Stand der Dokumentation:

04.07.2018

Produkthandbuch
ISE SMART CONNECT KNX REMOTE ACCESS

Best.-Nr. 1-0003-004

Gültig für Applikations-Software v4.1, Firmwareversion v4.0 und SDA Client v1.6

Inhaltsverzeichnis

1 Produktbeschreibung

1.1 Funktionen

- Sichere Datenübertragung von jedem Ort in der Welt über das Internet in Ihr zu Hause vom ersten Datenpaket an dank sicherem Portalserver https://securedeviceaccess.net
- Zugriff auf die HTML-Seiten von jedem Netzwerk-Endgerät (z.B. Kamera) – als ob man zuhause wäre
- KNX-Kommunikation mit der ETS per KNXnet/IP, IP-Direkt-Download und Eiblib/IP über den SDA Client für Windows
- Konfigurationszugriff auf Gira HomeServer mit dem HomeServer Experten über den SDA Client für Windows
- Zugriff auf Windows Rechner über die Remotedesktopverbindung über den SDA Client für Windows
- Viele weitere Anwendungsfälle über frei konfigurierbare TCP Portweiterleitungen über den SDA Client für Windows
- Benachrichtigungen können über KNX Telegramme ausgelöst, auf dem Server gespeichert und z.B. per E-Mail, Sprachanruf oder SMS weitergeleitet werden.
- KNX/TP Anschluss mit integriertem IP Interface (Tunneling Server) für den KNX Zugriff über die ETS oder andere Software, maximal drei gleichzeitige Verbindungen, für die Nutzung des Downloads, des Gruppen- und auch Busmonitors
- Statussignalisierung und Zugriffsmanagement der gesicherten Verbindungen über KNX Kommunikationsobjekte
- Zugriff funktioniert auch wenn der Internetzugang nicht über eine eindeutige Internet IP-Adresse verfügt, wie z.B. bei UMTS oder LTE üblich
- konfigurationsfrei bei Nutzung von DHCP
- Ein integrierter Ethernet Switch (zwei RJ45 Anschlüsse) vereinfacht die Verbindung mehrerer IP-Geräte. Dadurch können mehrere ISE SMART CONNECT KNX REMOTE ACCESS oder auch andere IP-Geräte in der Verteilung ohne Zuhilfenahme anderer aktiver Komponenten verbunden werden.
- Unterstützt beschleunigte Übertragung von der ETS zum ISE SMART CONNECT KNX REMOTE ACCESS oder anderen KNXnet/IP Geräten über direkte KNX-IP Verbindung.
- Die Konfiguration des ISE SMART CONNECT KNX REMOTE ACCESS erfolgt über die die jeweils aktuellste Version der ETS4 oder ETS5. Die Applikation greift auf ETS-Funktionen zu, die von früheren ETS-Versionen nicht unterstützt werden. Die Konfiguration mit älteren ETS-Versionen ist somit nicht möglich.

1.2 KNX Secure Ready

ISE SMART CONNECT KNX REMOTE ACCESS ist für KNX Secure vorbereitet. Die dazu notwendigen FDSK (Factory Default Setup Key, Fabrikschlüssel) befinden sich seitlich als Aufkleber auf dem Gerät und liegen zusätzlich dem Gerät bei. Geräte ohne diese Aufkleber sind nicht „Secure Ready“.

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

Die FDSK können Sie selbst nicht wiederherstellen.

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

1.3 Wie funktioniert Secure Device Access?

Dieser Abschnitt beschreibt die Funktionsweise der Secure Device Access Infrastruktur (Abkürzung SDA). Er stellt Ihnen die Komponenten vor, aus denen „Secure Device Access“ besteht und beschreibt, wie diese Komponenten zusammenarbeiten, damit Sie einfach und sicher von überall auf Ihr Zuhause zugreifen können.

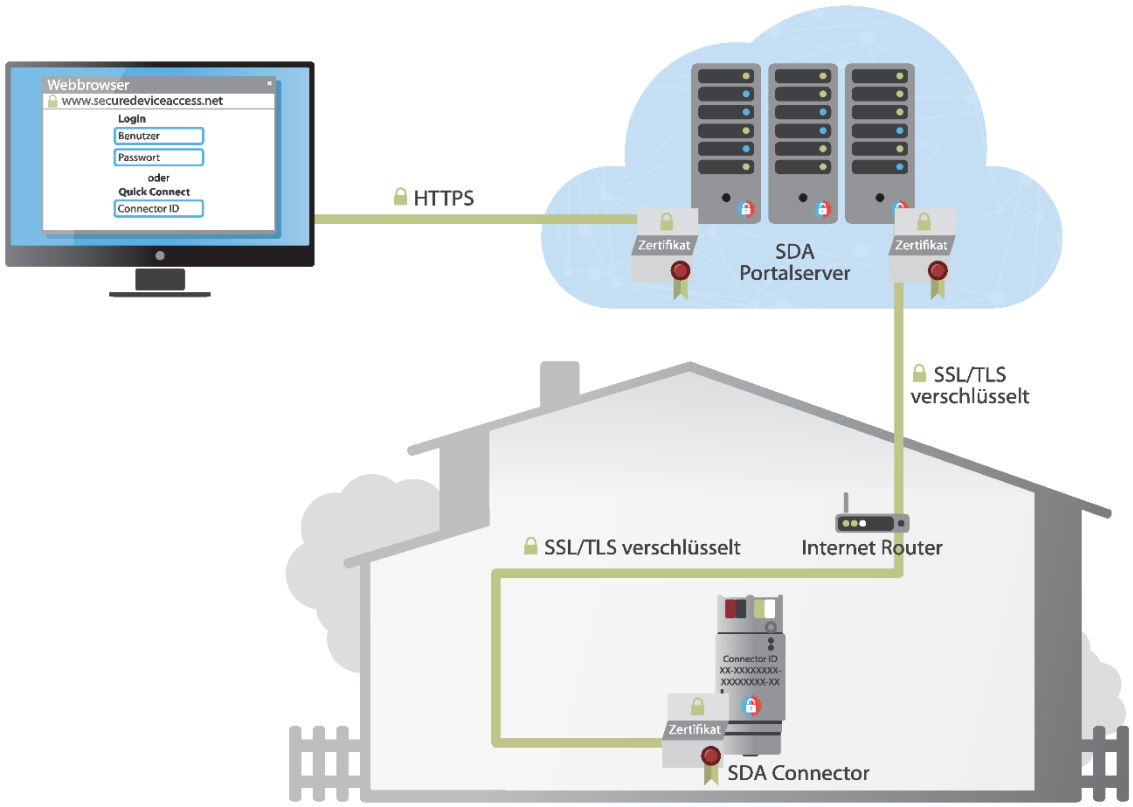


Abbildung 1: Übersicht über den sicheren Zugriff mit „Secure Device Access“

1.3.1 ISE SMART CONNECT KNX REMOTE ACCESS, allgemein „SDA Connector”

Der ISE SMART CONNECT KNX REMOTE ACCESS (im Folgenden „SDA Connector“ genannt) ist das Gerät, dessen Anleitung Sie gerade lesen. Es wird bei Ihnen zuhause installiert und macht Ihr Heimnetzwerk bereit für den sicheren Zugriff über das Internet.

Der SDA Connector wird einfach per Ethernet an das Heimnetzwerk angeschlossen. Er verbindet sich sodann automatisch über Ihren vorhandenen Internetzugang mit dem SDA Portalserver. Die Kommunikation zwischen SDA Connector und SDA Portalserver ist per AES verschlüsselt und mit digitalen Zertifikaten gesichert (Details siehe Abschnitt 1.3.4 „HTTPS-Proxy http-paccess.net“).

Über die Ethernet-Verbindung zum Heimnetzwerk können Sie jetzt bereits auf fast alle Ihre Netzwerk-Geräte über das Internet zugreifen. Abhängig von den vom jeweiligen Gerät unterstützten Netzwerkprotokollen erfolgt der Zugriff direkt über den SDA Portalserver oder über die für verschiedene Plattformen verfügbare Clientsoftware „SDA Client“ (siehe Abschnitt 1.3.7 „Clientsoftware (SDA Client)“.

Falls Sie in Ihrem Haus eine KNX-Installation haben, können Sie diese optional über den KNX Anschluss mit dem ISE SMART CONNECT KNX REMOTE ACCESS verbinden. Dadurch können Sie – oder Ihr Elektroinstallateur - von überall z.B. mit der ETS auf Ihre KNX-Geräte zugreifen.

1.3.2 Quick Connect

Jeder SDA Connector ist werksseitig mit einer eindeutigen kryptografisch sicheren „Registrierungs-ID“ (früher Connector ID genannt) versehen. Die Registrierungs-ID ist auf dem SDA Connector aufgedruckt und über ein digitales Zertifikat mit dem konkreten Gerät verbunden.

Mittels der Registrierungs-ID können Sie sofort nach dem Auspacken und Anschließen ohne weitere Anmeldung auf Ihre Endgeräte zugreifen.

Die Registrierungs-ID hat einen zufälligen Anteil und kann daher nicht geraten werden. Jeder, der die Registrierungs-ID Ihres SDA Connectors kennt, kann auf Ihre Geräte zugreifen. Je nach Anwendungsfall kann das ein Vorteil oder ein Nachteil sein.

Um den Zugriff per Quick Connect zu verhindern, können Sie jederzeit Ihren SDA Connector mit einem Konto auf dem SDA Portalserver verbinden. Danach ist kein Zugriff mehr per Quick Connect möglich, es sei denn, Sie schalten diesen explizit wieder frei.

1.3.3 SDA Portalserver

Über den Portalserver (erreichbar unter https://securedeviceaccess.net) verwalten Sie Ihren SDA Connector. Über den Portalserver können Sie auch weiteren Benutzern Zugriff auf Ihren SDA Connector und damit auf Ihre KNX- und Netzwerkgeräte gewähren.

Einem Konto auf dem Portalserver können beliebig viele SDA Connectoren zugeordnet werden.

Wenn Sie oder von Ihnen autorisierte Personen auf Endgeräte in Ihrem Gebäude zugreifen möchten, ist daran immer der Portalserver als Vermittlungsstelle beteiligt. Der Portalserver speichert die übertragenen Daten nicht, sondern leitet diese nur weiter.

Wir betreiben den Server in Deutschland unter Einhaltung der strengen europäischen Datenschutzrichtlinien.

Hinweis: Die Benutzung des SDA Portalservers erfordert aus technischen Gründen die Nutzung von Cookies im Internet Browser.

1.3.4 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 häufigen Fall ist der Zugriff über den SDA Portalserver besonders einfach. Jedes über einen SDA Connector 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.

Selbstverständlich ist auch hier die komplette Kommunikation über das Internet verschlüsselt und es erfolgt eine Benutzerauthentifizierung gemäß der für Ihren SDA Connector auf dem Portalserver eingestellten Zugriffsfreigaben.

Damit Sie sich keine Links merken müssen, verwaltet der SDA Portalserver für Sie eine Linkliste der Endgeräte, die über httpaccess.net erreichbar sind. Wenn das Netzwerkgerät – wie häufig der Fall – UPnP unterstützt, kann es der Portalserver automatisch in die Linkliste eintragen.

1.3.5 Kommunikation – sicher, zuverlässig und einfach zu handhaben

Das SDA Connector verwendet für die Kommunikation mit dem Portalserver die weit verbreiteten Standardprotokolle HTTPS, TLS/SSL und Websockets.

Alle Daten werden per AES verschlüsselt. Es wird kein einziges Bit Ihrer Daten unverschlüsselt übertragen.

SDA Connector und SDA Portalserver authentifizieren sich gegenseitig mit digitalen Zertifikaten und RSA-Schlüsselpaaren. Die Zertifikate sind von unserer eigenen Zertifizierungsstelle ausgestellt. So sind wir immun gegen die immer wieder auftauchenden gefälschten Zertifikate einer der weltweit tausenden von Zertifizierungsstellen.

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

Für Sie hat das den Vorteil, dass der SDA Connector ohne komplizierte Konfiguration einfach funktioniert. Auspacken, Anschließen, fertig. Das ist ein deutlicher Vorteil gegenüber anderen Ansätzen zum sicheren Fernzugriff wie VPN oder SSH-Tunneling.

Secure Device Access funktioniert im Unterschied zu anderen Lösungen sogar über einen Mobilfunkzugang, auch wenn dieser nicht über eine eindeutige von außen erreichbarer IP-Adresse verfügt.

1.3.6 SDA Benachrichtigungen

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

Diese Benachrichten können konfigurierbar per E-Mail, Telefon oder SMS weitergeleitet werden.

1.3.7 Clientsoftware (SDA Client)

Die SDA Clientsoftware (im folgenden SDA Client) installieren Sie auf Ihrem Windows PC. Über den SDA Client erhalten andere auf Ihrem PC laufende Anwendungen Zugriff auf Ihre Geräte ohne selbst das SDA-Protokoll unterstützen zu müssen.

Der SDA Client ist derzeit für Windows verfügbar. Andere Plattformen werden folgen.

Der SDA Client baut über den SDA Portalserver eine verschlüsselte Verbindung zum SDA Connector auf. Diese Verbindung wird anderen Anwendungen auf Ihrem PC und in Ihrem lokalen Netzwerk bereitgestellt, damit diese auf Geräte im entfernten Netzwerk zugreifen können.

Je nach Anwendungsfall wird der FDSK für die erste Authentifizierung in der ETS benötigt oder für die Verschlüsselung der Kommunikation.

Beispiele:

- Mit der ETS können Sie per KNXnet/IP KNX-Geräte konfigurieren.
- Mit dem Gira HomeServer Experten können Sie einen 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.

1.4 Definitionen und Begriffsklärungen

Connector ID

Alte Bezeichnung für Registrierungs-ID (lange oder vollständige Connector ID) oder Fernzugriffs-ID (kurze Connector ID).

Secure Device Access, SDA

Bezeichnet das komplette System, welches den sicheren Zugriff über das Internet auf Ihr Zuhause bereitstellt. Siehe Abschnitt 1.3 „Wie funktioniert Secure Device Access?".

Portalserver, SDA Portalserver

Zentraler Server der Secure Device Access Infrastruktur im Internet. Erreichbar unter https://securedeviceaccess.net. Über diesen Server verwalten Sie den Zugriff auf Ihre SDA Connectoren. Siehe Abschnitt 1.3.3 „SDA Portalserver".

SDA Connector, ISE SMART CONNECT KNX REMOTE ACCESS

Der SDA Connector ist ein kleines elektronisches Gerät, das an Ihr Heimnetzwerk angeschlossen wird und dieses mit dem Portalserver verbindet. Siehe Abschnitt 1.3.1 „ISE SMART CONNECT KNX REMOTE ACCESS, allgemein „SDA Connector"".

Registrierungs-ID

Jeder SDA Connector hat eine eindeutige Registrierungs-ID (früher Connector ID genannt), welche auf dem Gerät aufgedruckt ist. Diese Registrierungs-ID dient folgenden Zwecken:

- Sicherer Zugriff ohne Portalanmeldung (Quick Connect)
- Verknüpfung eines SDA Connectors mit einem Portalkonto

Die Registrierungs-ID ist zufällig und kann nicht geraten werden.

Fernzugriffs-ID

Jeder SDA Connector hat eine eindeutige Registrierungs-ID, welche auf dem Gerät aufgedruckt ist. Diese Registrierungs-ID besteht aus vier Blöcken, getrennt durch einen Bindestrich. Innerhalb der Konfiguration beispielsweise im SDA oder im Gira Projekt Assistent (GPA) wird eine verkürzte Variante der Registrierungs-ID angezeigt. Diese verkürzte Variante wird Fernzugriffs-ID genannt und besteht nur aus den ersten beiden Blöcken.

Quick Connect

Zugriff auf Geräte hinter einem SDA Connector ohne Portalanmeldung, nur durch Eingabe der Registrierungs-ID. Siehe Abschnitt 1.3.2. „Quick Connect". Der Quick Connect ist das Gegenstück zum Portal Connect.

Portal Connect

Zugriff auf Geräte hinter einem SDA Connector mit Portalanmeldung. Siehe Abschnitt 1.3.3. „SDA Portalserver“. Der Portal Connect ist das Gegenstück zum Quick Connect.

SDA Client

PC-Software, die anderen Anwendungen die Kommunikation über SDA erlaubt, ohne dass diese etwas über SDA wissen müssen.

Gerät, Netzwerkgerät

Ein in Ihrem Zuhause eingebautes Gerät mit Netzwerk oder KNX-Anschluss, auf das über SDA zugegriffen werden soll.

SDA Benachrichtigungen

Ein Nachrichtensystem, welches über Systemereignisse (z.B. An-/Abmelden eines SDA Connectors am Portal) oder KNX Gruppenobjekte generierte Nachrichten speichert und auf Wunsch z.B. über E-Mail, Telefon oder SMS weiterleitet.

httpaccess.net

Teil des SDA Portalservers für den konfigurationsfreien Zugriff auf Geräte, die einen integrierten Webserver haben.

Username

Benutzername für die Anmeldung am Portalserver. Der für SDA verwendete Benutzername ist immer eine E-Mail-Adresse.

Passwort

Zu einem Benutzernamen gehörendes Passwort für die Authentifizierung gegenüber dem SDA Portalserver.

Zugriffsgruppe

Sie können über den SDA Portalserver Ihren SDA Connector für andere Personen freigeben. Diese Personen können Sie den Zugriffsgruppen „Bewohner“ und „Installateur“ zuordnen. Über KNX-Taster können Sie den Zugriff nach Zugriffsgruppen getrennt erlauben oder verbieten.

Installateur

Zugriffsgruppe für externe Dienstleister. Der Zugriff für diese Gruppe ist standardmäßig gesperrt.

Bewohner

Zugriffsgruppe für Hausbewohner. Der Zugriff für diese Gruppe ist standardmäßig freigeschaltet.

Heimnetzwerk

Computernetzwerk (Ethernet) in Ihrem Zuhause. Über das Heimnetzwerk sind Ihre Netzwerkgeräte mit dem SDA Connector verbunden.

Fernzugriff

Gesicherter Zugriff über den SDA Portalserver und einen SDA Connector auf ein Gerät in Ihrem Heimnetzwerk.

Gesicherte Verbindung

Bezeichnet eine verschlüsselte und beidseitig authentifizierte Kommunikationsverbindung zwischen zwei Kommunikationspartnern.

TLS, SSL

Internetstandard (gemäß RFC 5246) für ein verschlüsseltes und optional authentifiziertes Kommunikationsprotokoll. SSL bedeutet „Secure Socket Layer“. Das Protokoll wurde 1999 umbenannt in TLS für „Transport Layer Security“. Beide Begriffe sind synonym. Das Protokoll ist weit verbreitet vor allem als Sicherheitsschicht von HTTPS.

Datenvolumen, Traffic

- Bezeichnet die über den SDA Portalserver übertragene Nutzdatenmenge. In unterschiedlichen Anwendungen werden stark unterschiedlich viele Daten übertragen. KNX-Kommunikation verursacht wenig, ein Livestream von einer Webcam verursacht hingegen viel Datenvolumen. Die übertragene Datenmenge belastet den SDA Portalserver. Es gibt daher unterschiedliche Abrechnungsmodelle für unterschiedliche Anwendungen mit Beschränkung des zulässigen Datenvolumens.

