst (Telefonsprachanruf), der die Benachrichtigung vorliest, in vielen verschiedenen Sprachen möglich (nutzt sms77.de oder Messagebird als Provider)
- IFTTT (If-this-then-that, nutzt IFTTT.com, nur für erfahrene Benutzer)

Hinweis

Für die Nutzung der Funktionen SMS, Text-to-Speech und IFTTT, die auf die Dienste von sms77.de, Messagebird.com oder IFTTT basieren, muss ein eigener Account bei sms77.de, Messagebird.com bzw. ifttt.com eingerichtet werden. Die entsprechenden Zugangsdaten müssen im Menüpunkt „Externe Dienste“ in der Ansicht „Meine Daten“ eingetragen werden!

Jede Weiterleitungsregel gibt die Möglichkeit, nach Dringlichkeit und/oder Kategorie (Textfilter; ist mindestens ein Wort enthalten, ist die Filterbedingung erfüllt) Benachrichtigungen auszuwählen und weiterzuleiten. Es können beliebig viele Weiterleitungsregeln konfiguriert werden, von denen jeweils alle aktiven beim Eingang einer Benachrichtigung ausgewertet werden.

Die Möglichkeit der Deaktivierung erlaubt das Erstellen von Regeln, die nicht immer benötigt werden, z. B. wenn man im Urlaub ist.

Beispiel: Sie wollen alle Nachrichten der Dringlichkeit „System“ per E-Mail weitergeleitet bekommen (darunter fallen z. B: die On-/Offline-Meldungen). Hierzu führen Sie folgendes aus:

- Klicken Sie auf „Neue Weiterleitung anlegen“.
- Deaktivieren Sie alle Dringlichkeiten außer „System“
- Aktivieren Sie die Option „Weiterleitung per E-Mail“.
  Tragen Sie die E-Mail-Adresse für den Empfang der Weiterleitungen ein.
- Speichern Sie die Weiterleitungsregel. Sie ist automatisch aktiviert.

Hinweis

Die vom System erzeugten Benachrichtigungen z. B: für On-/Offlinezustand des Gira S1 werden immer mit der Dringlichkeit „System“ und Kategorie „Fernzugriff“ erzeugt. Alle Dringlichkeiten bis auf „System“ und beliebige Kategorien können bei der Nutzung der Benachrichtigungen über KNX Objekte verwendet werden.

10.9. Portalbenutzer verwalten

Das Gira Geräteportal erlaubt die differenzierte Konfiguration von Zugriffsrechten auf Basis von Benutzern für jeden Gira S1. Für jeden Benutzer kann festgelegt werden:

- Portalrolle: Die Portalrolle definiert ausschließlich die Konfigurationsrechte vom Gira S1 im Gira Geräteportal. Möglich sind hier „Eigentümer“, „Administrator“ und „Benutzer“, wobei der Eigentümer ein Administrator mit einer Sonderstellung ist, und daher im Folgenden nur noch von Administrator und Benutzer gesprochen wird.
- Zugriffsgruppe: Über die Zugriffsgruppe kann der Zugang zum entfernten Netzwerk gesteuert werden. Möglich sind hier „Bewohner“ und „Installateur“, wobei ein Benutzer keiner oder auch beiden Gruppen zugeordnet sein kann.

Neben dem Hinzufügen von neuen Benutzern zu einem Gira S1, können Benutzerrechte auch wieder eingeschränkt bzw. die Verbindung eines Gira S1 mit einem Benutzer gelöscht werden.

Für Benachrichtigungen sowie die Funktion „Geräte suchen“ können die Rechte von Benutzern ohne administrative Rechte eingeschränkt werden.

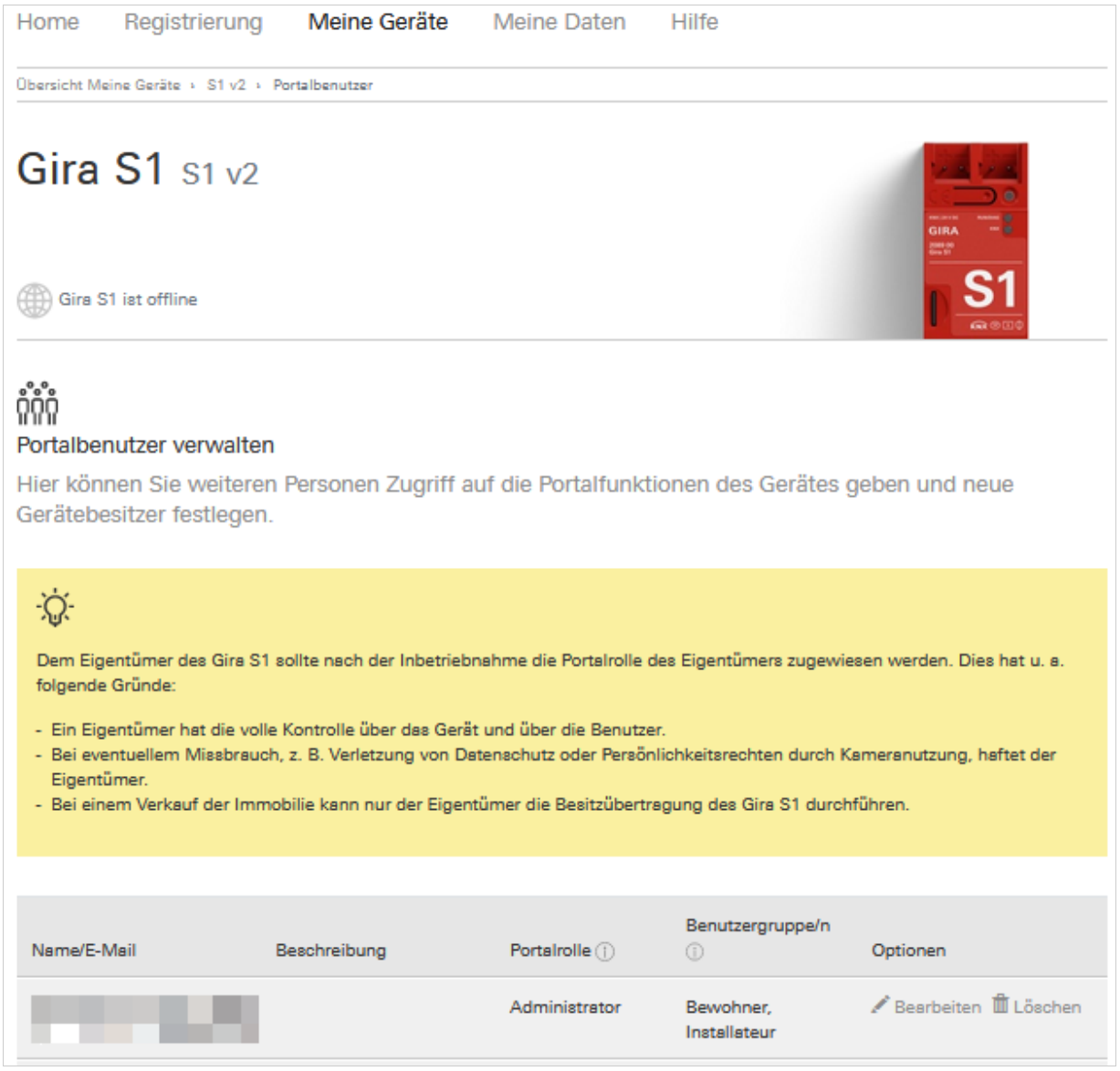


Bild 21: Zugriffsrechte für Benutzer verwalten

10.9.1. Die Portalrolle eines Benutzers an einem Gira S1

Der Unterschied zwischen einem Administrator und Benutzer liegt in den Rechten, auf dem Gira Geräteportal Konfigurationsänderungen vornehmen zu dürfen. Der Eigentümer des Gerätes ist automatisch auch Administrator. Jeder Administrator kann alle Eigenschaften und Benutzerrechte für den Gira S1 verwalten (mit Ausnahme der Eigentümerschaft), der Benutzer kann die Eigenschaften maximal anschauen.

Hinweis

Die Rolle eines Benutzers bezieht sich ausschließlich auf die Konfigurationsmöglichkeiten auf dem Gira Geräteportal und hat nichts mit den Zugriffsrechten über Fernzugriff auf das entfernte Netzwerk zu tun. Für letzteres dienen ausschließlich die Benutzergruppen.

10.9.2. Die Zugriffsgruppe eines Benutzers an einem Gira S1

Über die Zugriffsgruppen ist es möglich, gruppenabhängig dauerhaft oder eben auch nur temporär Zugriff auf das entfernte Netzwerk zu geben. Über KNX Kommunikationsobjekte können für die beiden Gruppen Bewohner und Installateur die Zugriffsmöglichkeiten jederzeit aktiviert bzw. deaktiviert werden.

Hinweis

Die Zugriffsgruppen eines Benutzers beziehen sich ausschließlich auf die Rechte, auf das entfernte Netzwerk über Fernzugriff zuzugreifen, um z. B. Webseiten zu besuchen oder mit der ETS auf die KNX Installation zuzugreifen. Wenn Sie die Konfigurationsmöglichkeiten auf dem Gira Geräteportal für einen Benutzer ändern wollen, nutzen Sie hierfür die Portalrollen.

10.9.3. Gerätebesitz übertragen - Schlüsselübergabe

Ab dem Moment, ab dem ein Gira S1 im Gira Geräteportal registriert wird, hat der Gira S1 einen Eigentümer. Es gibt ab dann immer genau einen Eigentümer.

Der Eigentümer ist die Person, die rechtlich für die Nutzung des Fernzugriffs verantwortlich ist. Zum Zeitpunkt der Installation bzw. Projektierung ist dies üblicherweise der Elektroinstallateur bzw. Systemintegrator. Bei der Schlüsselübergabe an den Eigentümer der Installation wird die Eigentümerschaft üblicherweise übertragen.

Der Eigentümer eines Gira S1 kann jederzeit allen anderen Benutzer, auch anderen Administratoren, alle Rechte entziehen, während ihm niemand den Zugriff verwehren kann.