Benutzerrolle

Ein Portalbenutzer hat bezogen auf einen für ihn freigegebenen SDA Connector entweder die Rolle „Benutzer“ oder „Administrator“.

Ein „Benutzer“ darf den SDA Connector zum Zugriff auf das Heimnetzwerk verwenden. Ein „Administrator“ darf zusätzlich den SDA Connector für weitere Benutzer freigeben, Freigaben entziehen und Benutzerrollen sowie Zugriffsgruppen festlegen.

Eigentümer

Der „Eigentümer“ (englisch „Owner“) eines SDA Connectors ist die rechtlich verantwortliche Person. Der Eigentümer hat immer die Benutzerrolle „Administrator“. Jeder mit einem Portalkonto verknüpfte SDA Connector hat genau einen Eigentümer. Per „Schlüsselübergabe“ kann der Eigentümer geändert werden.

Schlüsselübergabe

Bezeichnet die Funktion des SDA Portalservers, den Eigentümer eines SDA Connectors zu ändern. Dieser Fall tritt regelmäßig auf, wenn eine neue Gebäudeinstallation vom Errichter an den Bauherren übergeben wird, deshalb der Name „Schlüsselübergabe“. Siehe auch Abschnitt 3.9.1.

Authentifizierungsschlüssel

Authentifzierungsschlüssel werden von einer Software, die eine SDA Verbindung öffnen will wie z.B. eine Visualisierung, benutzt, um sich gegenüber dem Portal zu authentifizieren. Sie werden explizit von einem Benutzer im Portal angelegt und sind sozusagen ein „Ersatz“ für Portalbenutzer/Passwort, so dass ein Benutzer nie seine persönlichen Anmeldedaten in eine Anwendung eintragen oder gar Dritten übergeben muss. Siehe auch Abschnitt 3.8.3 „Authentifzierungsschlüssel“.

Lokales Netzwerk

Als lokales Netzwerk wird das Netzwerk bezeichnet, in dem sich der PC befindet, mit dem ich über SDA auf ein Gerät in meiner Installation (siehe auch „Entferntes Netzwerk“) zugreifen will. Der Zugriff erfolgt entweder über das Portal oder den SDA Client. Im Falle von KNX ist dies auch der PC, auf dem die ETS gestartet wird.

Entferntes Netzwerk

Als entferntes Netzwerk wird das Netzwerk bezeichnet, in dem sich der SDA Connector befindet. Über den SDA Connector bietet SDA einen sicheren Zugriff auf das entfernte Netzwerk über das Internet.

2 Anwendungsszenarien

2.1 Wichtige allgemeine Informationen

2.1.1 Quick Connect vs. SDA Portal

Die einfachste und schnellste Nutzungsvariante ist der Quick Connect. Beim Quick Connect greift man ausschließlich über Eingabe der Registrierungs-ID (siehe auch Abschnitt 1.3.2 “Quick Connect”), die auf dem Gerät aufgedruckt ist, auf die Installation aus der Ferne zu. Dies hat den Vorteil, dass man keine Benutzer im Portal anmelden muss. Ein Anwendungsfall ist z.B. ein ISE SMART CONNECT KNX REMOTE ACCESS auf einer Baustelle in Verbindung mit einem UMTS/LTE Router, der für jeden Kollegen schnell und unkompliziert nutzbar sein soll.

Unabhängig vom Einsatz von Quick Connect bzw. des SDA Portals stehen jeweils alle Zugriffsmöglichkeiten (ETS, HTTP, HomeServer, etc.) zur Verfügung.

2.1.2 Einschränkungen und Freigaben von Zugriffsrechten über KNX Kommunikationsobjekte

Wenn der ISE SMART CONNECT KNX REMOTE ACCESS 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 SDA-Fernzugriff unabhängig von Einstellungen im SDA Portal komplett deaktiviert werden.

2.2 Zugriff auf Webseiten im entfernten Netzwerk

SDA erlaubt den sicheren Zugriff auf Webseiten im entfernten Netzwerk. Hierfür werden die im entfernten Netzwerk unverschlüsselten (HTTP) Daten (siehe Abbildung 2) über eine verschlüsselte SSL/TLS Verbindung zum SDA Portalserver transportiert und wiederum über eine HTTPS Verbindung zum Internet Browser.

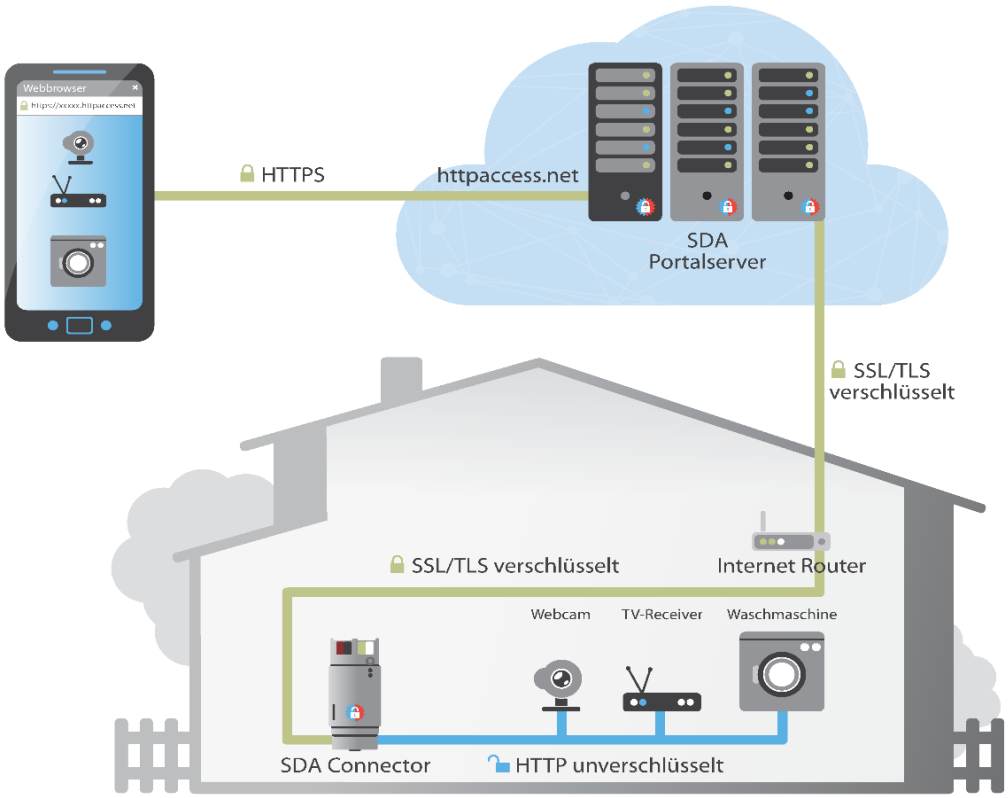


Abbildung 2: Sicherer Zugriff auf Webseiten mit „Secure Device Access“

Der HTTP Zugriff auf Webseiten im entfernten Netzwerk ist am einfachsten über das SDA Portal möglich. Hierbei ist ein Zugriff über Quick Connect oder auch Portal Connect schnell konfiguriert. Eine Beschreibung hierzu finden Sie in den Abschnitten 3.2 „HTTP Zugriff über Quick Connect“ sowie 3.5 „HTTP Zugriff über Portal Connect“.

2.3 Zugriff auf KNX-Installationen

Der SDA Client ermöglich den sicheren Zugriff auf KNX-Installationen über das Internet. Hierzu wird der SDA Client parallel zur ETS auf dem PC installiert und gestartet. Da das KNX/IP Protokoll heute völlig ungeschützt ist, überträgt der SDA Connector alle KNX/IP Daten SSL/TLS verschlüsselt an den SDA Portalserver, während dieser diese wiederum SSL/TLS verschlüsselt mit dem SDA Client austauscht. Für die ETS stellt der SDA Client dann lokal auf dem PC mit der ETS die KNX/IP Daten wiederum unverschlüsselt zur Verfügung, so dass die ETS völlig transparent und damit wie gewohnt genutzt werden kann.

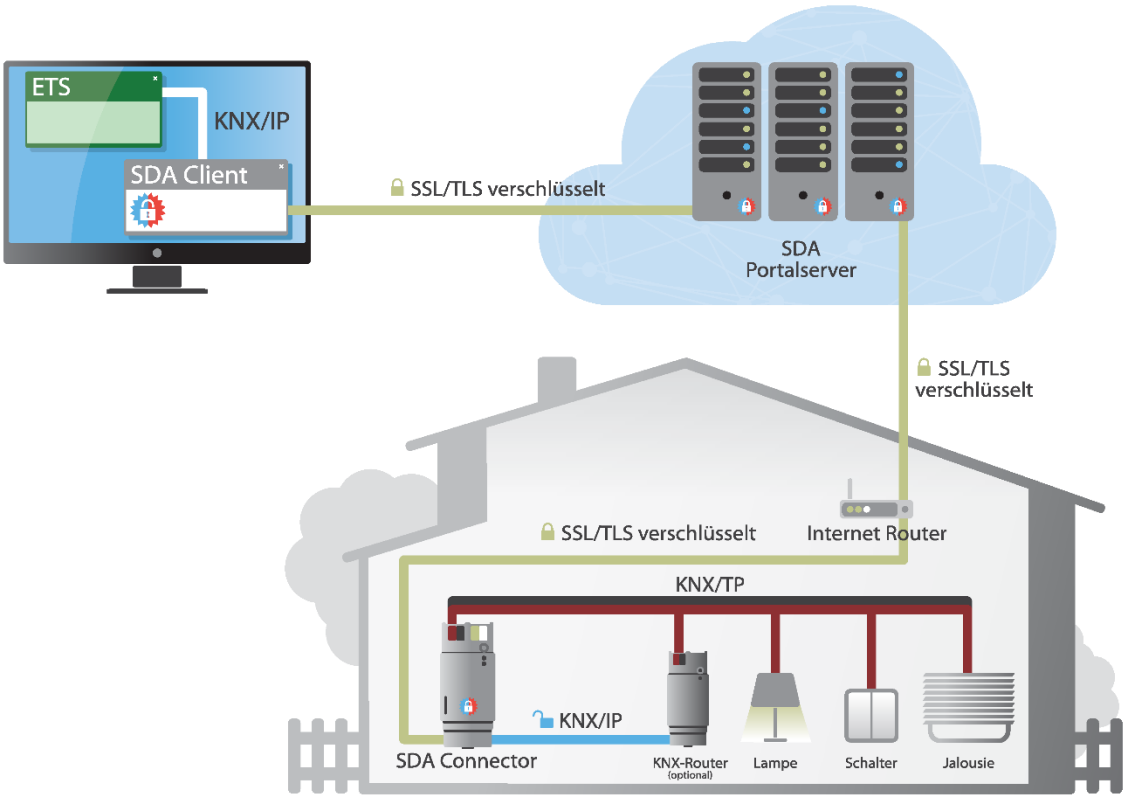


Abbildung 3: Sicherer Zugriff auf die KNX-Installation mit „Secure Device Access“

Nachdem mit dem SDA Client eine Verbindung zu einem bestimmten SDA Connector hergestellt wurde (siehe. Abschnitt 4.2 „Über den SDA Client mit einem SDA Connector verbinden“), 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 (z.B. „SDA - “) dem normalerweise in der ETS angezeigten Gerätenamen voranzustellen. Außerdem ist es der Einfachheit halber auch möglich, nur die KNX/IP Schnittstelle des SDA Connectors zur Verfügung zu stellen. Neben den KNX/IP Schnittstellen werden auch alle Geräte, die direkt über IP ladbar sind (siehe Abschnitt 7.3 „Übertragung beschleunigen: Übertragungsweg *KNX-TP* oder *IP* wählen“), der ETS bekannt gemacht, so dass auch diese beschleunigten Downloads über SDA funktionieren. Weitere Informationen finden Sie hierzu auch im Abschnitt 4.3. „Konfiguration der Zugriffsoptionen eines SDA Connectors“.

2.4 SDA Benachrichtigungen

SDA Benachrichtigungen sind dafür gedacht, aus der Installation, z.B. über KNX Gruppenobjekte, Informationen auf dem Portal in einer Nachrichtendatenkbank zu speichern. Auch Systemereignisse wie das An- und Abmelden eines SDA Connectors am Portal können auf diese Weise erfasst werden.

Eine SDA Benachrichtigung besteht aus folgenden Eigenschaften:

- Erzeugungsdatum
- Kategorie („System“ oder frei wählbarer Text)
- Betreff
- Inhaltstext
- Dringlichkeit (Niedrig, Hoch, Alarm, System)

- Optional einen Anhang, z.B. Bild einer IP Kamera

2.4.1 SDA Benachrichtigungen über KNX

Im Datenbankeintrag stehen 50 KNX Gruppenobjekte zur Verfügung, um Werte vom KNX zu empfangen und Benachrichtigungen 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 Benachrichtigungen 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.

2.5 Konfiguration 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. Auch hierbei werden alle Daten beim Transport über das Internet verschlüsselt.

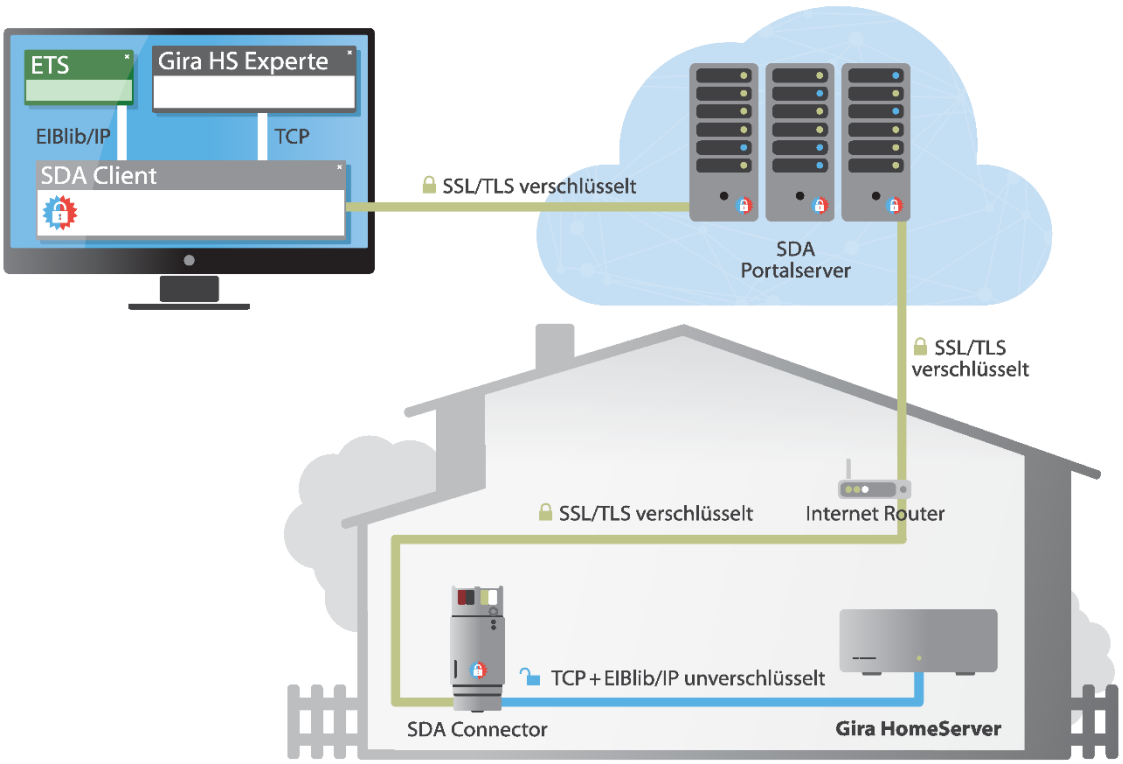


Abbildung 4: Sichere Konfiguration des Gira HomeServers mit „Secure Device Access“

Hinweis: Da für das Eiblib/IP sowie das HomeServer Konfigurationsprotokoll keine automatische Erkennung möglich ist, ist für die Nutzung dieser Protokolle über SDA folgendes zu beachten: Der SDA 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 SDA 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 hierzu finden Sie im Abschnitt 4.3.3. „Fernkonfiguration Gira HomeServer und Nutzung von Eiblib/IP“.

2.6 Zugriff über andere TCP Protokolle

Über SDA 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 SDA Client können Sie einfach den Zugriff konfigurieren. Weitere Informationen finden Sie im Abschnitt 4.3.4 „Nutzung weitere TCP Protokolle über SDA“.

Sollte Ihnen ein Protokoll fehlen oder Sie sich über die korrekte Nutzung nicht sicher sein, besuchen Sie bitte unser Forum oder senden Sie uns eine E-Mail an unseren Support.

2.7 Benutzerrechte und Zugriffsgruppen

Unabhängig von der Art des Zugriffs – also ob es um Webseiten, KNX, HomeServer, Remotedesktopverbindung u.ä. geht – können Zugriffsrechte für die vordefinierten Zugriffsgruppen Bewohner und Installateur sowie Quick Connect pro Beziehung zwischen SDA Connector und Portalbenutzer konfiguriert werden und über KNX Kommunikationsobjekte dynamisch gesteuert werden.

Ein typisches Szenario nach der Schlüsselübergabe könnte so aussehen:

- Mit dem SDA Connector sind ein oder mehrere Portalbenutzer meines Elektrohandwerkbetriebs/Systemintegrators in der Rolle des „Installateur“ verbunden, für Wartungszwecke.
- Mit dem SDA Connector sind ein oder mehrere Portalbenutzer in der Rolle des „Bewohner“ verbunden, typischerweise alle Familienmitglieder, für Visualisierungen auf dem Smartphone und Webseitenzugriffe.
- Der SDA Connector wird in der ETS über die Parameter so konfiguriert, dass die Benutzer mit der Zugriffsgruppe „Bewohner“ grundsätzlich Zugriff haben; außerdem haben die Benutzer der Zugriffsgruppe „Installateur“ standardmäßig keinen 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 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 SDA Zugriff komplett zu deaktivieren. Der SDA Connector meldet sich dann gar nicht mehr beim Portal an, ein Fernzugriff ist unmöglich.
- Der SDA Connector signalisiert einen Verbindungsaufbau über SDA 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 Authentifizierungsschlüsseln gesteuert werden. Von diesen kann jeder Benutzer an jedem SDA Connector, auf den er Zugriff hat, beliebig viele Schlüssel anlegen, z.B. für die Visualisierung (siehe Abschnitt 3.8.3 „Authentifzierungsschlüssel“).

3 Nutzung des SDA Portalservers

Der Portalserver ist unter der gesicherten Adresse https://securedeviceaccess.net erreichbar.

3.1 Startseite

Über die Startseite des Portals erlangt man durch die Eingabe eines Benutzers oder einer Registrierungs-ID (Textfeld „Connector ID“) entsprechenden Zugriff auf Konfigurationseinstellungen und Webseiten im entfernten Netzwerk.

Konkret bietet die Seite folgende Funktionen an:

- Die Anmeldung mit einem bereits auf dem Portal registrierten Benutzer.
- Die Registrierung eines neuen Benutzers im Falle einer Erstanmeldung.
- Die Nutzung des HTTP Zugriffs via Quick Connect mit der auf dem Gerät aufgedruckten Registrtierungs-ID.

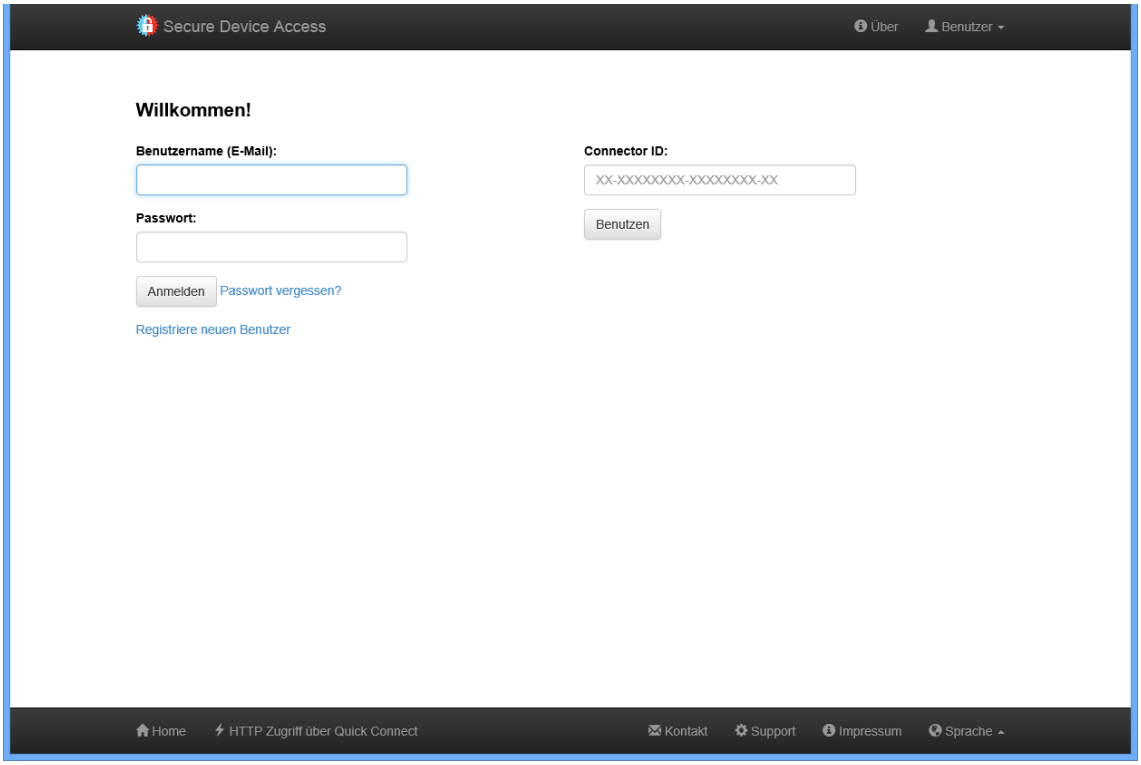


Abbildung: 5: SDA Portal – Startseite

3.2 HTTP Zugriff über Quick Connect

Wenn Sie sich für die Nutzung über Quick Connect entscheiden, können Sie das SDA Portal ohne Anmeldung eines registrierten Benutzers nutzen, um Webseiten von Geräten im entfernten Netzwerk zu besuchen.

Nach Eingabe der Registrierung-ID (Textfeld „Connector ID“) auf der Startseite und Drücken der Schaltfläche „Benutzen“ gelangen Sie auf eine Seite, die die bereits in der Vergangenheit genutzten Links zu Geräten in der Installation zwischenspeichert. 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 Drucker, DSL-Router, IP-Kameras, alle

Produkte der ISE SMART CONNECT Serie u.v.a.m. werden dabei erfasst. Technisch wird hier das Simple Service Discovery Protocol (kurz SSDP) benutzt.

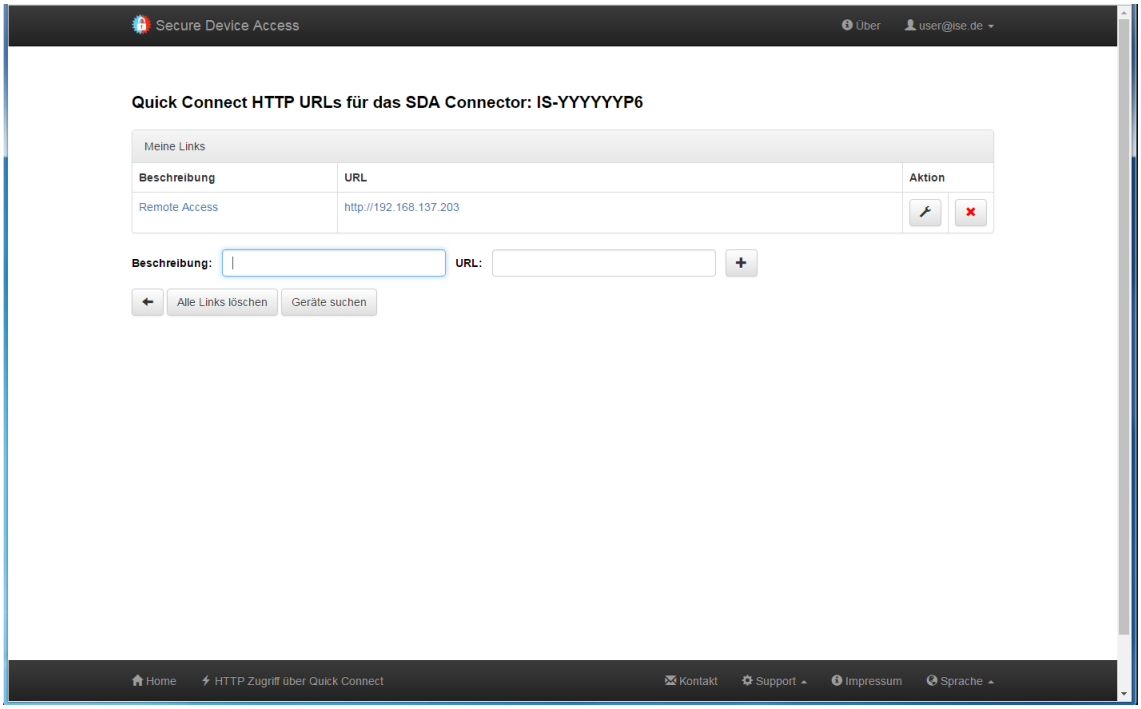


Abbildung 6: Zugriff auf HTTP Webseiten über Quick Connect

Manuell können Sie in dem Feld „URL“ einen HTTP Pfad im entfernten Netzwerk eintragen (z.B. „192.168.1.200/index.html“) und auch eine Beschreibung zum Link eintragen, so dass Sie dauerhaft einen schnellen Zugriff auf Ihre Geräte haben.

Nicht alle Webseiten können aus dem entfernten Netzwerk über SDA geladen werden. Insbesondere komplexere Seiten können ggf. nicht funktionieren. Bitte senden Sie uns in solch einem Fall gerne an den Support (siehe Kapitel 10 „Fehlersuche und Support“) eine E-Mail mit der genauen Produktbeschreibung, Screenshots und einer kurzen Fehlerbeschreibung.

Für angelegten Links stehen folgende Aktionen zur Verfügung:

Aktion	Beschreibung
	Editieren der URL
	Löschen des Links

3.3 Benutzerregistrierung

Wenn Sie nicht mit Quick Connect arbeiten möchten, können Sie sich als Benutzer beim SDA Portal registrieren. Insbesondere wenn Sie Benutzerrechte differenziert vergeben wollen oder mit mehreren Personen über den ISE SMART CONNECT KNX REMOTE ACCESS auf Ihr Netzwerk zugreifen wollen, ist dies notwendig bzw. sehr hilfreich.

Die Registrierung erfolgt nach dem heute üblichen Standard zur Verifikation der E-Mail-Adresse. Die Bestätigung eines Links in einer automatisch nach Start der Registrierung an die angegebene E-Mail-Adresse gesendete Verifikationsmail ist zwingend

erforderlich. Damit ist sichergestellt, dass eine Anmeldung unter einer fremden E-Mail-Adresse nicht möglich ist. Das Verfahren ist automatisiert, so dass es nur wenige Minuten in Anspruch nimmt.

3.4 SDA Connector Verwaltung

Nach erfolgreicher Benutzerregistrierung und Anmeldung am SDA Portal sehen Sie die Liste aller mit Ihrem Benutzer verbundenen Geräte. Bei der ersten Anmeldung ist sie typischerweise leer.

Sie können über folgende Wege mit einem Gerät verbunden werden:

1. Sie fügen mit den Bedienelementen unter der Liste Ihrer Geräte einen neuen SDA Connector über die Registrierungs-ID (Textfeld „Connector ID“) hinzu und werden damit der Eigentümer (wichtige Hinweise siehe Abschnitt 3.10 „Eigentümer und Übertragung der Eigentümerschaft“).
2. Ein anderer Benutzer gibt Ihnen Zugriffsrechte auf einen SDA Connector, der von dem anderen Benutzer administriert wird.
3. Ein anderer Benutzer überträgt Ihnen die Eigentümerschaft (wichtige Hinweise siehe Abschnitt Abschnitt 3.10 „Eigentümer und Übertragung der Eigentümerschaft“).

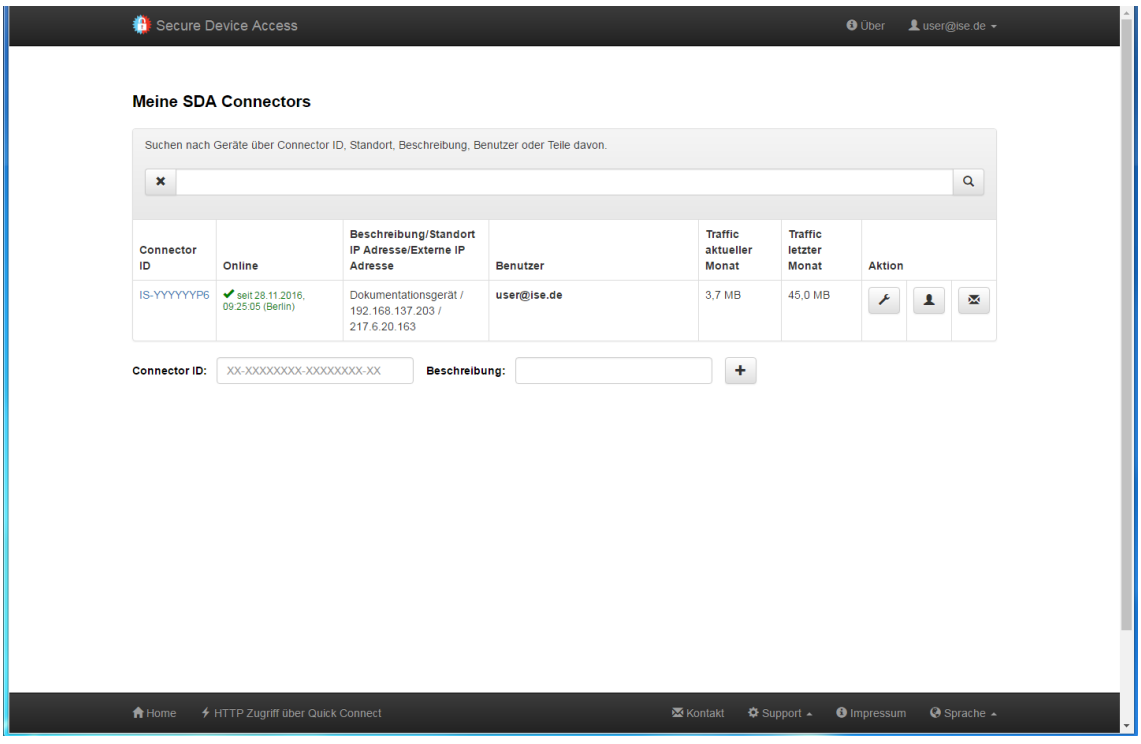


Abbildung 7: SDA Connectoren des angemeldeten Benutzers

In der Liste der mit Ihrem Benutzer verbundenen SDA Connectoren können Sie über die Links hinter dem entsprechenden SDA Connector in der Spalte „Fernzugriffs-ID“auf Webseiten im entfernten Netzwerk zugreifen.

In der Spalte „Online“ erhalten Sie Informationen über den aktuellen Verbindungsstatus des SDA Connectors. Die Uhrzeitangaben werden entsprechend der Zeitzoneneinstellung Ihres Benutzers dargestellt. Ist das Gerät aktuell nicht am Portalserver angemeldet, also „offline“, erscheint der Text in rot, andernfalls grün.

Die Spalte „Standort/Beschreibung“ erhält Textfelder, die vom Anwender frei vergeben werden. Der Standort ist eine Eigenschaft am SDA Connector und damit für alle Benutzer gleich, der Beschreibungstext kann von jedem mit dem SDA Connector verbundenen Benutzer frei vergeben werden. Das ermöglicht z.B. einem Installateur nach der Übergabe die Adresse zu hinterlegen, wenn der Bauherr als Standort „Zu Hause“ einträgt.

In der Spalte „Benutzer“ sehen der Eigentümer und die Administratoren alle mit dem Gerät verbundenen Benutzer. Ein normaler Benutzer sieht aus Gründen des Datenschutzes die anderen Benutzer nicht. Wenn ein Gerät das erste Mal mit einem Benutzer verbunden wird, ist dieser der Eigentümer (siehe Abschnitt 3.10 „Eigentümer und Übertragung der Eigentümerschaft“)

Der Eigentümer ist immer in **fett** dargestellt.

Die beiden folgenden Spalten zeigen das bisher verbrauchte Datenvolumen für den aktuellen sowie den Vormonat. Hinsichtlich des zur Verfügung stehenden Datenvolumens und der Nutzungsbedingungen siehe Kapitel 11 „Lizenzvertrag ISE SMART CONNECT KNX REMOTE ACCESS-Software“.

Als Aktionen können (ja nach Benutzerrechten) bis zu fünf zur Verfügung stehen:

Aktion	Beschreibung
	Eigenschaften und erweiterten Informationen eines SDA Connectors anzeigen und ändern (siehe Abschnitt 3.6 „Erweiterte Informationen zu einem SDA Connector“ und Abschnitt 3.7 „Eigenschaften eines SDA Connectors anzeigen und ändern“)
	Zugriffsrechte für andere Benutzer verwalten (siehe Abschnitt 3.8 „Zugriffsrechte für Benutzer verwalten“)
	SDA Benachrichtigungen anschauen und verwalten (siehe Abschnitt 3.9 „SDA Benachrichtigungen“

3.5 HTTP Zugriff über Portal Connect

Der Zugriff auf entfernte Webseiten über SDA mit angemeldetem Benutzer (Portal Connect) entspricht von der Funktionsweise im Wesentlichen dem Zugriff über Quick Connect, siehe Abschnitt 3.2. „HTTP Zugriff über Quick Connect“.

Es gibt hier allerdings die Möglichkeit, für Benutzer ohne Administrationsrechte die Funktion „Geräte suchen“ zu deaktivieren. Siehe hierzu auch Abschnitt 3.8 „Zugriffsrechte für Benutzer verwalten“.

3.6 Erweiterte Informationen zu einem SDA Connector

Zu einem angemeldeten SDA Connector hält der Portalserver Informationen vor, die insbesondere für die Diagnose von Problemen sehr wichtig sind.

Dazu gehören:

- Die Registrierungs-ID
- Die IP Adresse das SDA Connectors im entfernten Netzwerk
- Die Internet IP Adresse, über die der SDA Connector mit dem Portal kommuniziert. Dies ist die externe IP Adresse des Internet-Gateways, z.B. Ihrer Fritz Box
- Die SDA Softwareversion (auch SDA Service Version genannt), die aktuelle auf dem SDA Connector läuft

3.7 Eigenschaften eines SDA Connectors anzeigen und ändern

Die Seite zeigt detaillierte Informationen zum SDA Connector an. Über die Schaltfläche kann die Registrierungs-ID (SDA Connector ID) sichtbar gemacht werden, die Sie dann mit der Schaltfläche in die Zwischenablage kopieren können.

Darüber hinaus kann allgemein für den SDA Connector der Standort sowie der Quick Access Zugriff geändert werden, insofern der angemeldete Benutzer die Zugriffsrechte hierfür hat. Außerdem kann die automatische Erzeugung von SDA Benachrichtigungen beim An-/Abmelden des SDA Connector bzw. SDA Clients aktiviert werden.

Die Schlüsselübergabe dient der Übertragung des Eigentümers (s.u.), z.B. bei Übergabe vom Handwerker an den Eigentümer, und zum Löschen eines Connectors vom Portal. Letztere Funktion ist nur sinnvoll, wenn der SDA Connector verkauft wird, da alle Benutzerberechtigungen u.ä. irreversibel entfernt werden.

Dies ist nicht möglich, so lange Sie der Eigentümer des SDA Connectors sind! Siehe auch Abschnitt 2.7 „Benutzerrechte und Zugriffsgruppen“.)