Falls es zum Missbrauch des Gira S1 bzw. des Fernzugriff im Sinne des Lizenzvertrags oder anderer gesetzlicher Bestimmungen (Verletzung von Datenschutz oder Persönlichkeitsrechten durch Kameras o. ä.) kommt, haftet in erster Instanz der Eigentümer.

Das Übertragen der Eigentümerschaft ist im Gira Geräteportal möglich. Hierzu gibt es die Schaltfläche „Besitzübertragung“ auf der Seite „Portalbenutzer verwalten“.

Das Wechseln des Eigentümers erfolgt in einem gesicherten Verfahren:

1. Der aktuelle Eigentümer klickt auf die Schaltfläche „Besitzübertragung“, gibt die E-Mail-Adresse des gewünschten neuen Eigentümers ein und sendet die Anforderung ab.
2. Der gewünschte neue Eigentümer erhält eine E-Mail, in der ein Link enthalten ist um die Übernahme der Eigentümerschaft zu akzeptieren. Gleiches gilt zur Sicherheit nochmal für den aktuellen Eigentümer.

3. Wenn sowohl der neue als auch der aktuelle Eigentümer den Wechsel akzeptiert haben, erhalten beide eine entsprechende E-Mail und die Eigentümerschaft ist übergegangen.

Wird vom neuen oder vom aktuellen Eigentümer die Anfrage nicht bestätigt, findet keine Übertragung der Eigentümerschaft statt.

Hinweis

Beachten Sie bitte, dass der bisherige Eigentümer nach abgeschlossener Besitzübertragung die Benutzerrolle „Administrator“ behält. Wenn das nicht gewünscht ist, kann dies in der Ansicht „Portalbenutzer“ geändert werden.

10.10. VPN-Zugang einrichten

Unter „VPN-Zugang“ können Administratoren die folgenden Einstellungen vornehmen:

- VPN-Zugang aktivieren/deaktivieren.
- VPN-Zugang für einzelne Benutzer freigeben.
- Eigenschaften ändern.
- VPN-Konfigurationsdatei herunterladen.
- VPN-Zugang löschen.

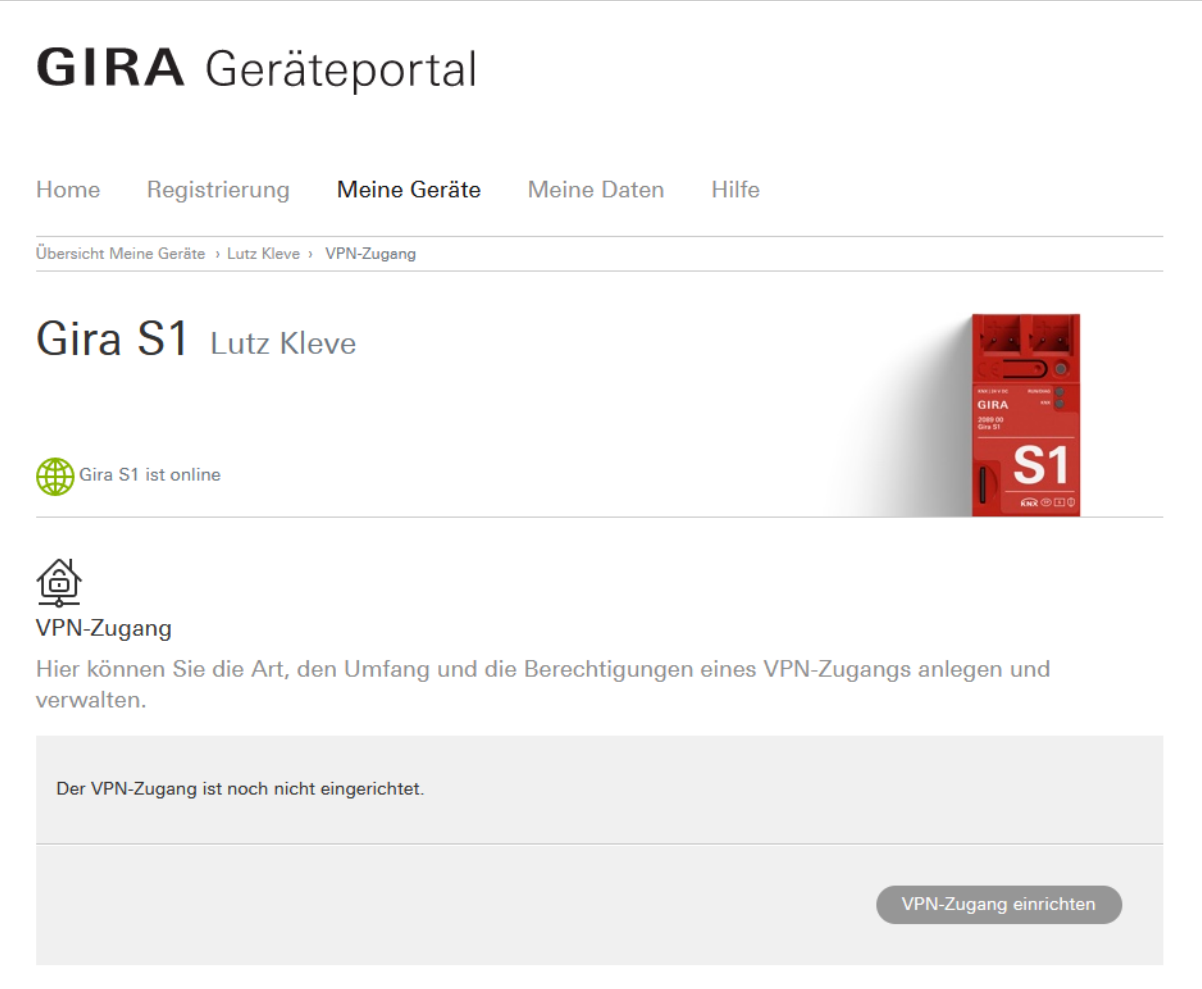


Bild 22: Gira Geräteportal – VPN-Zugang einrichten

Hinweis

Ändern Sie unter „VPN-Zugang“ die Eigenschaften, werden die aktuellen Konfigurationsdateien ungültig. Für jeden angelegten Benutzer wird eine neue Konfigurationsdatei erzeugt, welche Sie herunterladen und in den OpenVPN-Client des jeweiligen Benutzers importieren müssen.

10.11. FAQs

In der Ansicht „FAQs“ werden Ihnen die häufigsten Fragen zum Gira S1 und dessen Einstellungen im Gira Geräteportal beantwortet.

11. Gira S1 Windows Client

Der Gira S1 Windows Client ist eine Applikation, die auf einem PC installiert wird, mit dem sicher über das Internet auf Geräte im entfernten Netzwerk zugegriffen werden soll, falls nicht das HTTP Protokoll zum Einsatz kommt. Für Zugriff mit einem Internet Browser auf Webseiten im entfernten Netzwerk ist der Gira S1 Windows Client nicht erforderlich, siehe Kapitel 3.5 "Zugriff auf Webseiten im entfernten Netzwerk".

Die typischsten Anwendungsfälle für den Gira S1 Windows Client sind

- der Zugriff auf KNX Installationen über das KNX/IP oder das Eiblib/IP Protokoll und
- die Konfiguration eines Gira HomeServers mit dem Experten.

Darüber hinaus unterstützt der Gira S1 die Nutzung vieler weiterer TCP basierter IP-Protokolle wie z.B. das Remote Desktop Protocol (RDP) von Microsoft für den Fernzugriff auf einen Windows PC.

Der Gira S1 Windows Client ist derzeit für Microsoft Windows ab der Version 7 verfügbar. Sie finden die aktuelle Version www.download.gira.de

11.1. Installation

Starten Sie die Installation des Gira S1 Windows Clients, indem Sie einen Doppelklick auf die Installations-Datei ausführen. Im Laufe der Installation erscheint der folgende Dialog:

Bild 23: Installations-Dialog

Die Option „Trage Firewallausnahmen ein“ muss aktiviert bleiben, damit der Gira S1 Windows Client fehlerfrei funktioniert.

11.2. Verbindung zum Gira Geräteportal herstellen

Nach dem Start des Gira S1 Windows Client erscheint zunächst ein Anmeldedialog.

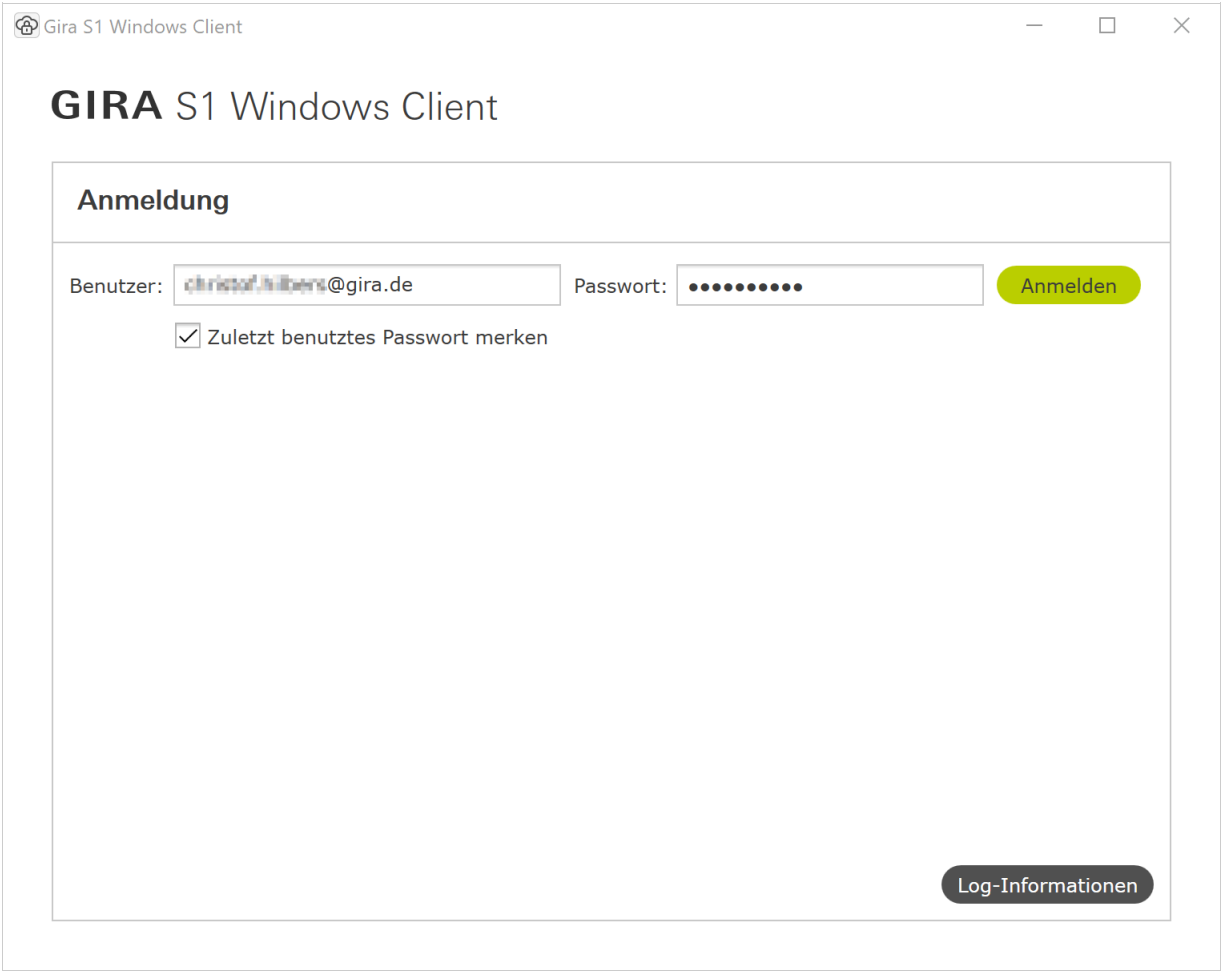


Bild 24: Anmeldung Gira S1 Client

Geben Sie hier mit den Anmeldedaten aus dem Gira Geräteportal an. Tragen Sie also Ihren Portal Benutzernamen (Hinweis: Es handelt sich hierbei immer um eine E-Mail-Adresse) und das zugehörige Passwort ein und klicken Sie auf „Anmelden“.

Zuletzt benutztes Passwort merken

Wenn Sie diese Option aktivieren, merkt sich der Gira S1 Windows Client das Passwort, so dass Sie beim nächsten Mal einfach auf „Anmelden“ klicken können, um sich am Geräteportal anzumelden.

Log-Informationen

Mit einem Klick auf die Schaltfläche „Log-Informationen“ öffnet sich ein Fenster, in dem Sie sich die bisher mitgeschriebene Log-Datei anschauen können. Mit einem Klick auf „Logfiles beim nächsten schließen löschen“ werden alle gespeicherten Log-Informationen beim Schließen des Gira S1 Windows Clients gelöscht. Mit einem Klick auf „ZIP-Archiv erzeugen“ werden die Log-Informationen in einem ZIP-Ordner gespeichert, der dann z.B: im Support-Fall an eine E-Mail angehängt werden kann. Für die Fehlersuche bei Problemfällen können Sie das „Erweiterte Logging“ aktivieren.

Nachdem Sie sich über die Schaltfläche „Anmelden“ beim Gira Geräteportal angemeldet haben, erscheint eine Liste mit allen Gira S1, für Sie Zugriffsrechte besitzen.

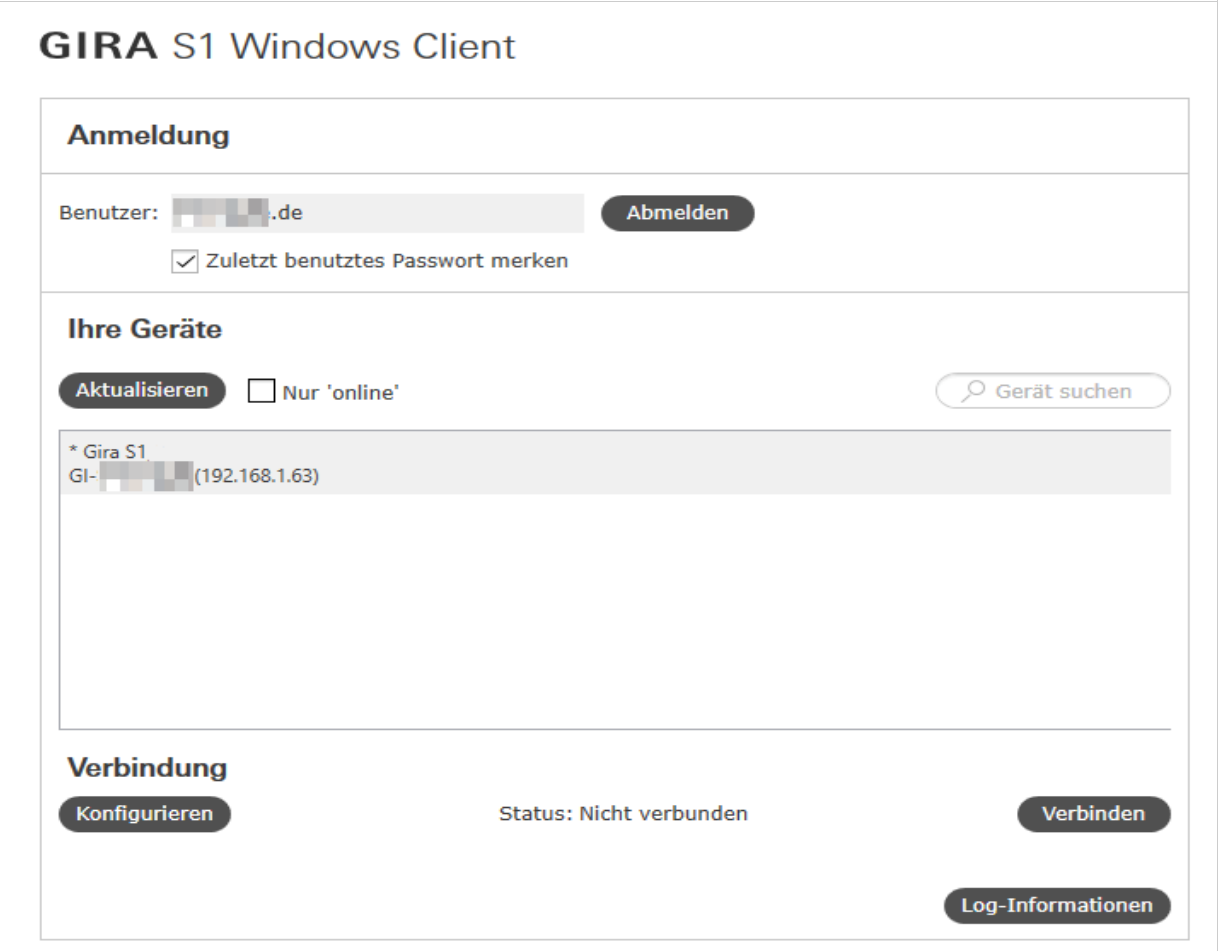


Bild 25: Anzeige der vorhandenen Gira S1

Verbindung aufbauen

Wenn Sie einen Gira S1 in der Liste auswählen, können Sie entweder auf „Verbinden“ klicken, um sich mit dem Gira S1 verbinden oder auf „Konfigurieren“ klicken, um die Konfiguration des Gira S1 zu ändern.

Wird der Gira S1 das erste Mal mit diesem Windows S1 Client benutzt, wird eine Default-Konfiguration erzeugt.

Nachdem Sie die Konfiguration ggf. auf Ihre Anwendungen angepasst haben (siehe Kapitel 11.3 "Konfiguration der Zugriffsoptionen eines Gira S1" ff.), können Sie die Verbindung über die Schaltfläche „Verbinden“ aufbauen.

Hinweis

Die über den Gira S1 Windows Client zur Verfügung gestellte Verbindung steht allen Teilnehmern zur Verfügung, die sich im selben Netzwerk befinden, wie der PC mit dem Gira S1 Windows Client. Bitte nutzen Sie den Gira S1 Windows Client daher nicht in öffentlichen Netzwerken.

Nur online

Wenn Sie die Option „Nur online“ aktivieren, werden in der Liste nur die Gira S1 angezeigt, die gerade Verbindung zum Internet haben, also „online“ sind.

11.3. Konfiguration der Zugriffsoptionen eines Gira S1

Wenn Sie sich mit dem Gira S1 verbunden haben, können Sie mit einem Klick auf „Konfigurieren“ die Zugriffsoptionen konfigurieren.
Neben dem HTTP Zugriff, für den kein Gira S1 Windows Client benötigt wird, ist die Standardanwendung des Gira S1 der sichere Fernzugriff auf KNX Installationen über das KNX/IP Protokoll. Deshalb ist die Konfiguration für diesen Dienst immer sichtbar und standardmäßig aktiviert.
Neben KNX/IP bietet der Gira S1 Windows Client auch den einfachen Zugriff für sichere Fernkonfigurationen des Gira HomeServers. Hier kann zum einen ein Projekt über den Gira HomeServer Experten aktualisiert werden, zum anderen über das Eiblib/IP Protokoll eine Busverbindung hergestellt werden. Weiter ist es auch möglich, direkte TCP Fernzugriff-Verbindungen zu nutzen, z.B. für das Microsoft Remote Desktop Protokoll (RDP).
Die Nutzung und damit auch Konfiguration des Zugriffs auf einen Gira HomeServer bzw. zusätzliche TCP Verbindungen ist optional und damit auch über die Einstellungen des jeweiligen Gira S1 (siehe Abbildung) an- bzw. abschaltbar.