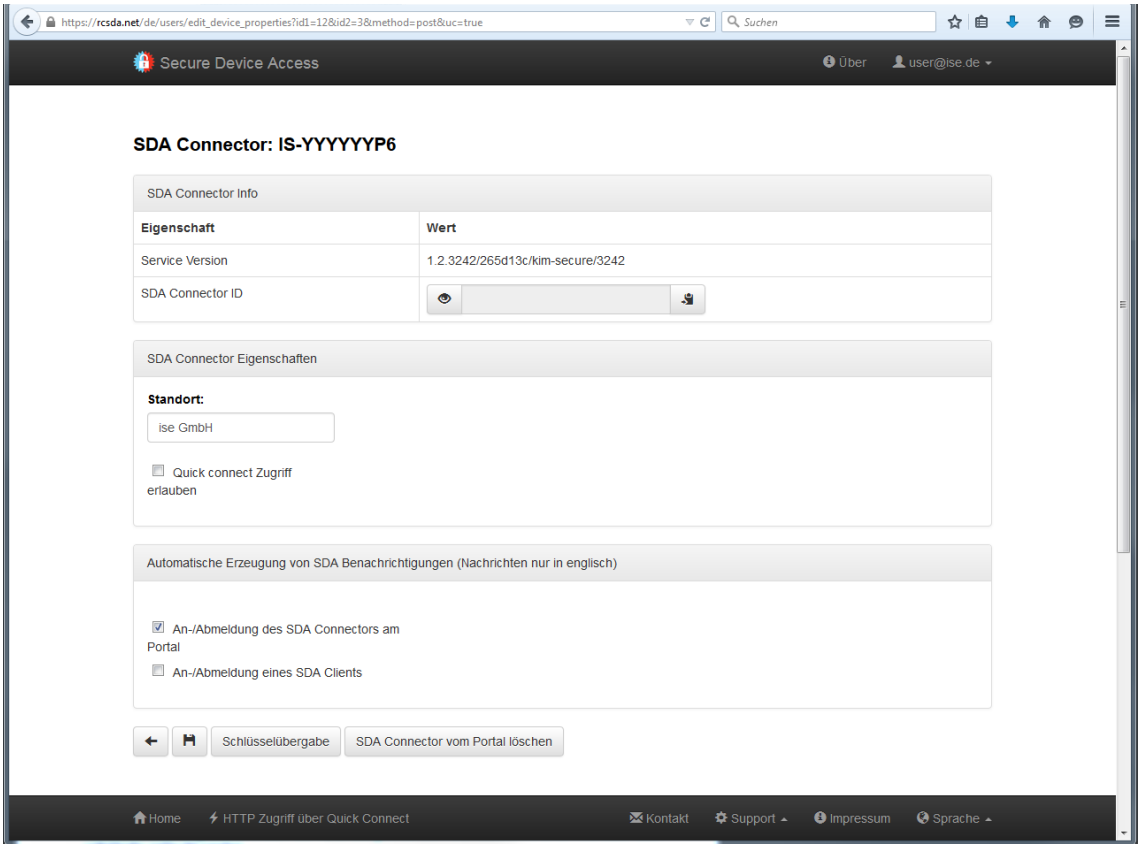


Abbildung 8: Eigenschaften eines SDA Connectors anzeigen und ändern

3.8 Zugriffsrechte für Benutzer verwalten

Das SDA Portal erlaubt die differenzierte Konfiguration von Zugriffsrechten auf Basis von Benutzern für jeden SDA Connector.

Für jeden Benutzer kann festgelegt werden (insofern der aktuell angemeldete Benutzer die entsprechenden Rechte besitzt):

Benutzer	Beschreibung
Rolle	Möglich sind hier „Eigentümer“, „Administrator“ und „Benutzer“, wobei der Eigentümer ein Administrator mit einer Sonderstellung ist (siehe Abschnitt Abschnitt 3.10 „Eigentümer und Übertragung der Eigentümerschaft“, und daher im Folgenden nur noch von Administrator und Benutzer gesprochen wird (s. u.).
Zugriffsgruppen	Möglich sind hier „Bewohner“ und „Installateur“, wobei ein Benutzer keiner oder auch beiden Gruppen zugordnet sein kann (s u.).

Neben dem Hinzufügen von neuen Benutzern zu einem SDA Connector, können Benutzerrechte natürlich auch wieder eingeschränkt bzw. die Verbindung eines SDA Connectors mit einem Benutzer auch vollständig gelöscht werden.

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

Darüber hinaus kann hier der angemeldete Benutzer seine Authentifizierungsschlüssel verwalten. Diese werden z. B. von Visualisierungen zusammen mit der Fernzugriffs-ID als SDA Anmeldeinformation genutzt, damit nicht die eigenen Benutzerinformationen weitergegeben werden müssen.

Eigentümer und Administratoren haben ggf. die Rechte, auch für andere Benutzer Konfigurationen vorzunehmen bzw. für diese einzuschränken. Abbildung 9 zeigt die Aktionen:

Aktion	Beschreibung
	Benutzer editieren
	Weiterleitungsregeln SDA Benachrichtigungen
	Rechte
	Authentifizierungsschlüssel
	Löschen

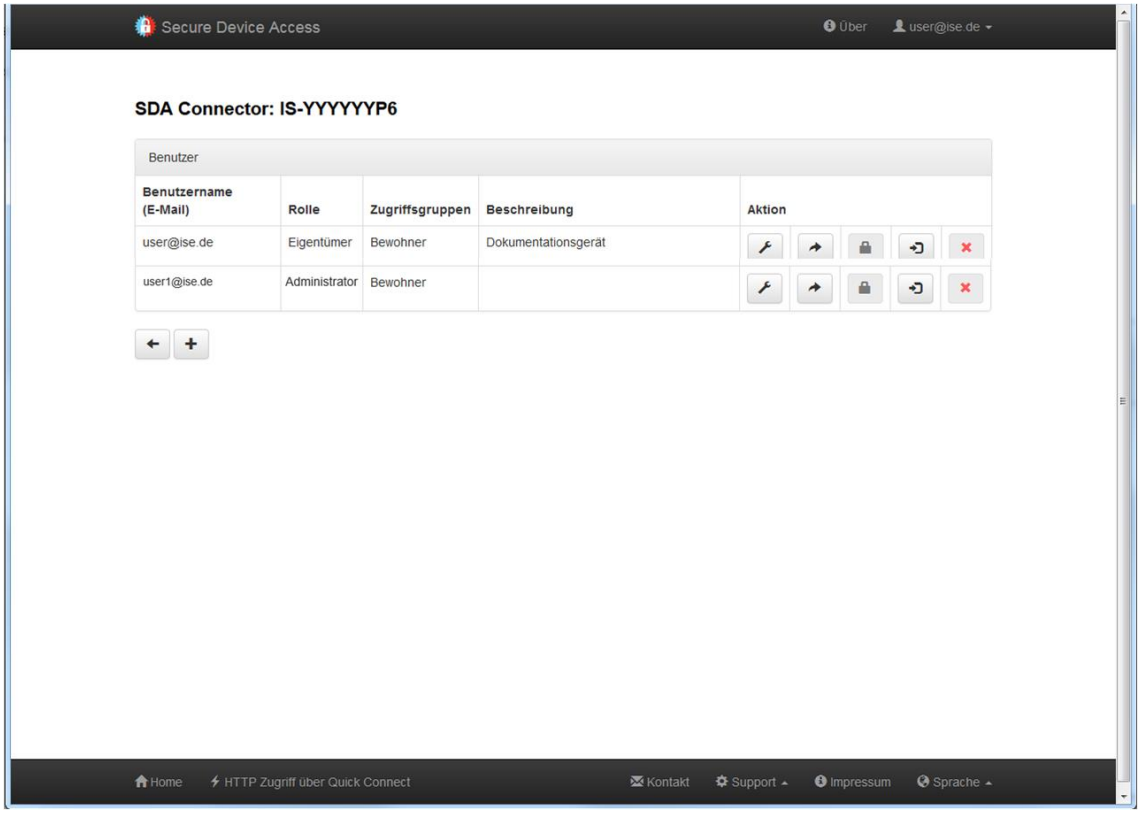


Abbildung 9: Zugriffsrechte für Benutzer verwalten

3.8.1 Die Rolle eines Benutzers an einem SDA Connector

Der Unterschied zwischen einem Administrator und Benutzer liegt in den Rechten, auf dem SDA Portal Konfigurationsänderungen vornehmen zu dürfen. Jeder Administrator kann alle Eigenschaften und Benutzerrechte für den SDA Connector verwalten (mit Ausnahme der Eigentümerschaft), der Benutzer kann die Eigenschaften maximal anschauen.

Für einen Benutzer ohne Administrationsrechte kann konfiguriert werden, ob dem Benutzer die Möglichkeit Geräte zu suchen zur Verfügung stehen soll (siehe Abschnitt 3.5 „Zugriffsrechte für Benutzer verwalten“).

Die Rolle eines Benutzers in Verbindung mit einem SDA Connector bezieht sich ausschließlich auf die Konfigurationsmöglichkeiten auf dem SDA Portal und hat absolut nichts mit den Zugriffsrechten über SDA auf das entfernte Netzwerk zu tun! Für letzteres dienen ausschließlich die Zugriffsgruppen (siehe Abschnitt 3.8.2 „Die Zugriffsgruppen eines Benutzers an einem SDA Connector“)!

3.8.2 Die Zugriffsgruppen eines Benutzers an einem SDA Connector

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. Darüber hinaus kann auch der Quick Connect über den KNX aktiviert bzw. deaktiviert werden. Lesen Sie dazu bitte das Kapitel 6 „Projektierung in der ETS“.

Die Zugriffsgruppen eines Benutzers in Verbindung mit einem SDA Connector beziehen sich ausschließlich auf die Rechte, auf das entfernte Netzwerk über SDA zuzugreifen, um z.B. Webseiten zu besuchen oder mit der ETS auf die KNX-Installation zuzugreifen. Wenn Sie die Konfigurationsmöglichkeiten auf dem SDA Portal für einen Benutzer ändern wollen, nutzen Sie hierfür die Rollen (siehe Abschnitt 3.8.1 „Die Rolle eines Benutzers an einem SDA Connector“)!

3.8.3 Authentifzierungsschlüssel

Der Zugriff von Software wie z.B. Visualisierungen kann über den Einsatz von Authentifizierungsschlüsseln gesteuert werden. Von diesen kann jeder Benutzer an jedem SDA Connector, auf den er Zugriff hat, beliebig viele Schlüssel anlegen, z.B. für die Visualisierung.

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

Um die Einrichtung einer Applikation für die Nutzung eines Authentifizierungsschlüssels zu erleichtern, kann über die Schaltfläche ein Aktivierungsschlüssel erzeugt werden. Dieser kann von der Applikation verwendet werden, um den zugehörigen Authentifizierungsschlüssel vom SDA Portal in die Applikation zu transferieren. Ein Aktivierungsschlüssel ist maximal 24 Stunden gültig und kann beliebig oft verwendet werden. Die automatische Deaktivierung des Aktivierungsschlüssels erfolgt zum Zeitpunkt, der in der Spalte „Datum Ende Aktivierung“ angegeben ist. Es wird empfohlen einen Aktivierungsschlüssel nach Beendigung der Einrichtung von Applikationen manuell über die Schaltfläche zu deaktivieren, um eventuellen Missbrauch zu vermeiden. Da der Aktivierungsschlüssel erheblich kürzer ist als ein Authentifizierungsschlüssel, ist ein Aktivierungsschlüssel leichter angreifbar.

Für erstellte Authentifizierungsschlüssels stehen folgende Aktionen zur Verfügung:

Aktion	Beschreibung
	Anzeigen des Authentifizierungsschlüssels
	Erzeugung eines Aktivierungsschlüssels für den Authentifizierungsschlüssel
	Entfernen eines Aktivierungsschlüssels für den Authentifizierungsschlüssel
	Kopieren des Authentifizierungsschlüssels in die Zwischenablage
	Löschen des Authentifizierungsschlüssels

3.9 SDA Benachrichtigungen

Über das Briefsymbol () gelangt man in die Nachrichtenliste eines Connectors. Alle Benachrichtigungen werden chronologisch sortiert angezeigt. Eventuelle Anhänge wie z.B. Kamerabilder können per Link direkt geöffnet werden.

Diese Benachrichtigungen können auch nach konfigurierbaren Regeln weitergeleitet werden (siehe Abschnitt 3.9.1 „Weiterleitungsregeln für SDA Benachrichtigungen“). Über die Aktion Löschen () können Regeln wieder entfernt werden.

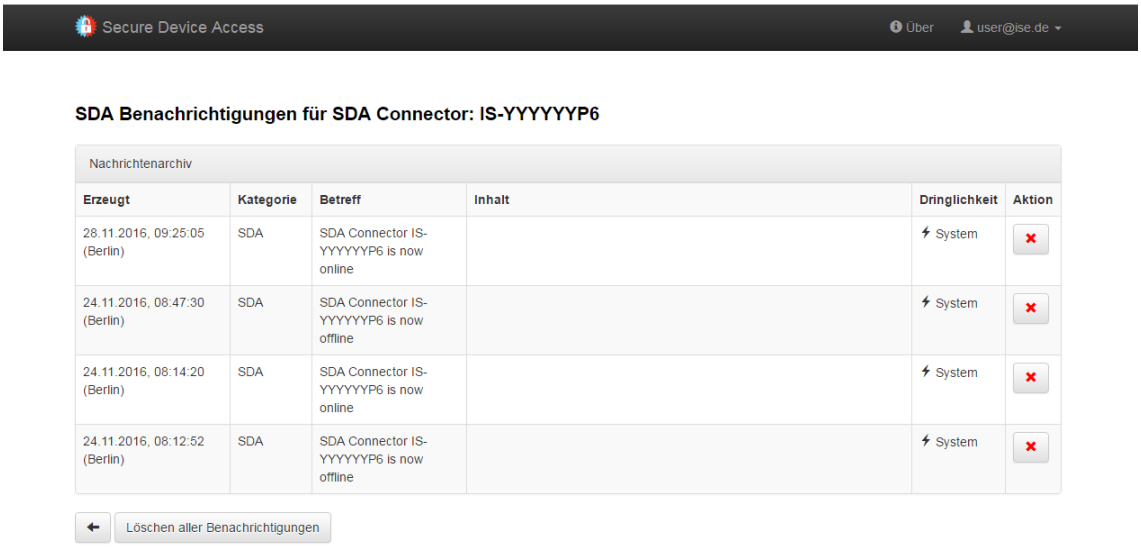


Abbildung 10: SDA Benachrichtigungen

3.9.1 Weiterleitungsregeln für SDA Benachrichtigungen

Als Administrator können Sie Weiterleitungsregeln für SDA Benachrichtigungen festlegen. In die entsprechende Auswahl kommen Sie durch Auswahl der Aktion Weiterleitungsregel (↱) in der Nutzerübersicht (siehe Abschnitt 3.8 „Zugriffsrechte für Benutzer verwalten“).

Die SDA Benachrichtigungen können bei der Erzeugung auf verschiedene Arten weitergeleitet werden, nämlich via:

- E-Mail (Standard ist die Benutzerkennung des Portals, Angabe mehrere Adressen möglich)
- SMS (nutzt sms77.de als Provider, Angabe mehrere Adressen möglich)
- Telefonsprachanruf, der die SDA Benachrichtigung vorliest, in vielen verschiedenen Sprachen möglich (nutzt sms77.de als Provider)
- IFTTT, Maker Channel (nutzt IFTTT.com, nur für erfahrene Benutzer)
  s. Abschnitt „SDA Benachrichtigungen als Trigger in IFTTT verwenden“, S. 29

> Für die Nutzung von Funktionen basierend auf sms77.de oder IFTTT muss ein eigener Account bei sms77.de eingerichtet werden. Die entsprechenden Zugangsdaten müssen im Menüpunkt „Externe Dienste“ bei den benutzerspezifischen Daten hinterlegt werden!

Jede Weiterleitungsregel gibt die Möglichkeit, nach Dringlichkeit und/oder Kategorie (Textfilter; ist mindestens ein Wort enthalten ist die Filterbedingung erfüllt) SDA Benachrichtigungen auszuwählen und weiterzuleiten.

Es können beliebig viele Weiterleitungsregeln konfiguriert werden, von denen jeweils alle aktiven beim Eingang einer SDA Benachrichtigung ausgewertet werden. Die Möglichkeit der Deaktivierung erlaubt das Erstellen von Regeln, die öfter aber nicht immer benötigt werden, z. B. nur, wenn man in Urlaub ist.

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

- Hinzufügen einer Weiterleitungsregel

- Deaktivieren aller Dringlichkeiten außer „System“
- Aktivieren von „Weiterleitung nach Kategorie“ und Eingabe von „SDA“ in das dann aktivierte Textfeld
- Aktivieren von „Weiterleitung per E-Mail“. Als Standardwert erscheint Ihre SDA Benutzer-ID. Die E-Mail für den Empfang der Weiterleitungen können Sie auch anpassen.
- Speichern Sie die Weiterleitungsregel. Sie ist automatisch aktiviert.

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

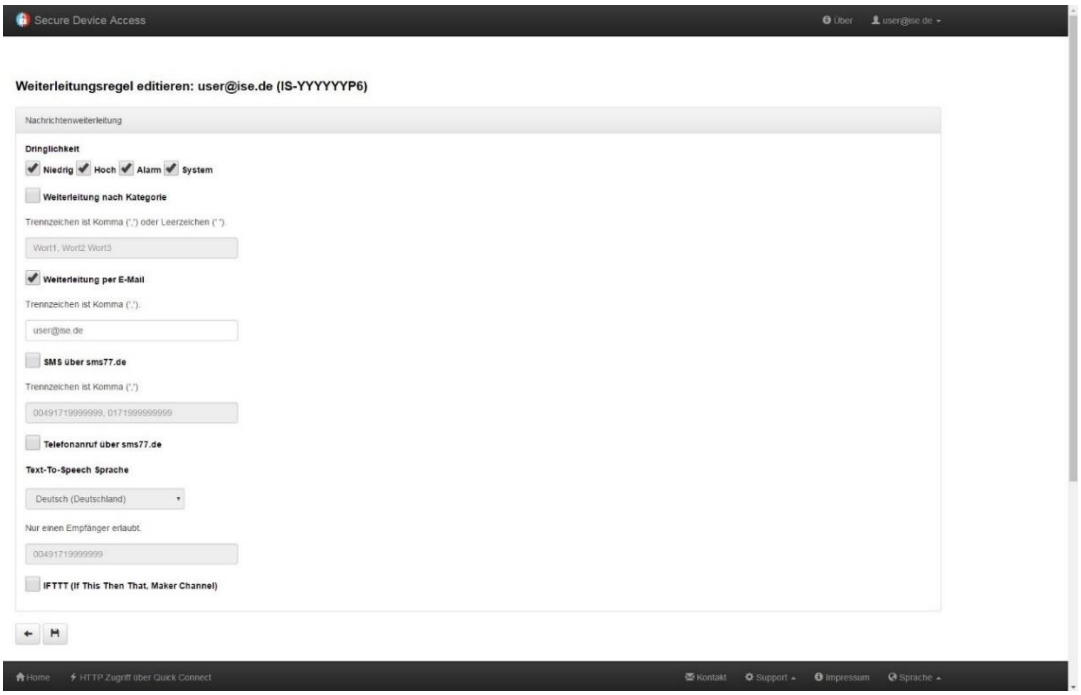


Abbildung 11: SDA Benachrichtigungen – Weiterleitungsregeln

3.9.2 SDA Benachrichtigungen als Trigger in IFTTT verwenden

SDA Benachrichtungen können an IFTTT weitergeleitet werden. Diese SDA Benachrichtigungen dienen in IFTTT dann als Trigger. SDA Benachrichtigungen können nicht als Action verwendet werden.

Die Beschreibung der Konzepte von IFTTT ist nicht Bestandteil dieser Dokumentation.

Um SDA Benachrichtungen weiterzuleiten, definieren Sie im SDA Portal beliebig viele Weiterleitungsregeln. Für jede dieser Weiterleitungsregeln können Sie eine Weiterleitung nach IFTTT konfigurieren.

IFTTT kennt die einzelnen Weiterleitungsregeln aus dem SDA nicht. Jede Weiterleitungsregel, für die IFTTT konfiguriert ist, ist demnach mit demselben Trigger (Event name = sda_notification) verknüpft.

Arbeitsschritte:

1. IFTTT mit dem SDA Portal verknüpfen.
2. Weiterleitungsregel im SDA Portal erstellen und diese für IFTTT konfigurieren.
3. Applet im IFTTT Portal erstellen und die SDA Benachrichtigungen als Trigger verwenden.