Bild 26: Gira S1 Konfigurationsoptionen

Statusanzeige nach dem Starten der Fernzugriffs-Verbindung

Das Starten der sicheren Verbindung zum Gira S1 geschieht über die Schaltfläche „Verbinden“. Im Fehlerfall direkt beim Verbindungsaufbau wird eine entsprechende Fehlermeldung angezeigt.
Wird die Verbindung erfolgreich hergestellt, werden die Konfigurationsmöglichkeiten deaktiviert, da bei laufender Verbindung die Konfiguration nicht geändert werden kann. Während einer aktiven Verbindung kann mit einem Klick auf „Konfigurieren“ trotzdem der Konfigurationsdialog geöffnet werden. In diesem Fall wird für die drei Verbindungsarten KNX/IP, Gira HomeServer und TCP im Konfigurationsdialog eine Schaltfläche mit einer Infografik eingeblendet. Sollte es zu Fehlern bei einzelnen Verbindungen kommen, z.B. wenn kein einziges KNX/IP Gerät gefunden wurde oder eine TCP Verbindung nicht hergestellt werden konnte, so erscheint zusätzlich noch eine Schaltfläche mit einem Warndreieck. Die Schaltflächen haben alle Tooltips und zeigen darüber hinaus den Text auch in einem Eingabefeld an, wenn man sie betätigt.
Wichtiger Hinweis: Ein häufiges Problem ist eine Konfiguration, die einen lokalen Port nutzt, der bereits von einer anderen Anwendung genutzt ist. Wählen Sie in diesem Fall bitte einen anderen lokalen Port aus!

11.3.1. Zugriff auf eine KNX Installation über KNX/IP

Bild 27: KNX/IP Fernzugriffskonfiguration

Die Konfiguration für den sicheren KNX/IP Fernzugriff besteht aus drei Optionen:

KNX/IP Fernzugriff aktivieren
Der KNX/IP Zugriff kann grundsätzlich deaktiviert werden, wenn man z.B. nur schnell per Remote Desktop auf einen PC zugreifen will und kein KNX/IP benötigt.

Ausschließlich den Gira S1 für den KNX Zugriff benutzen
Falls gewünscht kann man, z.B. weil im entfernten Netzwerk viele Geräte vorhanden sind und man es eilig hat, auch nur den Tunneling Server des Gira S1 über Fernzugriff zugänglich machen.

Präfix für gefundene KNX/IP Geräte
Wenn der KNX/IP Zugriff erlaubt ist, werden standardmäßig alle im entfernten Netzwerk gefundenen KNX/IP Tunneling Server und KNX/IP Geräte, die den schnellen IP Download unterstützen (siehe ETS Optionen), auf dem PC mit der ETS bekannt gemacht, so dass diese im Connection Manager der ETS erscheinen. (Beachten Sie den Hinweis zur Nutzung mit ETS4 Versionen kleiner ETS4.2). Um auf einen Blick zu erkennen, welche Geräte über Fernzugriff angebunden sind, kann ein Präfix mit maximal acht Zeichen frei eingegeben werden.

Wichtiger Hinweis:
Bei der Benutzung von ETS4 Versionen älter als ETS4.2 können Probleme beim automatischen Erkennen der KNX/IP Interfaces in der ETS4 auftreten, so dass diese nicht erscheinen. In diesem müssen Fall müssen die Interfaces manuell in der ETS4 konfiguriert werden!
Hierzu erstellen Sie in der ETS4 manuell eine neue Verbindung, vergeben den Namen nach Ihren Wünschen und kopieren aus dem Gira S1 Windows Client die entsprechende IP Adresse und den Port in die Eingabefelder in der ETS4. Hierzu gibt der Gira S1 Windows Client bei geöffneter Verbindung Hilfestellung, in dem Schaltflächen angeboten werden, um die entsprechenden Werte in die Zwischenablage zu kopieren.
Beachten Sie hierzu die folgende Abbildung.

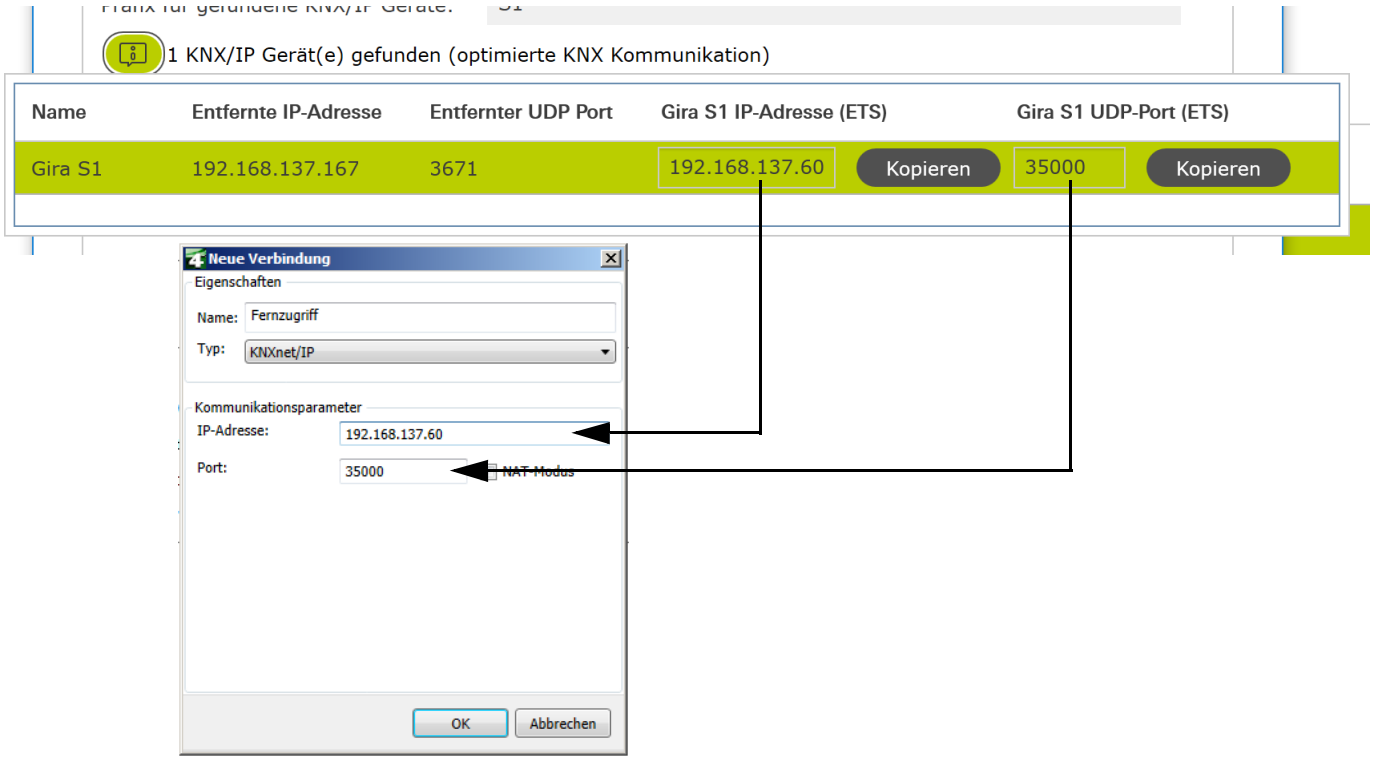


Bild 28: Manuelle KNX/IP Interfacekonfiguration für ETS kleiner ETS4.2.

Hinweis

Der Gira S1 Windows Client merkt sich für jeden Tunneling Server aus dem entfernten Netzwerk den lokal benutzten Port (ab 35000), so dass die manuell angelegten Verbindungen auch zu einem späteren Zeitpunkt bei einer erneuten Fernzugriffs-Verbindung zur gleichen Installation gültig bleiben.
Die Fernzugriff-Kommunikation ist speziell für die KNX Kommunikation optimiert, so dass diese auch bei langsamen Internetanbindungen noch zuverlässig funktioniert.

11.3.2. Fernkonfiguration Gira HomeServer und Nutzung von Eiblib/IP

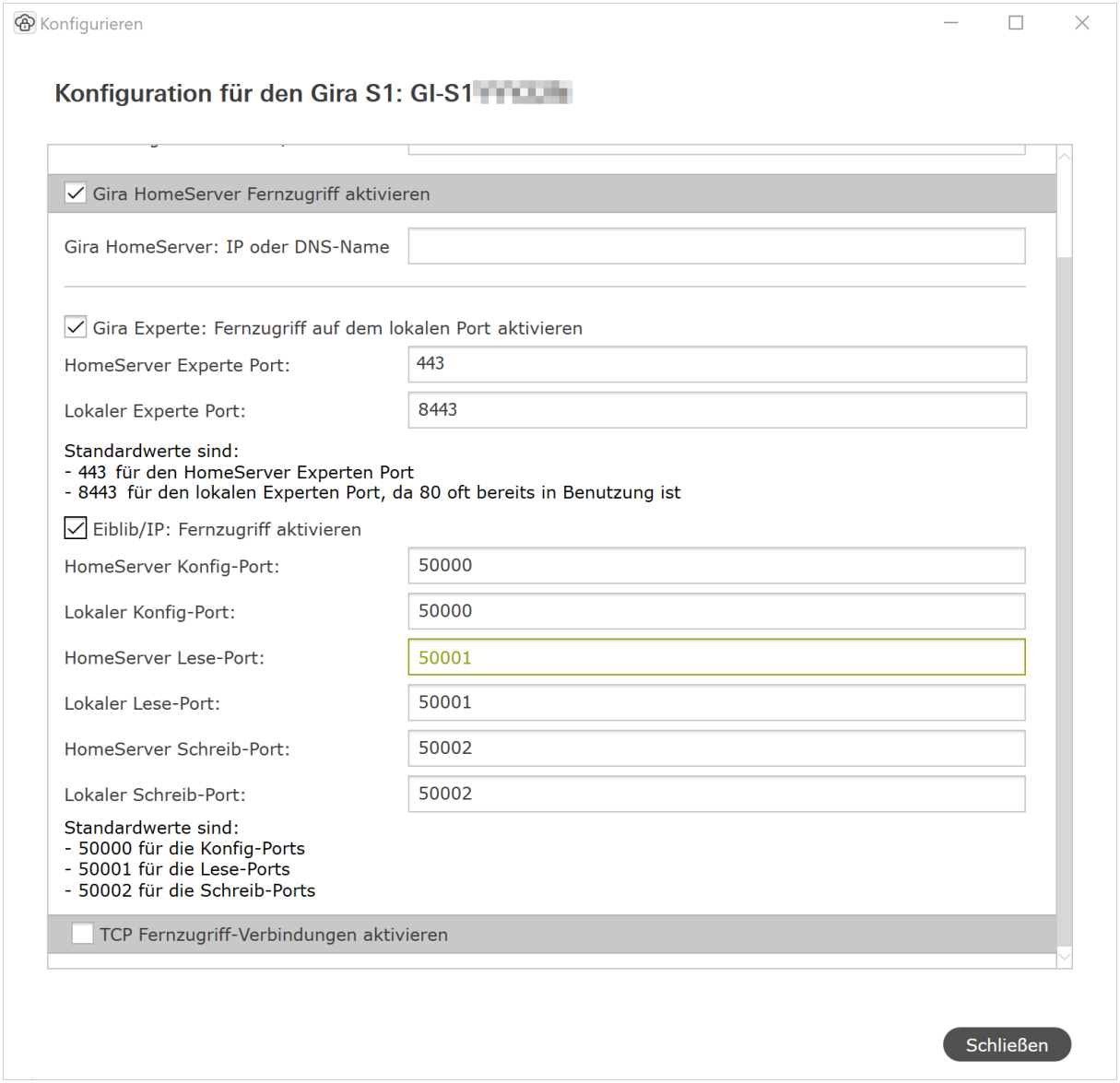


Bild 29: Gira HomeServer Fernzugriffskonfiguration.

Gira HomeServer IP oder DNS Name

Für den sicheren Fernzugriff auf dem Gira HomeServer muss hier die IP-Adresse oder der lokale DNS Name des Gira HomeServers in der Installation, also dem entfernten Netzwerk, eingegeben werden.

Gira Experte Fernzugriff auf dem lokalen Port 8443 aktiveren

Über diese Option besteht die Möglichkeit, den Fernzugriff für den Gira HomeServer Experten freizugeben. Wir empfehlen den Standardport 8443 zu nutzen. Es kann jedoch auch jeder andere freie Port genutzt werden, wobei die Ports kleiner 1000 nicht zu empfehlen sind.

Hinweis

Gira HomeServer ab Version 4.7.0 verwenden Port 443 für die Konfiguration; der Port ist als Standardwert gesetzt.

Um mit dem Experten über Fernzugriff den Gira HomeServer im entfernten Netzwerk laden zu können, müssen Sie im Experten im Dialog „Projekt übertragen“ mit aktiver Fernzugriff-Verbindung die Option „Andere Adresse“ auswählen und als IP Adresse immer die 127.0.0.1 eintragen, gefolgt vom konfigurierten Port (Standard ist 8443).

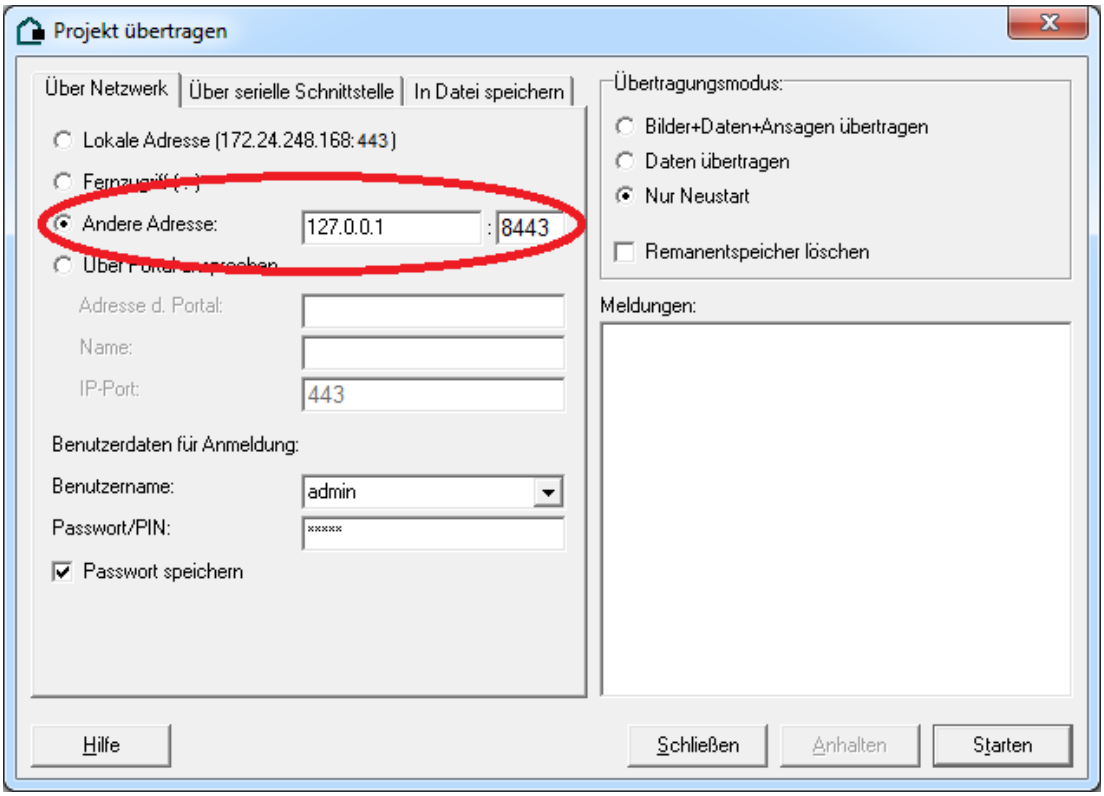


Bild 30: Projekt mit Experte über Fernzugriff übertragen.

Eibli/IP Fernzugriff aktivieren

Für das Eiblib/IP Protokoll werden standardmäßig die Ports 50000, 50001, 50002 genutzt, die üblicherweise auch auf dem lokalen PC frei sind, so dass hier Anpassungen i.d.R. nicht notwendig sind.

Für die Nutzung von Eiblib/IP mit dem Gira HomeServer müssen Sie wie gehabt in der ETS eine Verbindung vom Typ „Eiblib/IP“ anlegen. Wie schon beim Experten ist als Server-Adresse hier immer die 127.0.0.1 einzugeben. Die Ports können i.d.R. ihre Standardwerte (50000, 50001, 50002) behalten.

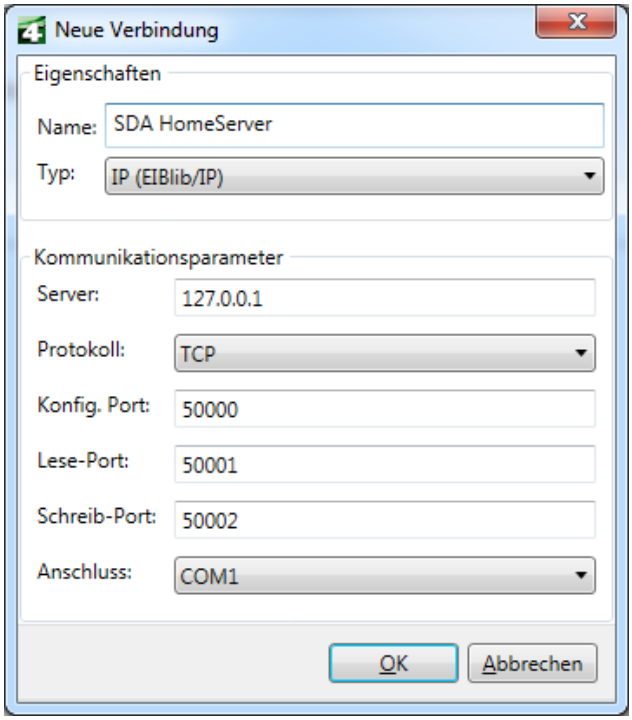


Bild 31: Gira HomeServer mit Eiblib/IP über Fernzugriff für KNX Anbindung nutzen.

11.3.3. Nutzung weitere TCP Protokolle über Fernzugriff

Über die Einstellungen bei „TCP Fernzugriff-Verbindungen“ können Sie weitere TCP basierte IP Protokolle über Fernzugriff nutzen. Klicken Sie dazu auf „Hinzufügen“ und tragen Sie die entsprechenden Werte für den Fernzugriff ein.

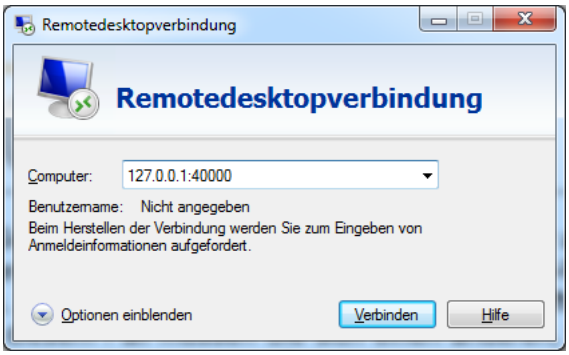
Recht bekannt ist z.B. das Microsoft Remote Desktop Protokoll (RDP), welches von der Microsoft Remote Desktop Verbindungsanwendung genutzt wird. Auch hier ist es i.d.R. der Fall, dass der Port bereits lokal vom PC benutzt wird, weshalb die Übersetzung auf einen Port notwendig ist, wie im Beispiel in der folgenden Abbildung.

Bild 32: TCP Fernzugriffskonfiguration.

Hinweis: Oft können Sie den TCP Port, der auf dem Gerät im entfernten Netzwerk angesprochen werden muss (im Beispiel hier 3389, der Standard-Port für RDP), auf Ihrem PC selbst nicht mehr verwenden, z.B. weil Sie auf Ihrem Rechner bereits Software installiert haben, die diesen Port bereits benutzt. In diesem Fall müssen Sie sich einen anderen, freien Port suchen. Hier hilft es z.B. Ports ab 40000 zu nutzen (wie in unserem Beispiel).