IFTTT mit dem SDA Portal verknüpfen

ℹ	Anleitungen zur Konfiguration innerhalb von IFTTT sind ohne Gewähr. IFTTT ist kein Produkt der ise Individuelle Software und Elektronik GmbH. Wir garantieren keinesfalls für die Aktualität und Richtigkeit von Dokumentationen zu Fremdprodukten.

1. IFTTT API Key ermitteln:
    a. Melden Sie sich am IFTTT Portal an.
    b. Geben Sie in die Suche <<Webhooks>> ein.
    c. Wählen Sie die Kachel des Service Webhooks.
    Die Seite des Service Webhooks wird geöffnet.
    d. Wählen Sie die Schaltfläche <<Connect>>.
    e. Wählen Sie die Schaltfläche <<Settings>> (rechts oben).
    f. Der API Key ist ein Teil der URL. Kopieren Sie den letzten Teil der URL (alles hinter „use/“)
2. API Key im SDA Portal eintragen:
    a. Melden Sie sich am SDA Portal an.
    b. Wählen Sie in der Menüleiste, in der Klappliste Ihres Benutzers, den Eintrag <<Externe Dienste>>.
    c. Geben Sie im Bereich <<IFTTT (If this then that) Anmeldedaten>> im Feld <<API Key>> den IFTTT API Key ein.
    d. Wählen Sie die Schaltfläche (Speichern).

Beispiel 1: IFTTT-URL

Angezeigte URL: https://maker.ifttt.com/use/wBXU7D6GY5SjAjilFf8r9

API Key: wBXU7D6GY5SjAjilFf8r9

Weiterleitungsregel im SDA Portal erstellen und diese für IFTTT konfigurieren

1. Melden Sie sich am SDA Portal an.
2. Wählen Sie in der Menüleiste, in der Klappliste, den Eintrag <<Meine SDA Connectors>>.
3. Wählen Sie in der Zeile des gewünschten Geräts die Aktion (Benutzer).
4. Wählen Sie in der Zeile des gewünschten Benutzers die Aktion (Weiterleitungsregeln).
5. Je nach Bedarf erstellen Sie eine neue Weiterleitungsregel oder bearbeiten eine vorhandene.
6. Konfigurieren Sie die Weiterleitungsregel wie gewohnt.
7. Um IFTTT zu aktivieren, wählen Sie die Checkbox <<IFTTT (If This Then That, Maker Channel>>.
8. Wählen Sie die Schaltfläche (Speichern).

Applet im IFTTT Portal erstellen und die SDA Benachrichtigungen als Trigger verwenden

Anleitungen zur Konfiguration innerhalb von IFTTT sind ohne Gewähr. IFTTT ist kein Produkt der ise Individuelle Software und Elektronik GmbH. Wir garantieren keinesfalls für die Aktualität und Richtigkeit von Dokumentationen zu Fremdprodukten.

1. Melden Sie sich am IFTTT-Portal an.
2. Erstellen Sie ein neues Applet:
   a. Wählen Sie im Menü <<My Applets>>.
   b. Auf der Seite <<Applets>> wählen Sie die Schaltfläche <<New Applet>>.
   c. Starten Sie die Konfiguration des Service, indem Sie den blauen Text „+ this“ wählen.
   d. Im Schritt <<Choose a service>> suchen Sie nach <<Webhook>>.
   e. Wählen Sie die Kachel des Service Webhook.
      Die Seite des Service Webhook wird geöffnet.
   f. Im Schritt <<Choose trigger>> wählen Sie die Kachel <<Receive a web request>>.
   g. Im Schritt <<Complete trigger fields>> geben Sie als <<Event Name>> den folgenden Text genauso ein:
      sda_notification
      Die SDA-Benachrichtungen sind als Trigger konfiguriert.
      Konfigurieren Sie nun wie gewohnt die gewünschte Aktion.

3.10 Eigentümer und Übertragung der Eigentümerschaft

Ab dem Moment, ab dem ein SDA Connector nicht ausschließlich über Quick Connect genutzt wird, sondern das erste Mal über das Portal einem Benutzer hinzugefügt wird, hat der SDA Connector einen Eigentümer. Es gibt ab dann immer genau einen Eigentümer. Der Eigentümer wird bei der Anzeige von Benutzern, die mit dem SDA Connector verbunden sind, immer **fett** dargestellt.

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

Der Eigentümer eines SDA Connectors kann jederzeit alle anderen Benutzer, auch andere Administratoren, alle Rechte entziehen, während ihm niemand den Zugriff verwehren kann.

Falls es zum Missbrauch des SDA Connectors bzw. des SDA Zugriffs 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 SDA Portal möglich. Hierzu gibt es die Schaltfläche „Schlüsselübergabe“ auf der Seite zur Anzeige und zum Ändern der SDA Connector Eigenschaften. Das Wechseln des Eigentümers erfolgt in einem gesicherten Verfahren:

1. Der aktuelle Eigentümer wählt die Schaltfläche „Schlüsselübergabe“ an, gibt den Benutzernamen 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 der gewünschte neue und der aktuelle Eigentümer beide akzeptiert haben, erhalten beide eine entsprechende E-Mail und die Eigentümerschaft ist übergegangen.

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

4 Nutzung des SDA Clients

Der SDA 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 SDA Client nicht erforderlich, siehe Abschnitt 2.2 „Zugriff auf Webseiten im entfernten Netzwerk“.

Die typischsten Anwendungsfälle für den SDA 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 SDA 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 SDA Client ist derzeit für Microsoft Windows ab der Version 7 verfügbar.

Sie finden die aktuelle Version der SDA Client Installationsanwendung auf http://www.securedeviceaccess.net unter Support/Downloads.

4.1 Allgemeine Einstellungen

Die allgemeinen Einstellungen öffnen Sie über die Schaltfläche „Zahnrad“ (oben rechts, siehe Abbildung 12: SDA Client - Allgemeine Einstellungen öffnen“, (1)).

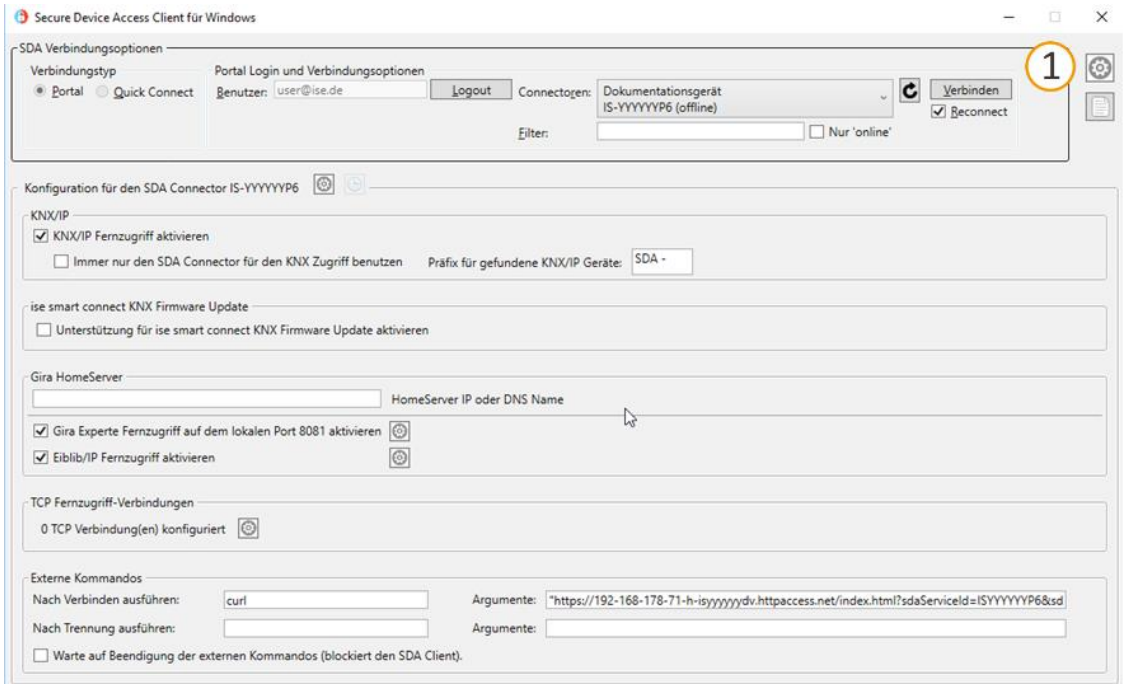


Abbildung 12: SDA Client - Allgemeine Einstellungen öffnen

In den allgemeinen Einstellungen können Sie bspw. das Erweiterte Logging für die Fehlersuche bei Problemfällen aktivieren. Auch können Sie die Logfiles löschen oder von diesen ein ZIP Archiv erzeugen, das dann im Support-Fall einfach an eine E-

Mail angehängt werden kann. Außerdem können Sie festlegen, ob der SDA Client sich das zuletzt benutzte Passwort merken soll.

Tabelle 1: Allgemeine Einstellungen - Details zu spezifischen Einstellungen

Einstellung	Beschreibung
ETS Zugriff für das gesamte lokale Netzwerk (LAN) aktivieren (ansonsten nur für diesen PC)	Definiert, für welche Clients alle KNX/IP Geräte verfügbar sind, die über den Fernzugriff via ISE SMART CONNECT KNX REMOTE ACCESS erreichbar sind. Der Client ist der PC, auf dem Ihre ETS läuft. Der PC wird anhand seiner IP-Adresse identifiziert. Die KNX/IP Geräte werden in der ETS unter <<Gefundene Schnittstellen>> angezeigt. Um diese KNX/IP Geräte in der ETS schneller zu finden, können Sie einen Präfix für deren Namen definieren (Bereich <<KNX/IP>> → Einstellung <<Präfix für gefundene KNX/IP Geräte>>). • Aktiviert: Alle im gleichen lokalen Netzwerk laufenden Clients haben Zugriff auf die KNX/IP Geräte. • Deaktiviert: Die KNX/IP Geräte sind nur für den aktuellen Client verfügbar. Die Einstellung wird erst ausgewertet, wenn Sie sich das nächste Mal mit dem SDA Connector verbinden (Schaltfläche <<Verbinden>>).
Sicheren Fernzugriff auf den Gira HomeServer für neue SDA Connector Konfigurationen automatisch aktivieren	Standardmäßig für neue SDA Connector Konfigurationen (siehe folgende Abschnitte) die Gira HomeServer Unterstützung aktivieren. Dies ist dann sinnvoll, falls Sie in Ihren Projekten regelmäßig den Gira HomeServer nutzen.
Verbindungs-Timeout	Verbindungs-Timeout für die Verbindung zum SDA Portal. Drei Sekunden sind ein guter Wert sowohl für eine normale Internetverbindung von zu Hause oder dem Büro aus als auch oft noch für mobile Internetverbindung ab 3G. Falls Sie aber auch mal über eine langsamere Internetverbindung SDA benutzen wollen, erhöhen Sie den Timeout-Wert.
ETS4 Version prüfen	Aufgrund von möglichen Einschränkungen bei der Nutzung der automatischen Suche der KNX/IP Verbindungen mit ETS Versionen älter als ETS4.2 befindet sich hier auch die Möglichkeit zur ETS4 Kompatibilitätsprüfung. Siehe hierzu auch Abschnitt 4.3.1 „Zugriff auf eine KNX-Installation über KNX-IP“.

4.2 Über den SDA Client mit einem SDA Connector verbinden

Für den Verbindungsaufbau zu einem SDA Connector gibt es zwei Möglichkeiten: den Quick Connect (siehe Abschnitt 1.3.2. „Quick Connect“) und den Portal Connect (siehe Abschnitt 1.3.3. „SDA Portalserver“)

Zuerst wählen Sie daher nach dem Start des SDA Clients den Verbindungstyp aus.

4.2.1 Verbindung via Quick Connect herstellen

Wählen Sie „Quick Connect“ als Verbindungstyp (siehe Abbildung 13). Danach geben Sie in das Feld „Connector ID“ die Registrierungs-ID an. Wenn Sie einen SDA Connector benutzen möchten, den Sie bereits zu einem früheren Zeitpunkt mit Quick Connect genutzt haben, können Sie diese auch aus der Liste auswählen.

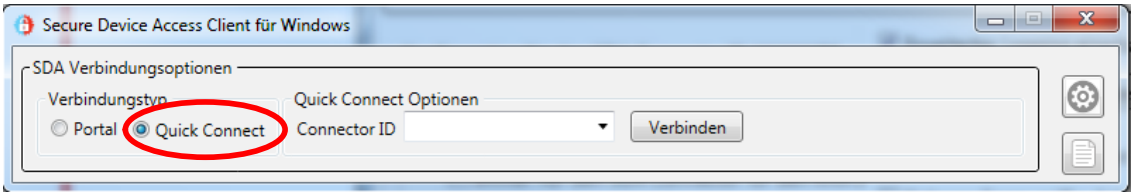


Abbildung 13: SDA Connector über Quick Connect verbinden

Nach Eingabe einer gültigen Registrierungs-ID erscheint die Konfiguration für diesen. Wird der SDA Connector das erste Mal mit diesem Client benutzt, wird eine Default-Konfiguration erzeugt.

Nachdem Sie die Konfiguration ggf. auf Ihre Anwendungen angepasst haben (siehe Abschnitt 4.3 „Konfiguration der Zugriffsoptionen eines SDA Connectors“ ff.), können Sie die Verbindung über die Schaltfläche „Verbinden“ aufbauen.

4.2.2 Verbindung via Portal Connect herstellen

Wählen Sie „Portal Connect“ als Verbindungstyp (siehe Abbildung 14). Danach geben Sie Ihren Portal Benutzernamen (**Hinweis:** Es handelt sich hierbei immer um eine E-Mail-Adresse.) und das zugehörige Passwort ein.

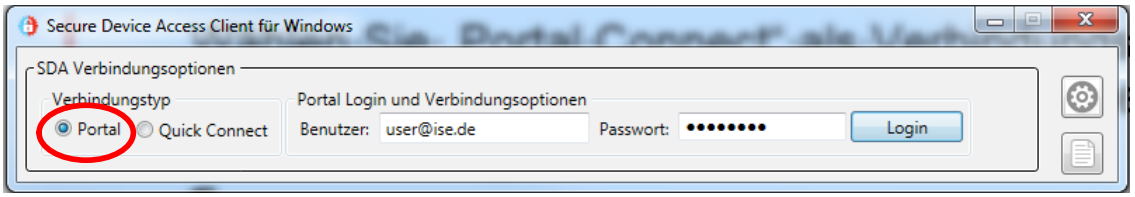


Abbildung 14: Login beim SDA Portal Server

Nachdem Sie sich dann über die Schaltfläche „Login“ beim SDA Portal Server angemeldet haben, erscheint eine Liste mit allen SDA Connectors, für die Ihr Benutzer Zugriffsrechte besitzt.

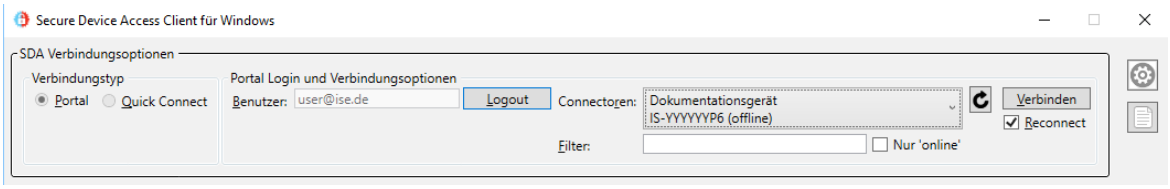


Abbildung 15: SDA Connector über Portal Connect benutzen

Nach Auswahl eines SDA Connectors aus der Liste erscheint die Konfiguration für diesen. Wird der SDA Connector das erste Mal mit diesem Client benutzt, wird eine Default-Konfiguration erzeugt.

Nachdem Sie die Konfiguration ggf. auf Ihre Anwendungen angepasst haben (siehe Abschnitt 4.3 „Konfiguration der Zugriffsoptionen eines SDA Connectors“ ff.), können Sie die Verbindung über die Schaltfläche „Verbinden“ aufbauen.

Darüber hinaus können Sie die Option „Reconnect“ anwählen. Falls Reconnect aktiviert ist, versucht der Windows Client nach einem Verbindungsabbruch (z.B. durch DSL Reconnect) automatisch die Verbindung wiederherzustellen. Diese Option kann auch nach Bedarf zusammen mit der Ausführung Externer Kommandos (s.u.) genutzt werden.

Falls Sie mit mehreren SDA Connectors arbeiten, besteht die Möglichkeit einen Filter zu nutzen. Sie können einen Text eingeben und die Auswahl auch auf die derzeit am Portal angemeldeten („online“) Connectors begrenzen.

4.3 Konfiguration der Zugriffsoptionen eines SDA Connectors

Neben dem HTTP Zugriff, für den kein SDA Client benötigt wird, ist die Standardanwendung des ISE SMART CONNECT KNX REMOTE ACCESS der sichere Fernzugriff auf KNX-Installationen über das KNX/IP Protokoll. Deshalb ist die Konfiguration für diesen Dienst immer sichtbar und standardmäßig aktiviert. Darüber hinaus kann über SDA auch mit dem ise Update Tool bei Bedarf aus der Ferne die Software von ISE SMART CONNECT Geräten aktualisiert werden.

Neben KNX/IP bietet der SDA Client auch den einfachen Zugriff für sichere Fernkonfigurationen des Gira HomeServers. Hier kann zum einen ein Projekt über den 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 SDA Connectors (siehe Abbildung) an- bzw. abschaltbar.

Mit der Option „Externe Kommandos“ ist es möglich, nach dem Herstellen einer Verbindung, als auch nach dem Abbruch einer Verbindung externe Programme auszuführen.

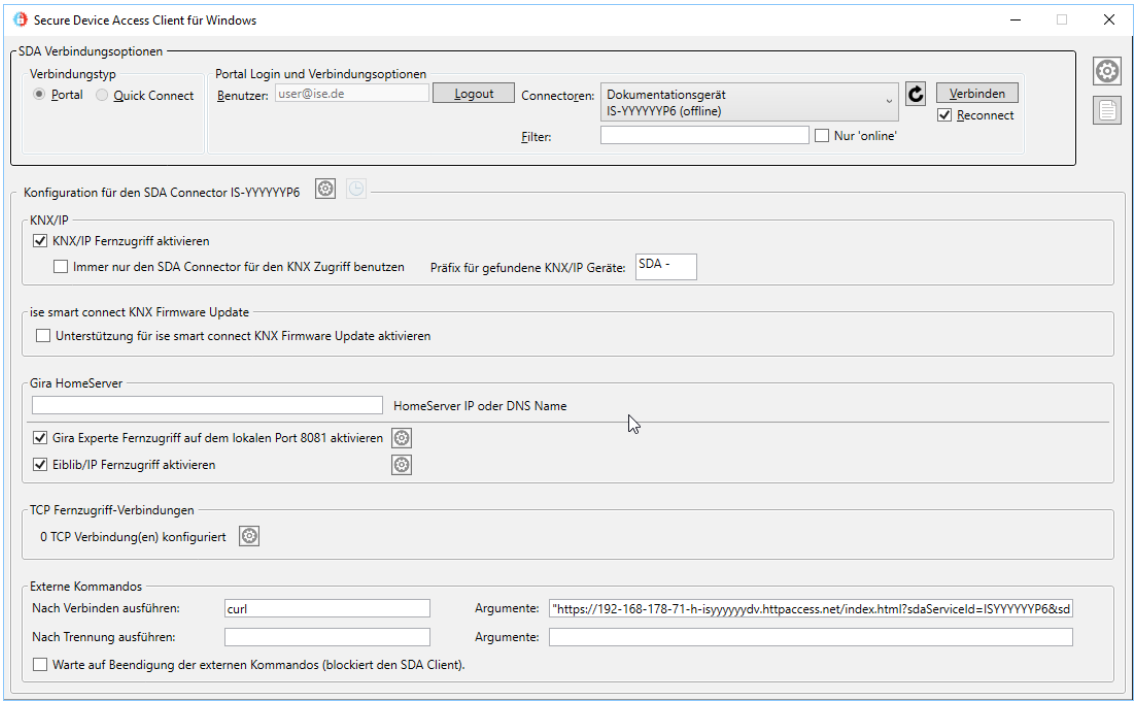


Abbildung 16: SDA Connector Konfigurationsoptionen

4.3.1 Zugriff auf eine KNX-Installation über KNX-IP

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

Wenn der KNX/IP Zugriff erlaubt ist, dann 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 wichtigen Hinweis zur Nutzung mit ETS4 Versionen kleiner ETS4.2 am Ende dieses Abschnitts). Um auf einen Blick zu erkennen, welche Geräte über SDA angebunden sind, kann ein Präfix mit maximal acht Zeichen frei eingegeben werden.

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 ISE SMART CONNECT KNX REMOTE ACCESS über SDA zugänglich machen.

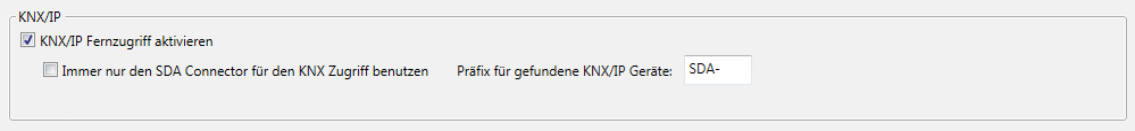


Abbildung 17: KNX/IP Fernzugriffskonfiguration

<u>Wichtiger Hinweis</u>: 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 manuelle eine neue Verbindung, vergeben den Namen nach Ihren Wünschen und kopieren aus dem SDA Client die entsprechende IP Adresse und den Port in die Eingabefelder in der ETS4. Hierzu gibt der SDA Client bei geöffneter Verbindung Hilfestellung, indem Schaltflächen angeboten werden, um die entsprechenden Werte in die Zwischenablage zu kopieren. Beachten Sie hierzu die folgende Abbildung.

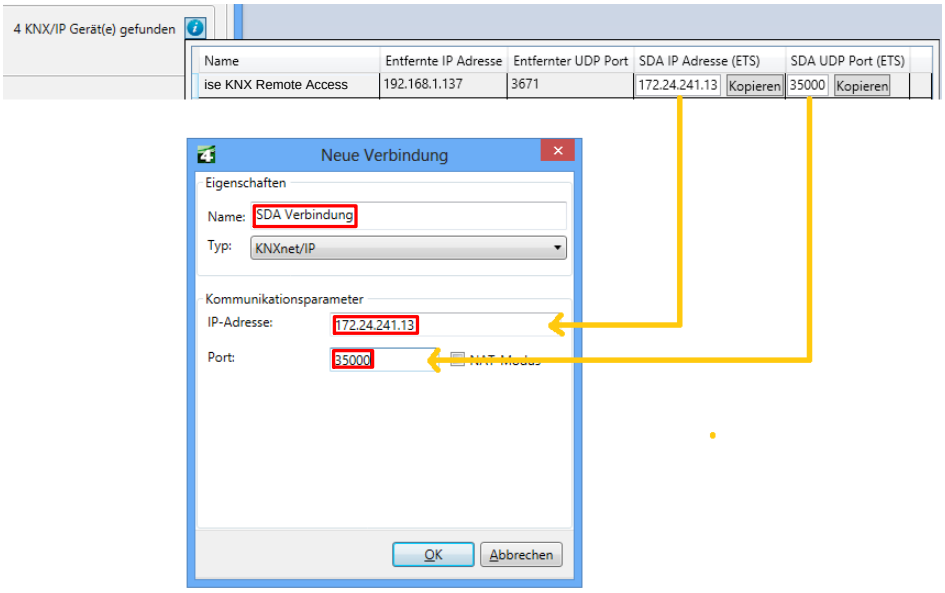


Abbildung 18: Manuelle KNX/IP Interfacekonfiguration für ETS kleiner ETS 4.2

Hinweis: Der SDA 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 SDA Verbindung zur gleichen Installation gültig bleiben.

Hinweis: Die SDA Kommunikation ist speziell für die KNX Kommunikation optimiert, so dass diese auch bei langsamen Internetanbindungen noch zuverlässig funktioniert.

4.3.2 Softwareaktualisierung von ISE SMART CONNECT Geräten

Für die Aktualisierung der Gerätesoftware (Firmware) von ISE SMART CONNECT Geräten ist bei Bedarf das ise Update Tool erhältlich. Wenn Sie im SDA Client die Option für das Firmware Update aktivieren, können Sie mit dem ise Update Tool dann auch aus der Ferne die Software aktualisieren.

Beachten Sie herbei bitte, dass zum Zeitpunkt des Starts des ise Update Tools die SDA Verbindung bereits bestehen sollte.

Eine Beschreibung des Updatevorgangs mit dem ise Update Tools wird mit dem Tool mitgeliefert.

Wichtiger Hinweis: Die Suche und Abfrage der Geräte für das Firmwareupdate verzögert den SDA Verbindungsaufbau spürbar. Bitte aktivieren Sie diese Option daher nur, wenn Sie ein Firmwareupdate durchführen wollen. Darüber hinaus unterstützen viele ISE SMART CONNECT Produkte mittlerweile das Firmwareupdate über die Webseiten des Geräts!

4.3.3 Fernkonfiguration Gira HomeServer und Nutzung von Eiblib/IP

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

Es besteht dann die Möglichkeit, den Fernzugriff für den HomeServer Experten freizugeben. Da der HomeServer über den Port 80 konfiguriert wird, der üblicherweise auf PCs bereits in Benutzung ist, empfehlen wir den Port 8081. Es kann aber auch jeder andere freie Port genutzt werden. Die Ports kleiner 1000 sind aber nicht zu empfehlen.

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.

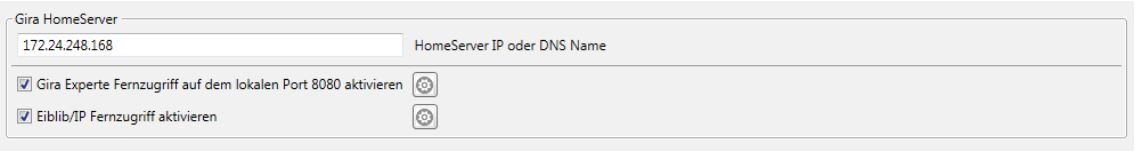


Abbildung 19: Gira HomeServer Fernzugriffskonfiguration

Um mit dem Experten über SDA den HomeServer im entfernten Netzwerk laden zu können, müssen Sie im Dialog „Projekt übertragen“ mit aktiver SDA Verbindung die Option „Andere Adresse“ auswählen, als IP Adresse immer die 127.0.0.1 eintragen, gefolgt vom konfigurierten Port (Standard ist 8081).

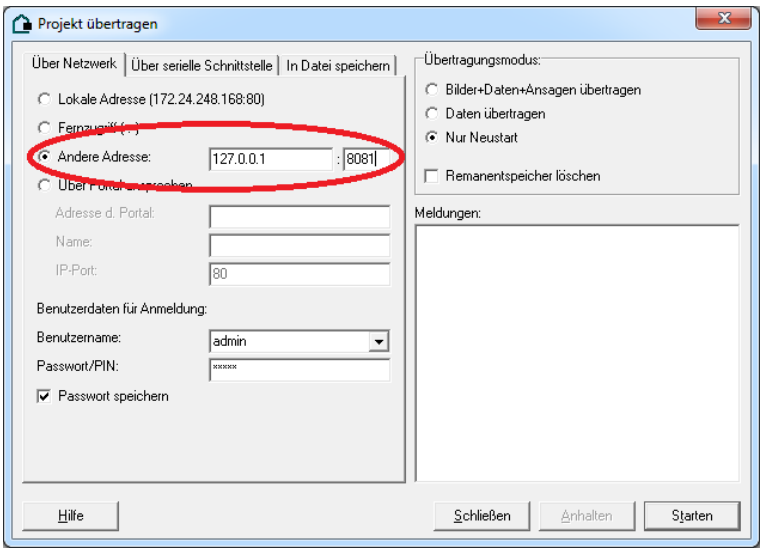


Abbildung 20: Projekt mit Experte über SDA übertragen

Für die Nutzung von Eiblib/IP mit dem 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.

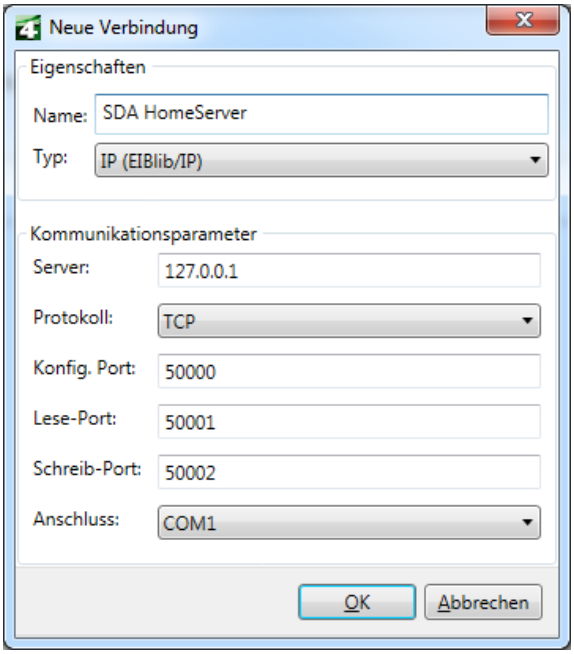


Abbildung 21: HomeServer mit Eiblib/IP über SDA für KNX Anbindung nutzen

4.3.4 Nutzung weitere TCP Protokolle über SDA

Über die Einstellungen bei „TCP Fernzugriff-Verbindungen“ können Sie weitere TCP basierte IP Protokolle über SDA nutzen. 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 lokale vom PC benutzt wird, weshalb die Übersetzung auf einen Port notwendig ist, wie im Beispiel in der folgenden Abbildung.

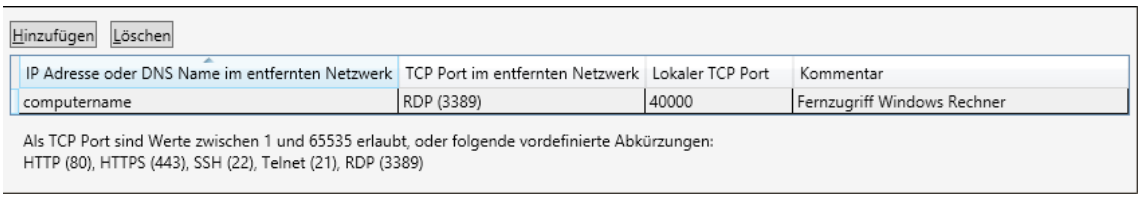


Abbildung 22: TCP Fernzugriffskonfiguration

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 SDA 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:

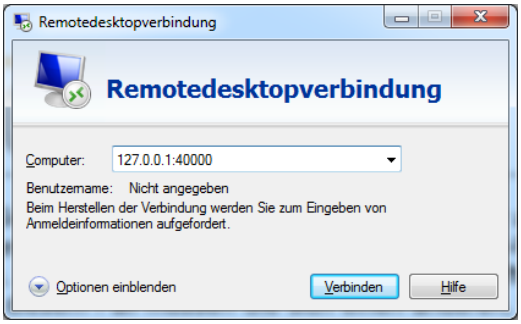


Abbildung 23: Nutzung von Remotedesktop

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.

4.3.5 Externe Kommandos/Programme ausführen

Mit der Option „Externe Kommandos“ ist es möglich, nach dem Herstellen einer Verbindung, als auch nach dem Abbruch einer Verbindung externe Programme auszuführen.

So können z.B. via curl Dateien geladen oder auf das entfernte System kopiert werden, oder nach einem Verbindungsabbruch ein Programm auf dem Client angehalten und nach dem erneuten Verbindungsaufbau wieder gestartet werden. Gerade in Kombination mit der Reconnect Option beim Verbinden (s.o.) sind die Kommandos für Automatisierungen gut nutzbar.

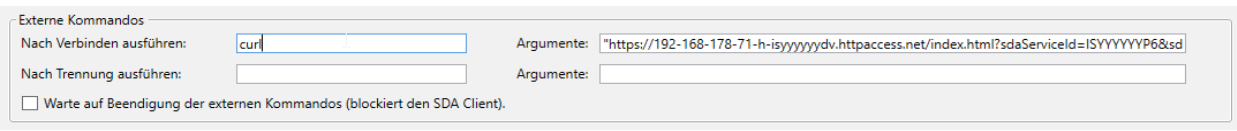


Abbildung 24: Konfiguration Externe Kommandos

In das linke Eingabefeld wird jeweils der Name des Kommandos bzw. Programms, ggf. mit Pfadangabe, eingetragen. Alle Parameter, die zur Ausführung übergeben werden sollen, kommen in das jeweilige Argumente-Eingabefeld.

Darüber hinaus kann konfiguriert werden, ob auf die Beendigung der externen Kommandos gewartet werden soll.

Achtung: Das Warten auf ein Kommando blockiert den Windows Client vollständig, bis das Programm beendet ist.

4.4 Starten der SDA Verbindung und Statusanzeige

Das Starten der sicheren Verbindung zum SDA Connector geschieht für Quick und Portal Connect gleichermaßen über die Schaltfläche „Verbinden“. Im Fehlerfall direkt beim Verbindungsaufbau wird eine entsprechende Fehlermeldung angezeigt.

Wird die Verbindung erfolgreich hergestellt, werden Konfigurationsmöglichkeiten deaktiviert, da bei laufender Verbindung die Konfiguration nicht geändert werden kann.

Im oberen Element wird ein grüner Text mit Datum und Uhrzeit des Verbindungsstarts sowie IP Informationen des lokalen PC und des SDA Connectors im entfernten Netzwerk angezeigt. Dies ist für Diagnosezwecke und zur Informationen für Experten sehr hilfreich.

Für alle drei Verbindungsarten (KNX/IP, Gira HomeServer, TCP) wird gleichermaßen nach dem Start eine Schaltfläche mit einer Info-Grafik 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. In der folgenden Abbildung konnte eine TCP Verbindung nicht hergestellt werden.

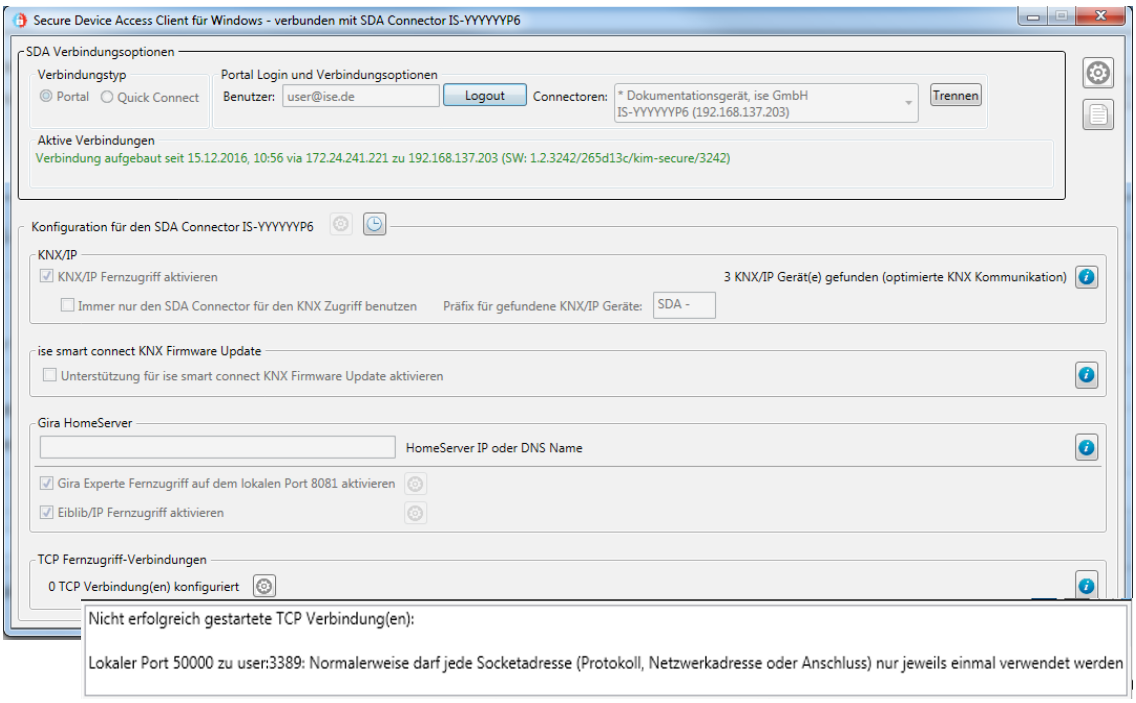


Abbildung 25: Statusinformationen im SDA Client nach Verbindungsaufbau

Wichtiger Hinweis: Das mit Abstand am häufigsten auftretende Problem ist eine Konfiguration, die einen lokalen Port nutzt, der bereits von einer anderen Anwendung genutzt ist. Im Beispiel in der Abbildung ist dies der Port 50000. In diesem Fall ist

die Betriebssystemfehlermeldung „Normalerweise darf jede Socket Adresse (Protokoll, Netzwerkadresse oder Anschluss) nur jeweils einmal verwendet werden“. Wählen Sie in diesem Fall bitte einen anderen lokalen Port aus!

Hinweis für Experten: Unterhalb der Schaltfläche für die Allgemeinen Einstellungen oben rechts befindet sich eine Schaltfläche mit einem beschriebenen Blatt Papier als Bild, welches für Experten detaillierte Verbindungsinformationen in einem Logbuch-Fenster zur Verfügung stellt.

4.5 Messung der Kommunikationsgeschwindigkeit

Durch Betätigen der Schaltfläche mit dem Stoppuhrsymbol rechts neben der Konfigurationsschaltfläche ist es nach dem erfolgreichen Verbinden möglich, eine Zeitmessung für einen Kommunikations-Roundtrip, also die Zeit vom Versenden einer Anfrage in das Zielnetzwerk des SDA Connectors bis zum Erhalt einer Antwort vom SDA Connector, zu messen. Bei schnellen Verbindungen liegt diese Zeit im Bereich von 30-40 Millisekunden und kann entsprechend bei langsamen Verbindungen im Sekundenbereich liegen.