Wenn Sie nun eine Remotedesktopverbindung über Fernzugriff zu dem Zielrechner (in unserem Beispiel „Computername“) herstellen wollen, müssen Sie den Port noch extra angeben, wenn er nicht dem Standard-Port entspricht.

In unserem Beispiel kann die Verbindung wie folgt aufgebaut werden:



Hinweis: Es ist eine übliche Schreibweise für die explizite Angabe eines Ports (nur notwendig wenn nicht der Standard-Port), den Port mit einem vorangestellten „:“ direkt hinter den sog. Hostnamen zu schreiben. Bei HTTP z.B. http://127.0.0.1:40003/index.html.

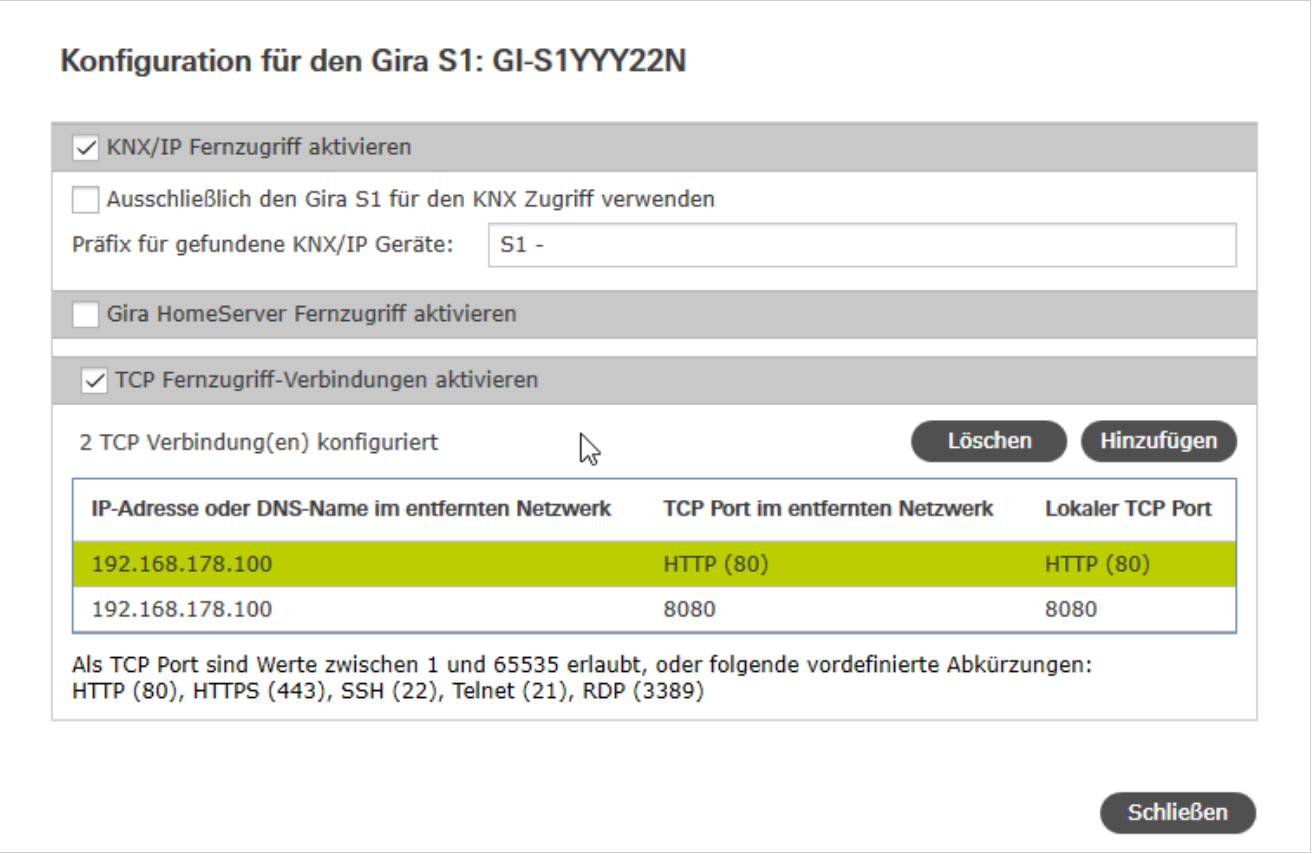
Auch Protokolle wie Telnet und SSH können problemlos über SDA genutzt werden.

11.3.4. Fernkonfiguration Gira TKS-IP-Gateway

Wenn Sie das Gira TKS-IP-Gateway über den Fernzugriff konfigurieren möchten, verwenden Sie bitte die Option „TCP Fernzugriff-Verbindungen aktivieren“.

Legen Sie bitte 2 Verbindungen mit den beiden Ports HTTP (80) und 8080 an. Als IP-Adresse tragen Sie jeweils die IP-Adresse des TKS-IP-Gateways ein.

Um den Assistenten des TKS-IP-Gateways aufzurufen, geben Sie anschließend bei bestehender Fernzugriffs-Verbindung zum Gira S1 die Adresse **http://localhost:80** in die Adresszeile Ihres Browsers ein.



11.4. Beenden einer Fernzugriffs-Verbindung

Nach erfolgter Nutzung beenden Sie eine aktive Verbindung durch die Schaltfläche „Trennen“. Außerdem wird die Verbindung automatisch geschlossen, wenn der Gira S1 Windows Client beendet wird.

12. Technische Daten

KNX Medium	TP1
Sicherheit	KNX Data Secure (X-Mode)
Inbetriebnahmemodus	S-Mode (ETS)
Versorgung KNX	DC 21…30 V SELV
Stromaufnahme KNX	typ. 2,5 mA
Anschluss KNX	Bus-Anschlussklemme
Externe Versorgung	
Spannung	DC 24...30 V
Leistungsaufnahme	2 W (bei DC24 V)
Anschluss	Anschlussklemme
IP-Kommunikation	Ethernet 10/100 BaseT (10/100 Mbit/s)
Anschluss IP	RJ45-Buchse
Unterstützte Protokolle	DHCP, AutoIP, TCP/IP, UDP/IP (Core, Tunneling, Device Management), ARP, ICMP, IGMP
Umgebungstemperatur	0 °C bis +45 °C
Lagertemperatur	-25 °C bis +70 °C
Einbaubreite	36 mm (2 TE)
microSD Karte	bis 32 GB (SDHC)

12.1. Zubehör

Zusatz-Spannungsversorgung
Bestell-Nr.: 1296 00

KNX Spannungsversorgung 320 mA
Bestell-Nr.: 1086 00

13. Häufig gestellte Fragen (FAQ)

- Wie finde ich die IP-Adresse meines Gira S1?
  Öffnen Sie dazu den Windows Explorer. Im Bereich „Netzwerk“ - „Andere Geräte“ wird der Gira S1 mit seiner IP-Adresse angezeigt.
- Wieviel Internet-Datenverkehr (Traffic) entsteht, wenn der Gira S1 mit dem Portal verbunden ist?
  Für das Aufrechterhalten der Verbindung entstehen ca. 400 Byte Datenverkehr/Minute. Dies entspricht ca. 560kB/Tag bzw. 16,5MB/Monat. Dieses Datenvolumen wird vom Gira Geräteportal nicht als Nutzdaten im Sinne der Begrenzung des Datenvolumens im Lizenzvertrag zum Gira S1 angerechnet.
- Welchen Kommunikationskanal benutzt der Gira S1 zum Gira Geräteportal?
  Der Gira S1 kommuniziert mit dem Gira Geräteportal ausschließlich über eine HTTPS Verbindung über den Standardport 443. Über diese eine Verbindung werden in beide Richtungen alle Daten ausgetauscht, so dass i.d.R. keine Konfiguration in der Firewall notwendig ist.
- Warum müssen Cookies aktiviert sein, um den Fernzugriff zu benutzen?
  Für die Absicherung der Zugriffe werden Cookies benutzt. Wir verwenden Cookies ausschließlich zur Sicherung der Verbindung. Es erfolgt kein Tracking oder Austausch mit Dritten!
- Mit welchen Protokollen kann auf Geräte im entfernten Netzwerk zugegriffen werden?
  Ohne Installation des Gira S1 Windows Clients können Sie auf Geräte im entfernten Netzwerk zugreifen, die per HTTP erreichbar sind. Das sind fast alle Geräte, die eine browserbasierte Benutzeroberfläche haben. Diese Geräte werden per UPnP automatisch gefunden.
  Mit dem Gira S1 Windows Client funktionieren neben KNX/IP und dem Gira HomeServer alle TCP-basierten Protokolle, z.B. telnet, ssh, HTTPS, Windows-Remotedesktop, ftp uvm.
- Warum melden die entsprechenden Kommunikationsobjekte bei der Nutzung des HTTP Zugriffs nach dem Schließen des Browsers nicht sofort, dass keine Verbindung mehr besteht?
  Ausführliche Beschreibung hierzu siehe Kapitel 8.6 "Objekttabelle".
- In meiner ETS4 erscheinen nicht automatisch die KNX/IP Schnittstellen, die über den Gira S1 Windows Client veröffentlich sind. Warum ist das so?
  Mit ETS4 Versionen älter als ETS4.2 kann es zu diesem Problem kommen (siehe Kapitel 11.3.1 "Zugriff auf eine KNX Installation über KNX/IP").
- Können die drei KNX/IP ETS Schnittstellen für Download, Gruppen und Busmonitor benutzt werden?
  Ja, die Schnittstellen unterstützen alle Downloadoperationen sowie den Gruppen- und Busmonitor.
- Ist die Gerätewebseite des Gira S1 auch über das Internet sicher erreichbar?
  Ja, die Statusseite des Geräts kann über das Internet gesichert abgerufen werden.
- Warum meldet die ETS beim Herunterladen des Applikationsprogramms den Fehler, dass auf einen geschützten Bereich nicht geschrieben werden kann?
  Bitte stellen Sie sicher, dass Ihre ETS-Version aktuell ist. Der Gira S1 benötigt die ETS ab Version 4.2 bzw. 5.0.2 oder höher.
  Prüfen Sie außerdem, ob die Versionen des Applikationsprogramms und der Gira S1 Firmware zueinander passen.
- Ist der Portalserver wirklich nötig?
  Ja, nur über einen Server lässt sich ein Fernzugriff realisieren, der so gut wie immer funktioniert und nicht aufwändig konfiguriert werden muss.
- Welche Daten speichert der Server?
  Der Server speichert nur die für die Erbringung des Dienstes absolut notwendigen Daten. Neben den bei der Anmeldung angegebenen Daten und über die Benutzeroberfläche einsehbaren Daten gehören dazu Informationen über die Menge und den Zeitpunkt des übertragenen Datenvolumens. Der Server speichert zu keiner Zeit Nutzdaten!

- Ist der Betrieb der Server innerhalb Deutschlands garantiert?
  Ja. Unsere Portal- sowie die Datenserver (zur gleichmäßigen Verteilung des Datenverkehrs) werden alle garantiert in Deutschland betrieben. Die Server werden zur Sicherung der hohen Verfügbarkeit bei seriösen Hosting-Providern als sog. Root Server gemietet, so dass kein Dritter unbefugten Zugriff auf den Server und die Daten hat. Durch den Betrieb in Deutschland greift das gegenüber anderen Ländern deutlich restriktivere deutsche Datenschutzgesetz.
- Warum schließt die Lizenz einen Dauerbetrieb (24x7) aus und enthält eine Datenvolumenbegrenzung?
  Da alle Daten über den Portalserver laufen müssen (s. o.), ist eine Dauernnutzung, insbesondere z.B. mit Videostreaming, sehr leistungsintensiv. Um grundsätzliche eine gute Performance zu garantieren sind daher gewisse Einschränkungen notwendig.
  Sollten Sie Anwendungsfälle haben, die über diese Bedingungen hinausgehen kontaktieren Sie uns bitte gerne. Lizenzmodelle mit erweitertem Umfang sind für die Zukunft nicht ausgeschlossen.
- Wenn eine Webseite über Fernzugriff aufrufen wird, funktioniert diese nicht richtig, obwohl sie lokal funktioniert. Was kann das sein?
  Nicht alle Webseiten können aus dem entfernten Netzwerk über Fernzugriff geladen werden. Insbesondere komplexere Seiten (z.B. mit Flash- oder intensiver Javascript-Nutzung) können ggf. nicht funktionieren.
- Ich habe einen partiellen Download mit der ETS4 durchgeführt und nun funktioniert die Gruppenkommunikation nicht. Warum?
  In der ETS4 gibt es einen Implementierungsfehler hinsichtlich des partiellen Downloads, der sich bei unserem Produkt bemerkbar macht. Bitte laden Sie mit der ETS4 das Gerät nie mit partiellem Download, sondern führen Sie immer einen Applikationsdownload durch. In der ETS5 existiert dieses Problem nicht.
- Warum sehe ich nach dem Entladen der Applikation auf der Gerätewebseite des Gira S1 noch die vorher konfigurierten physikalischen und IP Adresse?
  Die Gerätewebseite wird derzeit nach dem Entladen erst nach einem Geräteneustart aktualisiert.

14. Fehlersuche und Support

Der folgende Fehlerbaum soll versuchen, die häufigsten Probleme zu lösen.

Leuchtet die orange LED „KNX“ dauerhaft? Kurze unregelmäßige Unterbrechungen sind zulässig.

NEIN → Prüfen Sie die KNX Verkabelung und die LED-Statusanzeigen.

JA

Leuchtet die grüne LED „RUN/DIAG“ dauerhaft?

JA → Prüfen Sie die generelle Freigabe des Fernzugriffs über die KNX Kommunikationsobjekte 1 und 2.

NEIN

Blinkt die grüne LED „RUN/DIAG“ gleichmäßig und langsam mit 1Hz?

JA → Prüfen Sie die Geräteparametrierung in der ETS

NEIN

Ist das Gerät in der Windows-Netzwerkumgebung sichtbar?

NEIN → Prüfen Sie die Netzwerkverkabelung und die Parametrierung der IP-Adresse in der ETS.

JA

Wird das Gerät auf dem Gira Geräteportal als Online angezeigt?

NEIN → Prüfen Sie die Verbindung zum Internet. Falls Sie kein DHCP benutzen, überprüfen Sie den angegebenen DNS Server. Beachten Sie die Gerätewebseite für weitere Fehlerinformationen.

JA

OK

Prüfen Sie Konfiguration und Status der Benutzergruppen im Gira Geräteportal und auf der Gerätewebseite.

Starten Sie das Gerät über die Gerätewebseite neu.

15. Gira S1 Gerätewebseite

Auf der Gerätewebseite des Gira S1 werden alle Einstellungen und Parameter auf einen Blick angezeigt. Außerdem können Sie hier die Netzwerkeinstellungen ändern, eine Logdatei speichern, die Sie im Fehler- oder Servicefall an die Gira Hotline weitergeben können, einen Neustart und einen Werksreset auslösen sowie ein Firmwareupdate ausführen.
Die Gerätewebseite wird im Internetbrowser angezeigt.

Bild 33: Gerätewebseite Gira S1

Gerätewebseite aufrufen

Wenn Sie die IP-Adresse des Gira S1 kennen, können Sie die Gerätewebseite aufrufen, indem Sie die IP-Adresse in die Adresszeile eines Internetbrowser (Chrome, Firefox...) eingeben. Der PC muss sich dazu im gleichen Netzwerk befinden, wie der Gira S1.
Wenn Sie die IP-Adresse nicht kennen, öffnen Sie den Windows Explorer und klicken Sie dort auf „Netzwerk“. Im Bereich „Andere Geräte“ wird der Gira S1 angezeigt. Führen Sie einen Doppelklick auf das Symbol des Gira S1 aus, um die Gerätewebseite aufzurufen.

Passwort eingeben

Auf der sich öffnenden Webseite geben Sie bitte als Passwort die Registrierungs-ID des Gira S1 ein. Die Registrierungs-ID befindet sich auf einem Aufkleber am Gerät.

Zugangsdaten für die Diagnoseseite

Um die Diagnoseseite des Gira S1 zu öffnen, verwenden Sie bitte die folgenden Zugangsdaten:
Nutzername: device
Passwort: GPA Initial Device Password (befindet sich auf einem Aufkleber am Gerät)

16. Lizenzvereinbarung

Im Folgenden sind die Vertragsbedingungen für die Benutzung der Software durch Sie als dem „Lizenznehmer“ aufgeführt.

Durch Annahme dieser Vereinbarung und durch die Installation der Gira S1-Geräte-Software oder der Ingebrauchnahme eines „Gira S1-Gerätes“ schließen Sie einen Vertrag mit der Firma Gira, Giersiepen GmbH & Co KG und erklären sich an die Bestimmungen dieses Vertrages gebunden. Dies ist ausschließlich eine Lizenzvereinbarung und keine Vereinbarung über den Verkauf von Waren.

1. Definitionen

Lizenzgeber: Gira, Giersiepen GmbH & Co KG, Radevormwald, Deutschland

Lizenznehmer: Der rechtmäßige Empfänger der Gira S1-Geräte-Software.

Gira S1-Geräte: Der Begriff Gira S1-Geräte meint die Gira S1-Geräte, die jeweils aus einem Hardware-Gerät und der zugehörigen Firmware bestehen.

Firmware: Software, die auf dem Gira IP-Gerät eingebettet ist und zum Betrieb des selbigen dient.

Inbetriebnahme-Software: Die Inbetriebnahme-Software bezeichnet das Anwendungsprogramm, das zur Projektierung und Konfiguration der Gira S1-Geräte bereitgestellt wird.

Software von Dritten: Third Party IP

Dieses Produkt verwendet Software aus dritten Quellen, die im Rahmen der GNU General Public License (GPL), bzw. Lesser GNU General Public License LGPL verwendet werden, sowie im Rahmen der Berkeley Software Distribution (BSD) und der MIT Lizenz.

Die in diesem Produkt verwendeten Software-Pakete, die in den genannten Rahmen lizenziert sind, werden auf der Gerätewebseite in der Rubrik „Lizenzen“ beschrieben.

Die Lizenztexte der GPL und LGPL sind über die folgende Web-Seite verfügbar: http://www.gnu.org/licenses/licenses.html

2. Lizenzgegenstand

Gegenstand dieses Vertrages ist die auf dem Gira S1 bereitgestellte Software, sowie die zugehörige Dokumentation in schriftlicher oder elektronischer Form.

3. Rechte zur Nutzung der Gira S1-Software

Der Lizenzgeber räumt dem Lizenznehmer das nicht ausschließliche, zeitlich unbegrenzte und nicht übertragbare und nicht unterlizenzierbare Recht ein, die Firmware gemäß den Geschäftsbedingungen dieser Nutzungslizenz auf dem Gira S1-Gerät für die in der gültigen Fassung der Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) genannten Zwecke und Anwendungsbereiche zu nutzen.

Der Lizenznehmer verpflichtet sich sicherzustellen, dass jeder, der das Programm nutzt, dies nur im Rahmen dieser Lizenzvereinbarung durchführt und diese Lizenzvereinbarung einhält.

4. Beschränkung der Nutzungsrechte, Weitergabe an Dritte

4.1. Der Lizenznehmer ist nicht berechtigt, die Gira S1-Software ganz oder auszugsweise in anderer Weise als hierin beschrieben zu nutzen, zu kopieren, zu bearbeiten oder zu übertragen. Davon ausgenommen ist eine (1) Kopie, die vom Lizenznehmer ausschließlich für Archivierungs- und Sicherungszwecke angefertigt wird.

4.2. Der Lizenznehmer ist nicht berechtigt, Reverse-Engineering Techniken auf die Gira S1-Software anzuwenden oder die Gira S1-Software in eine andere Form umzuwandeln. Zu solchen Techniken gehören insbesondere das disassemblieren (Umwandlung binär kodierter Maschinenbefehle eines ausführbaren Programmes in eine für Menschen lesbarere Assemblersprache) oder dekompilieren (Umwandlung binär kodierter Maschinenbefehle oder Assemblerbefehle in Quellcode in Form von Hochsprachenbefehlen).