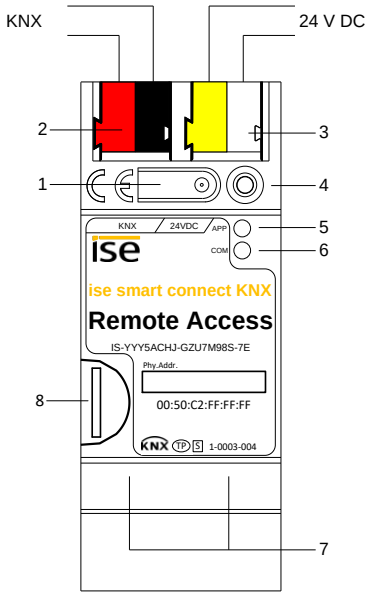
Wichtiger Hinweis: Bei einer Dauer des Kommunikations-Roundtrips von durchschnittlich über fünf Sekunden wird die KNX Kommunikation problematisch.

4.6 Beenden einer SDA Verbindung

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

5 Montage, elektrischer Anschluss und Bedienung

5.1 Geräteaufbau



Abmessungen:

Breite (B):

36 mm (2 TE)

Höhe (H):

90 mm

Tiefe (T):

74 mm

Abbildung 26: ISE SMART CONNECT KNX REMOTE ACCESS

1	Programmier-Taste für KNX	Versetzt das Gerät in den ETS-Programmiermodus oder hebt diesen auf.
2	Anschluss KNX (Twisted Pair)	links: (+ / rot) rechts: (- / schwarz)
3	Anschluss Spannungsversorgung	DC 24...30 V, 2 W (bei 24 V) links: (+ / gelb) rechts: (- / weiß)
4	Programmier-LED KNX (rot)	rot: Gerät ist im ETS-Programmiermodus
5	LED APP (grün)	grün: Normalbetrieb aus / blinkt: Start- bzw. Diagnosecode, siehe 7.2.1 / 7.2.2
6	LED COM (gelb)	gelb: Normalbetrieb (kurze Dunkelphasen zeigen KNX-Telegrammverkehr an) aus / blinkt: Start- bzw. Diagnosecodes, siehe 7.2.1 / 7.2.2
7	Anschluss Ethernet	LED 10/100 Speed (grün) an: 100 MBit/s aus: 10 MBit/s LED Link/ACT (orange) an: Verbindung zum IP-Netz aus: keine Verbindung blinkt: Datenempfang auf IP
8	microSD-Kartenhalter	In der derzeitigen Gerätesoftware wird die SD Karte nicht genutzt. Mediengröße: bis zu 32 GB microSDHC Formatierung: FAT32

5.2 Sicherheitshinweise

Einbau und Montage elektrischer Geräte dürfen nur durch eine Elektrofachkraft erfolgen. Dabei sind die geltenden Unfallverhütungsvorschriften zu beachten. Bei Nichtbeachten der Installationshinweise können Schäden am Gerät, Brand oder andere Gefahren entstehen.

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

Weitere Informationen entnehmen Sie bitte der dem Gerät beigefügten Bedienungsanleitung.

5.3 Montage und elektrischer Anschluss

Gerät montieren

- Aufschnappen auf Hutschiene nach DIN EN 60715, vertikale Montage,
  Netzwerkanschlüsse müssen unten liegen.

Es ist keine KNX/EIB-Datenschiene erforderlich, Verbindung zu KNX-TP wird über die beiliegende eine Busanschlussklemme hergestellt.

Temperaturbereich beachten (0 °C … + 45 °C), nicht oberhalb von Wärme-abgebenden Geräten installieren und ggf. für ausreichende Lüftung/Kühlung sorgen.

Gerät anschließen

- Verbinden Sie die KNX-TP-Busleitung mit dem KNX-Anschluss des Geräts mittels beigefügter KNX-Busanschlussklemme. Die Busleitung muss mit intaktem Mantel bis nahe an die Geräteklemme geführt werden! Busleitungsadern ohne Mantel (SELV) müssen sicher getrennt installiert werden von allen Nicht-Sicherheitskleinspannungsleitungen (SELV/PELV) geschützt werden (Abstand ≥ 4 mm einhalten oder Abdeckungen verwenden, siehe auch VDE-Bestimmungen zu SELV (DIN VDE 0100-410 / „Sichere Trennung“, KNX-Installationsvorschriften)!

- Verbinden der externen Spannungsversorgung mit dem Spannungsversorgungsanschluss (3) des Geräts mit einer KNX-Geräteanschlussklemme, vorzugsweise gelb/weiß.
  Polung: links/gelb: (+), weiß/rechts: (-).

  Hinweis: Wird als Hilfsenergiequelle der „ungedrosselte“ Hilfspannungsausgang einer KNX-Spannungsversorgung genutzt, muss dafür gesorgt werden, dass die Gesamtstromaufnahme inklusive aller KNX-TP-Geräte am Liniensegment nicht den Bemessungsstrom der Spannungsversorgung überschreitet.

- Verbinden von einer oder zwei IP-Netzwerkleitungen mit dem Netzwerkanschluss des Geräts (7).

Abdeckkappe anbringen / entfernen

Zum Schutz der KNX-Bus- und Spannungsversorgungsanschlüsse vor gefährlichen Spannungen insbesondere im Anschlussbereich kann zur sicheren Trennung eine Abdeckkappe aufgesteckt werden.

Das Montieren der Kappe erfolgt bei aufgesteckter Bus- und Spannungsversorgungsklemme und angeschlossener, nach hinten geführter Bus- und Spannungsversorgungsleitung.

- Abdeckkappe anbringen: Die Abdeckkappe wird über die Busklemme geschoben bis sie spürbar einrastet (vgl. Abbildung 27A).
- Abdeckkappe entfernen: Die Abdeckkappe wird entfernt, indem sie seitlich leicht eingedrückt und nach vorne abgezogen wird (vgl. Abbildung 27B).

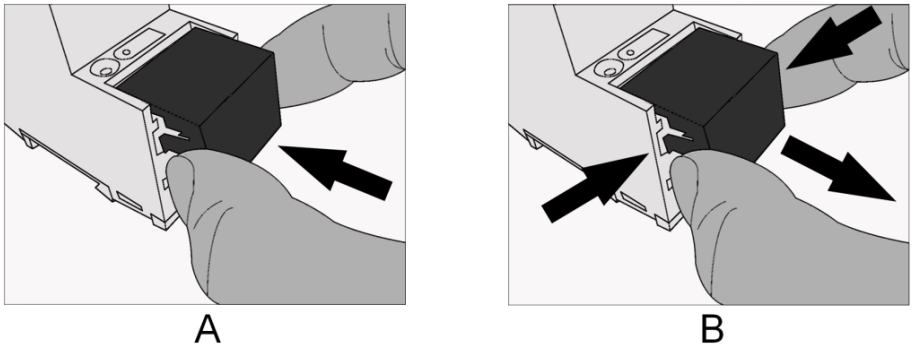


Abbildung 27: Abdeckkappe anbringen / entfernen

6 Projektierung in der ETS

Hinweis: Der ISE SMART CONNECT KNX REMOTE ACCESS ist im Auslieferungszustand bzw. nach einem Factory Reset, bevor er also das erste Mal mit einer ETS geladen wird, folgendermaßen konfiguriert:

- Der Fernzugriff ist grundsätzlich aktiviert, und zwar für die Benutzergruppe „Bewohner“ sowie via „QuickConnect“.
- Die physikalische Adresse ist 15.15.255, die drei zusätzlichen pyhsikalischen Adressen für den Tunneling Server haben alle die Adresse 15.15.254.

Die Projektierung des ISE SMART CONNECT KNX REMOTE ACCESS gliedert sich in folgende Schritte:

Vorbereitungen:	**Erläuterungen siehe**
1 Gerät montieren, mit KNX-Busanschluss und Hilfsspannung verbinden.	→ Kapitel 5
2 Den ISE SMART CONNECT KNX REMOTE ACCESS im IP-Netzwerk mit Internetanschluss installieren.	

Projektierung per ETS:	
Nach der Montage des Gerätes und dem Anschluss von Bus, Spannungsversorgung und Ethernet kann das Gerät in Betrieb genommen werden. Die vorbereitende Projektierung erfolgt mit Hilfe der Engineering Tool Software ETS, erhältlich über die KNX Association, siehe www.knx.org.	
1 ISE SMART CONNECT KNX REMOTE ACCESS als Gerät in der ETS anlegen.	→ Abschnitt 6.1
2 Physikalische Adresse des Geräts sowie die bis zu drei physikalischen Adressen des Interfaces wie üblich entsprechend der KNX-Topologie zuordnen.	
Der ISE SMART CONNECT KNX REMOTE ACCESS benutzt als eines der ersten Geräte auf dem Markt die Möglichkeit der ETS ab ETS4, dass die Schnittstellenadressen bereits im ETS Projekt konfiguriert werden können. Dabei stellt die ETS auch sicher, dass keine Überschneidungen mit anderen Geräten im Projekt stattfinden. Wir empfehlen daher dringend, diese Funktion zu nutzen!	→ Abschnitt 6.2
3 IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse des ISE SMART CONNECT KNX REMOTE ACCESS einstellen oder die Auswahl „IP-Adresse automatisch (von einem DHCP-Server) beziehen“ treffen.	→ Abschnitt 6.3
4 Allgemeine Parameter inklusive ggf. DNS Server zum ISE SMART CONNECT KNX REMOTE ACCESS einstellen.	→ Abschnitt 6.4.1
5 Gruppenadressen an Gruppenobjekte wie üblich anbinden.	→ Abschnitt 0
6 Der ISE SMART CONNECT KNX REMOTE ACCESS ist nun bereit zur Inbetriebnahme mittels *„ETS Programmieren“* und zum Test der Funktionen.	

6.1 Projektierung Schritt 1 – ISE SMART CONNECT KNX REMOTE ACCESS als Gerät in der ETS anlegen

Wenn noch nicht geschehen, importieren Sie die ETS-Geräte-Applikation zum ISE SMART CONNECT KNX REMOTE ACCESS einmalig in den Geräte-Katalog ihrer ETS, beispielsweise indem Sie die Funktion „*Produkte importieren*" auf der Startseite der ETS nutzen.

Die ETS-Applikation können Sie von unserer Website unter www.ise.de kostenlos herunterladen.
Die weiteren Erläuterungen in diesem Dokument beziehen sich auf

Abbildung 28: Produktimport über die ETS4-Startseite

Hardware		Applikations-Software	
Gerät:	ISE SMART CONNECT KNX REMOTE ACCESS	**Applikation**:	ISE SMART CONNECT KNX REMOTE ACCESS
Hersteller:	ise GmbH	**Version:** V4.1	
Bestell-Nr.	1-0003-004		
Version:	V1.0		
Bauform:	REG (Reiheneinbau)		

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"* (ETS 4.2) bzw. „*Applikationsprogramm*" (ETS 5).

Dort können Sie nun mit dem Knopf „*Applikationsprogramm aktualisieren*" (ETS 4.2) bzw. „*Aktualisieren*" (ETS 5) den alten Datenbankeintrag ersetzen. Hierbei gehen bestehende Verknüpfungen mit Gruppenadressen nicht verloren. Das neu hinzugefügte Gerät kann nun wieder gelöscht werden.

In der ETS 4.2 benötigen Sie hierfür eine spezielle Lizenz, ab der ETS 5 ist dies mit jeder Lizenz möglich.

6.2 Projektierung Schritt 2 – Physikalische Adressen zuordnen

Der ISE SMART CONNECT KNX REMOTE ACCESS 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.

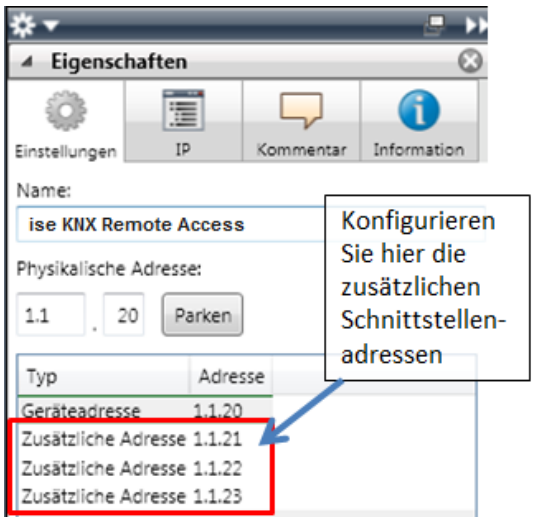


Abbildung 29: Konfigurieren von Adressen

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 bei 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 i.d.R. die zusätzlichen Adressen automatisch vor.

6.3 Projektierung Schritt 3 – IP-Adresse, Subnetzmaske und Adresse des Standardgateways einstellen

Neben der physikalischen Adresse im KNX-Netzwerk muss dem ISE SMART CONNECT KNX REMOTE ACCESS eine Adressierung im IP-Datennetzwerk zugewiesen werden. Dazu gehören folgende Informationen:

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

Dies kann auf zwei Wegen geschehen – über

- automatischen Bezug der Daten von einem DHCP-Server (z. B. im Router des Datennetzwerks integriert) oder
- manuelle Einstellung in der ETS.

Gehen Sie dazu wie folgt vor:

1. Wählen Sie das Gerät in der ETS aus.

2. Zeigen Sie die Eigenschaften des Geräts im Sidebar der ETS an, wie in Abbildung 30 gezeigt.

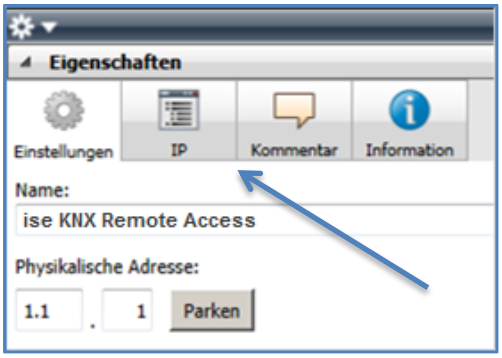


Abbildung 30: Geräte-Eigenschaftendialog der ETS

3. Wählen Sie den Reiter „IP“ entsprechend Abbildung 31. Wählen Sie nun entweder
   ⊙ *IP-Adresse automatisch beziehen (Standard)*

   Die Adressdaten werden automatisch von einem DHCP-Server im Datennetzwerk bezogen.
   oder
   ⊙ *Folgende 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. Abschnitt 6.4 „Allgemeine Parameter einstellen“)!

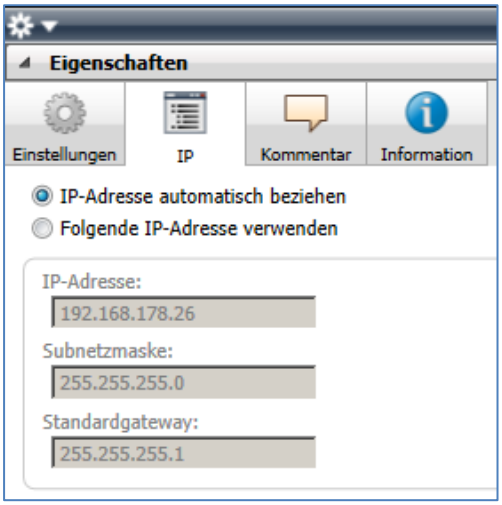


Abbildung 31: Einstellung der IP-Adressdaten des Geräts unter dem Reiter „IP“ im Sidebar der ETS

Bei der Einstellung ⊙ *IP-Adresse automatisch beziehen* muss ein DHCP-Server dem ISE SMART CONNECT KNX REMOTE ACCESS 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 steh, wird dem Gerät automatisch eine neue IP-Adresse zugewiesen.

6.4 Allgemeine Parameter einstellen

6.4.1 Parameter-Seite *Allgemein*

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

Parameter	Eintrag / Auswahl	Bemerkungen
DNS Server (falls kein DHCP)	**Standard Gateway**	Die IP-Adresse des Standardgateways wird verwendet (siehe Abschnitt 6.3 Projektierung Schritt 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.
Fernzugriff generell	**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 SDA Portal Server aufzubauen nach jedem Neustart.
	deaktiviert	Verbietet dem Gerät eine Verbindung zum SDA Portal Server aufzubauen nach jedem Neustart.
Fernzugriff für die Gruppe „Bewohner“, für die Gruppe „Installateure“ oder via „Quick Connect“ nach Neustart	**wie vor Neustart**	Der Fernzugriffstatus der jeweiligen Gruppe bzw. „Quick Connect“ 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 bzw. „Quick Connect“ nach jedem Neustart.
	deaktiviert	Verbietet den Fernzugriff für die jeweilige Gruppe bzw. „Quick Connect“ bei jedem Neustart.

Parameter	Eintrag / Auswahl	Bemerkungen
Anzahl der SDA Benachrichtigungsobjekte	**0**|1...|49|50	Hier wird die Anzahl der SDA Benachrichtigungsobjekte festgelegt (max. 50). Entsprechend der Auswahl werden die Gruppenobjekte „101 ff“ sichtbar.
Trennzeichen für Fließkommazahlen	„,“ „.“	

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

Tabelle 2SDA Benachrichtigung „N“

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 Bytes, DPT 9.*) Text (14 Bytes, DPT 16.001)	Der gewünschte Datentyp der jeweiligen SDA Benachrichtigung kann ausgewählt werden.
Benachrichtigung nur bei Wertänderung	„ “ „✓“	
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	Text	Der Filter kann aus einem festen Wert oder bis zu zwei Bedingungen bestehen. Beim DPT 1.001 (Bool) ist der Filter über eine Auswahlliste möglich. Beschreibung siehe Parameterdialog.
Priorität	Niedrig Hoch Alarm	
Kategorie	Text	Kann zum Filtern der SDA Benachrichtigungen und deren Weiterleitungen auf dem SDA Portal genutzt werden.
Betreff	Text	Beschreibung siehe Parameterdialog. Wird beim Versand von Emails als „Betreff“ genutzt.
Text	Text	Beschreibung siehe Parameterdialog. Wird beim Versand von E-Mails als „Text“ genutzt.
Anhang hinzufügen	„Nein“ „Ja“	
URL des Anhangs	Text	Nur http-Anfragen werden unterstützt. Beachten Sie die maximal zulässige Dateigröße von 250kByte.

6.5 Gruppenadressen an Gruppenobjekte anbinden

Am ISE SMART CONNECT KNX REMOTE ACCESS stehen die folgenden Gruppenobjekte zur Anbindung von Gruppenadressen bereit.

Wichtiger Hinweis für alle Gruppenobjekte, die eine laufende Verbindung signalisieren: Bei der Nutzung des HTTP Zugriffs, also ohne SDA 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 SDA Portalserver zusammen. HTTP Verbindungen können bis zu fünf Minuten benötigen, bis sie geschlossen werden. Das heißt, dass die entsprechenden Gruppenobjekte, die eine aktive Verbindung signalisieren, das Schließen auch erst zu diesem Zeitpunkt signalisieren. Bei der Nutzung des SDA Clients hingegen erfolgt der Verbindungsabbau synchron.