4.3 Die Lizenz für Gira S1-Software ist an die Nutzung des Gira S1-Geräts gebunden. Eine Weitergabe der Gira S1-Software an Dritte oder ein zugänglich machen der Software für Dritte ist nur in Verbindung mit der Weitergabe der Gira S1-Geräte zulässig.

Bei Weitergabe an einen Dritten erlischt das Recht des Lizenznehmers zur eigenen Nutzung.

Der Lizenznehmer darf die Software und alle zur Nutzung der Software erforderlichen Lizenzschlüssel mit Ausnahme von entsprechend gekennzeichneter Software nur an Dritte weitergeben, wenn

4.3.1 der Lizenznehmer etwaige Sicherungskopien sowie die zur Nutzung der Software erforderlichen Lizenzschlüssel von seinem System durch Löschung und/oder Deinstallation entfernt.

4.3.2 der Dritte sich vor der Weitergabe und Nutzung zur Einhaltung dieser Nutzungsbedingungen gegenüber Gira verpflichtet.

Der Lizenznehmer wird den Dritten vor Weitergabe des Gira S1-Gerätes auf diese Nutzungsbedingungen ausdrücklich hinweisen.

4.4. Der Lizenznehmer ist nicht berechtigt, die Gira S1-Software zu vermieten, zu verleasen oder Unterlizenzen an dem Programm zu erteilen.

4.5. Der Lizenznehmer benötigt eine schriftliche Genehmigung des Lizenzgebers, um Software zu erstellen und zu vertreiben, die von der Gira S1-Software abgeleitet ist.

4.6. Die Mechanismen des Lizenzmanagements und des Kopierschutzes der Gira S1-Software dürfen nicht analysiert, nicht publiziert, nicht umgangen und nicht außer Funktion gesetzt werden.

5. Eigentum, Geheimhaltung

5.1. Die Gira S1-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) und jegliche Änderung hieran sind und bleiben Eigentum des Lizenzgebers. Der Lizenzgeber behält auch alle weiteren Rechte und Anteile an dem Lizenzgegenstand. Der Lizenznehmer wird diese Rechte beachten.

5.2. Der Lizenzgegenstand, d.h. weder die Software, noch die Datensicherungskopie, noch die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) darf nicht –weder ganz oder in Teilen, weder entgeltlich noch unentgeltlich- an Dritte weitergegeben werden. Der Lizenznehmer stimmt zu, den Lizenzgegenstand ausschließlich zum Zwecke der Rechtsausübung unter dieser Nutzungslizenz zu verwenden.

6. Änderungen

Der Lizenzgeber darf den Lizenzgegenstand jederzeit ohne Ankündigung erweitern, verbessern oder anderweitig abändern. Die Lizenzenzbedingungen gelten entsprechend fort.

7. Gewährleistung

Die Gira S1-Software wird zusammen mit der Software von Dritten ausgeliefert, die im Abschnitt 1 aufgelistet ist. Für die Software Dritter wird keinerlei Gewährleistung übernommen.

Bezüglich der Lizenzbedingungen für diese Software verweisen wir auf die unter Abschnitt 1 angegebenen Links (URLs). Diese Bedingungen werden mit in diesen Vertrag einbezogen.

Der Lizenzgeber wird dem Lizenznehmer innerhalb von 36 Monaten nach Auslieferung der Software auf Anfrage den vollständigen, maschinenlesbaren Source Code der unter Punkt 1 gelisteten Drittsoftware (Open Source Software) zur Verfügung stellen. Hierfür wird der Lizenzgeber dem Lizenznehmer die Versandkosten in Rechnung stellen.

7.1 Die Gira S1-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) werden dem Lizenznehmer in der jeweils gültigen Fassung zur Verfügung gestellt. Die Gewährleistungszeit für die Gira S1-Software beträgt 24 Monate. Während dieser Zeit leistet der Lizenzgeber wie folgt Gewähr:

- Die Software ist bei Übergabe frei von Material- und Herstellungsfehlern.
- Die Software arbeitet gemäß der ihr beigefügten Dokumentation in der jeweils gültigen Fassung.
- Die Software ist auf den vom Lizenzgeber genannten Computer-Stationen ablauffähig.

Die Erfüllung der Gewährleistung erfolgt ausschließlich durch Ersatzlieferung.

7.2 Im Übrigen wird für die Fehlerfreiheit der Gira S1-Software und ihrer Datenstrukturen keine Gewährleistung übernommen. Die Gewährleistung erstreckt sich auch nicht auf Mängel, die auf unsachgemäße Behandlung oder andere Ursachen außerhalb des Einflussbereiches des Lizenzgebers zurückzuführen sind. Weitere Gewährleistungsansprüche sind damit ausgeschlossen.

8. Haftung

Der Lizenzgeber ist nicht haftbar für Schäden aus entgangenem Gewinn, aus Verlust von Daten oder aus anderem finanziellen Verlust, die im Rahmen der Benutzung der Gira S1- Software entstehen.

Diese Haftungsbeschränkung gilt für alle Schadensersatzansprüche des Lizenznehmers, gleich aus welchem Rechtsgrund. Die Haftung ist der Höhe nach auf den Kaufpreis des Produkts beschränkt.

Der Haftungsausschluss gilt nicht für Schäden, die durch Vorsatz oder grobe Fahrlässigkeit vom Lizenzgeber verursacht wurden. Unberührt von dem Haftungsausschluss bleiben auch Ansprüche des Lizenznehmers, die auf den gesetzlichen Vorschriften zur Produkthaftung beruhen.

9. Datenschutz

Durch Abschluss dieses Lizenzvertrages stimmen Sie der Geltung der GIRA Datenschutzhinweise in ihrer jeweils gültigen Fassung zu. Siehe http://www.gira.de/impressum/datenschutz.html

10. Anwendbares Recht und Gerichtsstand

Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter ausdrücklichem Ausschluss des UN-Kaufrechtabkommens.

Gerichtsstand ist das für den Sitz des Lizenzgebers zuständige Gericht.

11. Beendigung

Dieser Vertrag und die darin gewährten Rechte enden, wenn der Lizenznehmer eine oder mehrere Bestimmungen dieses Vertrages nicht erfüllt oder diesen Vertrag schriftlich kündigt. Die übergebene Gira S1-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) einschließlich aller Kopien sind in diesem Falle unverzüglich und unaufgefordert vollständig zurückzugeben. Ein Anspruch auf Rückerstattung des bezahlten Preises ist in diesem Falle ausgeschlossen.

Mit Beendigung des Vertrages erlischt die Lizenz zur Nutzung der Gira S1-Software. Die Gira S1-Geräte müssen in diesem Fall außer Betrieb genommen werden. Eine weitere Nutzung der Gira S1-Geräte ohne Lizenz ist ausgeschlossen.

12. Nebenabreden und Vertragsänderungen

Nebenabreden und Vertragsänderungen bedürfen zu ihrer Gültigkeit der Schriftform.

13. Ausnahme

Alle Rechte die nicht ausdrücklich in diesem Vertrag erwähnt werden, sind vorbehalten.

17. GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-rea-

dable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many peo-

ple have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

18. OpenSSL Lizenzen

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

18.1. OpenSSL License

/* ==

* Copyright (c) 1998-2011 The OpenSSL Project.All rights reserved.

*

* Redistribution and use in source and binary forms, with or without modification,

* are permitted provided that the following conditions are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright notice,

* this list of conditions and the following disclaimer in the documentation

* and/or other materials provided with the distribution.

*

* 3. All advertising materials mentioning features or use of this software must

* display the following acknowledgment: "This product includes software developed

* by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

*

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse

* or promote products derived from this software without prior written permission.

* For written permission, please contact openssl-core@openssl.org.

*

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL"

* appear in their names without prior written permission of the OpenSSL Project.

*

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project

* for use in the OpenSSL Toolkit (http://www.openssl.org/)"

*

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY

* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

* PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS

* CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

* EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

* PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

* PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF

* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE

* OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF

* ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

```
* ====================================================================
*
*     This product includes cryptographic software written by Eric Young
*     (eay@cryptsoft.com).This product includes software written by Tim
*     Hudson (tjh@cryptsoft.com).
*
*/
```

18.2. Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
*     All rights reserved.
*
*     This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
*     The implementation was written so as to conform with Netscapes SSL.
*
*     This library is free for commercial and non-commercial use as long as the following
*     conditions are aheared to.The following conditions apply to all code found in this
*     distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code.
*     The SSL documentation included with this distribution is covered by the same copyright
*     terms except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
*     Copyright remains Eric Young's, and as such any Copyright notices in the code are not
*     to be removed. If this package is used in a product, Eric Young should be given attribution
*     as the author of the parts of the library used. This can be in the form of a textual message
*     at program startup or in documentation (online or textual) provided with the package.
*
*     Redistribution and use in source and binary forms, with or without modification,
*     are permitted provided that the following conditions are met:
*     1. Redistributions of source code must retain the copyright notice, this list of
*      conditions and the following disclaimer.
*     2. Redistributions in binary form must reproduce the above copyright notice, this list of
*     conditions and the following disclaimer in the documentation and/or other materials provided
*     with the distribution.
*     3. All advertising materials mentioning features or use of this software must display the
*     following acknowledgement: "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)". The word 'cryptographic' can be left out
*     if the rouines from the library being used are not cryptographic related :-).
*     4. If you include any Windows specific code (or a derivative thereof) from
*     the apps directory (application code) you must include an acknowledgement:
*     "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
*     THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR
*     IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
*     MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
*     IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
*     INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
*     BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
*     USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
*     THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
```

```
*     NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
*     EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
*     The licence and distribution terms for any publically available version or
*     derivative of this code cannot be changed.i.e. this code cannot simply be
*     copied and put under another distribution licence

*     [including the GNU Public Licence.]
*/
```