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
1	Fernzugriff zulassen	Schreiben	1 Bit	1.003	K-S--
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Erlaubt oder verbietet dem Gerät eine Verbindung zum SDA Portal Server 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	Fernzugriff zulassen – Status	Lesen	1 Bit	1.003	KL-Ü-
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Zeigt an, ob das Gerät eine Verbindung zum SDA Portal Server aufbauen darf.				
Beschreibung:	1 = Erlaubt, 0= Verboten				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
3 (Bewohner) 5 (Installateure) 7 (Quick Connect)	Fernzugriff zulassen	Schreiben	1 Bit	1.003	K-S--
Rubrik:	Fernzugriff	Datentyp:	Freigeben		
Funktion:	Erlaubt oder verbietet den Fernzugriff jeweils für Mitglieder der Gruppe bzw. über „Quick Connect“.				

Beschreibung: 1 = Erlauben, 0= Verbieten

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
4 (Bewohner) 6 (Installateure) 8 (Quick Connect)	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 bzw. über „Quick Connect" zugelassen ist.

Beschreibung: 1 = Erlaubt, 0= Verboten

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
20	Status Portalverbindung	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	Zustand Fernzugriffsverbindung	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 (Installateure) 24 (Quick Connect)	Zustand Fernzugriffsverbindung	Lesen	1 Bit	1.011	KL-Ü-

Rubrik: Fernzugriffsverbindung

Datentyp: Status

Funktion: Zeigt an, ob eine Fernzugriffsverbindung jeweils für die Gruppe bzw. über „Quick Connect" derzeit aktiv ist.

Eine aktive Verbindung wird ggf. auch für eine andere Gruppe signalisiert, wenn einem Mitglied dieser Gruppe per Quick Connect oder 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)
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 Webseite des ISE SMART CONNECT KNX REMOTE ACCESS Geräts.

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)
101 - 150	SDA Benachrichtigung Auslöser Nr. 1/2/3/…/49/50	Schreiben	1 Bit	1.001	K-S--

Rubrik:	Schalten	Datentyp:	Ein/Aus
Funktion:	Sendet eine SDA Benachrichtigung zum SDA Portal Server. Der boolsche Wert kann in der SDA Benachrichtigung mitgesendet werden.		
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Gruppenadressen „101 bis 150". Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Abschnitt 6.4.1 „Parameter-Seite *Allgemein*").		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	SDA Benachrichtigung Auslöser Nr. 1/2/3/…/49/50	Schreiben	1 Byte	5.001	K-S--

Rubrik:	Prozent	Datentyp:	Prozent (0..100%)
Funktion:	Sendet eine SDA Benachrichtigung zum SDA Portal Server. Der Prozentwert kann in der SDA Benachrichtigung mitgesendet werden.		
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Gruppenadressen „101 bis 150". Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Abschnitt 6.4.1 „Parameter-Seite *Allgemein*").		

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	SDA Benachrichtigung Auslöser Nr. 1/2/3/…/49/50	Schreiben	1 Byte	5.010	K-S--
Rubrik:	Zähler	Datentyp:			
Funktion:	Sendet eine SDA Benachrichtigung zum SDA Portal Server. Der Prozentwert kann in der SDA Benachrichtigung mitgesendet werden.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Gruppenadressen „101 bis 150". Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Abschnitt 6.4.1 „Parameter-Seite *Allgemein*").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	SDA Benachrichtigung Auslöser Nr. 1/2/3/…/49/50	Schreiben	2 Byte	9.*	K-S--
Rubrik:	Fließkomma	Datentyp:	KNX-Fließkomma (floating point)		
Funktion:	Sendet eine SDA Benachrichtigung zum SDA Portal Server. Der Fließkommawert kann in der SDA Benachrichtigung mitgesendet werden.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Gruppenadressen „101 bis 150". Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Abschnitt 6.4.1 „Parameter-Seite *Allgemein*").				

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
101 - 150	SDA Benachrichtigung Auslöser Nr. 1/2/3/…/49/50	Schreiben	14 Bytes	16.001	K-S--
Rubrik:	Text	Datentyp:	Zeichen (ISO 8859-1)		
Funktion:	Sendet eine SDA Benachrichtigung zum SDA Portal Server. Der Textwert kann in der SDA Benachrichtigung mitgesendet werden.				
Beschreibung:	Dies ist einer von 5 möglichen DP-Typen für die 50 Gruppenadressen „101 bis 150". Die Festlegung des DP-Typs erfolgt durch eine entsprechende Auswahl unter den Allgemeinen Parametern (siehe Abschnitt 6.4.1 „Parameter-Seite *Allgemein*").				

7 Inbetriebnahme

7.1 Bedienung

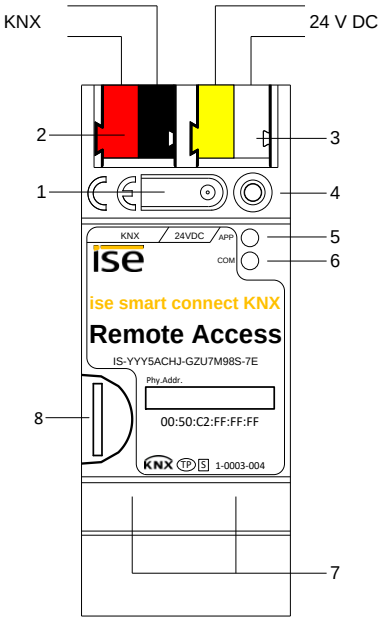


Abbildung 32: ISE SMART CONNECT KNX REMOTE ACCESS

1	Programmier-Taste für KNX	Versetzt das Gerät in den ETS-Programmiermodus oder hebt diesen auf.
2	Anschluss KNX (Twisted Pair)	links: (+ / rot) rechts: (- / schwarz)
3	Anschluss Spannungsversorgung	DC 24...30 V, 2 W (bei 24 V) links: (+ / gelb) rechts: (- / weiß)
4	Programmier-LED KNX (rot)	rot: Gerät ist im ETS-Programmiermodus
5	LED APP (grün)	grün: Normalbetrieb aus / blinkt: Start- bzw. Diagnosecode, siehe 7.2.1 / 7.2.2
6	LED COM (gelb)	gelb: Normalbetrieb (kurze Dunkelphasen zeigen KNX-Telegrammverkehr an) aus / blinkt: Start- bzw. Diagnosecodes, siehe 7.2.1 / 7.2.2
7	Anschluss Ethernet	LED 10/100 Speed (grün) an: 100 MBit/s aus: 10 MBit/s LED Link/ACT (orange) an: Verbindung zum IP-Netz aus: keine Verbindung blinkt: Datenempfang auf IP
8	microSD-Kartenhalter	In der derzeitigen Gerätesoftware wird die SD Karte nicht genutzt. Mediengröße: bis zu 32 GB microSDHC Formatierung: FAT32

7.2 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.

7.2.1 LED-Statusanzeige beim Gerätestart

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

LED „APP“ (grün)	LED „COM“ (gelb)	Bedeutung	
○ aus	○ aus	Fehler: Keine Versorgungsspannung: Bitte Anschlüsse und Spannungsversorgung prüfen.	×
○ aus	● gelb	Gerät startet.	✓
○……● grün blinken langsam (ca. 1 Hz)	● gelb	Hinweis: Das Gerät ist komplett hochgefahren, aber noch unparametriert. Ein ETS Download ist notwendig.	×
○……● grün blinken schnell	○ aus	Fehler: Bitte kontaktieren Sie den Support. Die Firmware kann nicht gestartet werden.	×
●…○…●…○…●… grün ○…●…○…●…○… gelb blinken langsam im Wechsel (ca. 1Hz)		Fehler: Bitte kontaktieren Sie den Support. Die neu geladene Firmware kann nicht gestartet werden. Das System versucht, die bisherige Firmware zu aktivieren (Ungültige Firmware).	×

7.2.2 LED-Statusanzeige im Betrieb

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

LED „*APP*" (grün)	Bedeutung
● grün	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.
●...○ Einmal blinken langsam, mit 1 Hz, dann 2 s Pause	Hinweis: Kein Fernzugriff erlaubt. Das Gerät verbindet sich nicht mit dem SDA Portal Server, ein Fernzugriff ist technisch unmöglich.
●...○...●...○...●...○ Dreimal blinken langsam, mit 1 Hz, dann 2 s Pause	Hinweis: Der Fernzugriff ist für mindestens eine Gruppe bzw. „Quick Connect" erlaubt und es gibt mindestens eine aktive Verbindung. Der Fernzugriff ist also in Benutzung.

LED „COM" (gelb)	Bedeutung
● gelb	Normalbetrieb: KNX-Verbindung ist hergestellt, kein KNX-Telegrammverkehr.
●...○...●...○...●...○ schnelles gelbes Blinken mit kurzen Dunkelphasen	Normalbetrieb: KNX-Verbindung ist hergestellt, KNX-Telegrammverkehr.
○ aus	Fehler: Verbindung zu KNX ist unterbrochen. Prüfen Sie die Busverbindung.

7.3 Übertragung beschleunigen: Übertragungsweg *KNX-TP* oder *IP* wählen

Die Programmierung (Übertragung von der ETS zum Gerät) erfolgt in der Programmierumgebung der ETS. Für die Übertragung wird keine zusätzliche KNX/EIB-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.

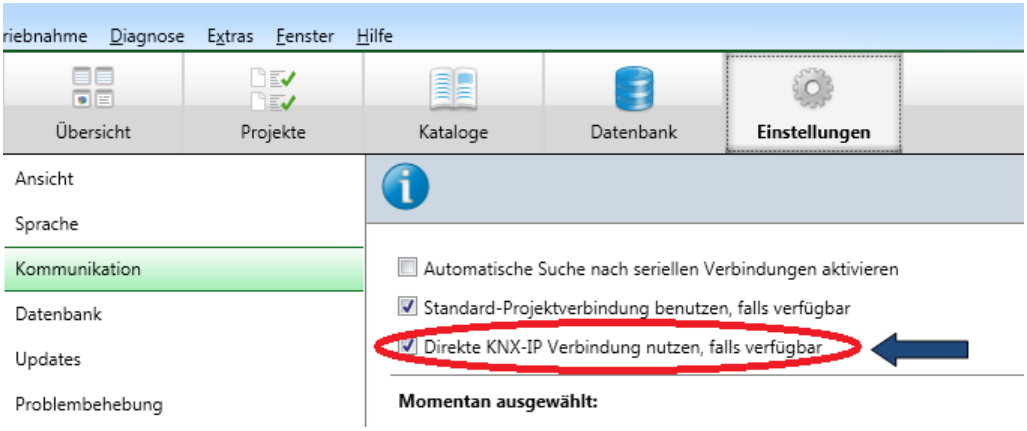


Abbildung 33: Die Einstellung *„Direkte KNX-IP-Verbindung nutzen, falls verfügbar"* beschleunigt die Übertragung von der ETS zum Gerät

Für die Übertragung der ETS über die IP-Seite setzen Sie die Einstellung

☑ *Direkte KNX-IP-Verbindung nutzen, falls verfügbar.*

unter ETS-Startseite → Tab *Einstellungen* → Eintrag *Kommunikation.*

7.4 Physikalische Adresse des Geräts programmieren

- Stellen Sie sicher, dass Gerät und Busspannung eingeschaltet sind.
- Stellen Sie sicher, dass die Programmier-LED (4) nicht leuchtet.
- Programmiertaste (1) kurz drücken – Programmier-LED (4) leuchtet rot.
- 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* im Side-Bar (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.

Wichtiger Hinweis: Die zusätzlichen Adressen des Tunneling Servers, den der ISE SMART CONNECT KNX REMOTE ACCESS mitbringt und der bis zu drei Verbindungen unterstützt, werden ebenfalls über die ETS bei den Eigenschaften des Geräts konfiguriert.

7.5 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.

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

7.6 An Gerätewebseite anmelden

Über die Applikation „Gerätewebseite“ können Sie auf ISE SMART CONNECT KNX REMOTE ACCESS zugreifen.

Startseite der Gerätewebseite aufrufen

Rufen Sie die Gerätewebseite über einen der nachfolgenden Wege auf:

- Geben Sie die IP-Adresse des Geräts in die Adresszeile Ihres Browsers ein.
- Alternativ wählen Sie das Gerät in der Netzwerkumgebung (s. Abbildung 34): Doppelklicken Sie das Icon des Geräts.

Abbildung 34: Aufruf der Gerätewebseite über Netzwerkumgebung

Die Startseite der Gerätewebseite wird angezeigt. Die Gerätewebseite ist passwortgeschützt.

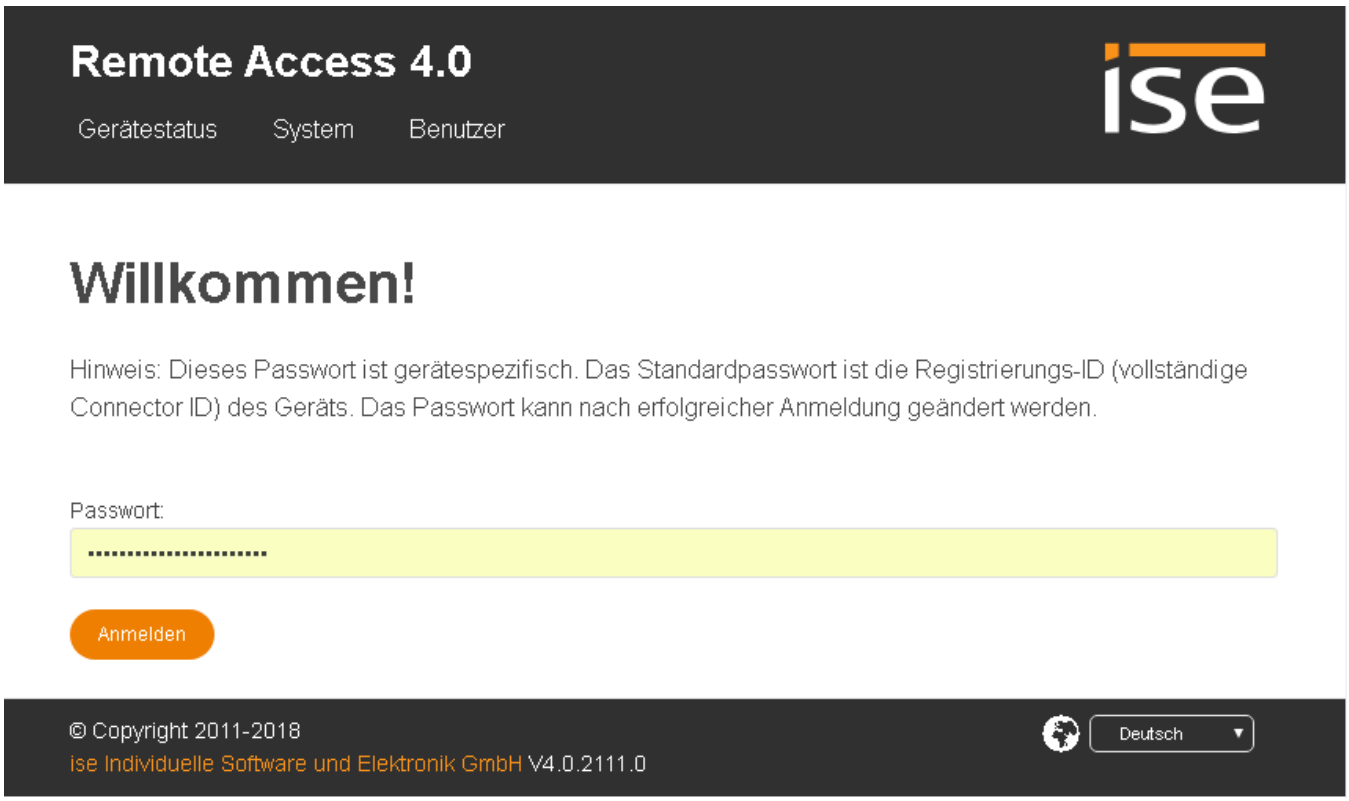


Abbildung 35: Startseite der Gerätewebseite

An Gerätewebseite anmelden

1. Bei Ihrer ersten Anmeldung geben Sie im Feld „Passwort“ die Registrierungs-ID des Geräts ein.
   Die Registrierungs-ID finden Sie auf einem Produktaufkleber des Geräts (1). Beachten Sie die Groß- und Kleinschreibung (case-sensitive).
2. Wählen Sie die Schalfläche „Anmelden“.
3. Nach dem Anmelden ändern Sie Ihr Passwort.

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen, müssen Sie wieder das initiale Passwort „Registrierungs-ID des Geräts“ verwenden.

Passwort ändern

1. Wählen Sie in der Menüleiste „Benutzer“ → „Passwort ändern“.
2. Geben Sie auf der Seite „Passwort ändern“ ihr aktuelles Passwort und das neue Passwort ein.
3. Wählen Sie die Schaltfläche „Speichern“.

7.7 Werksreset

Werksseitig voreingestellt ist folgende physikalische KNX-Adresse:15.15.255

Nach dem Werksreset verhält sich das Gerät wie im Auslieferzustand. Für die Gerätewebseite gilt als Passwort dann wieder die Registrierungs-ID des Geräts. Das Gerät ist unprojektiert. Dies ist nach dem Hochfahren des Gerätes an der langsam blinkenden grünen APP-LED (5) zu erkennen.

7.7.1 Über die Programmiertaste am Gerät

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

- Sicherstellen, dass das Gerät ausgeschaltet ist.
- Programmiertaste (1) drücken, gedrückt halten und das Gerät einschalten.
- Programmiertaste (1) gedrückt halten bis die Programmier-LED (4), die RUN-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 RUN-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.

7.7.2 Über die Webseite des Gerätes

Der Werksreset kann auch über die Webseite des Gerätes ausgelöst werden.

- Rufen Sie die Gerätewebseite auf und melden Sie sich an (s. Abschnitt 7.6 „An Gerätewebseite anmelden“, S. 62).
- Auf der Webseite in der oberen Menüleiste *Device Status* auswählen.
- Auf der Status-Seite in der oberen Menüleiste *Factory Reset* auswählen.
- Bei der Sicherheitsabfrage den Werksreset bestätigen.
- Die nachfolgend angezeigte Seite *Factory Reset* zeigt die Durchführung des Werksresets an. Sobald dieser abgeschlossen ist, wird wieder die Startseite geladen.

7.8 Information Anzeigen über die Webseite

Der Aufruf der Webseite ist im Abschnitt 7.6 "An Gerätewebseite anmelden“, S. 62, beschrieben.

Die Startseite des Geräts zeigt nach erfolgreicher Anmeldung die System Information, die System Configuration und die Application Information.

Wichtiger Hinweis: Falls der ISE SMART CONNECT KNX REMOTE ACCESS gerade neu gestartet wurde, kann der angezeigte Verbindungsstatus mit dem Portalserver für einen kurzen Moment nach dem Hochfahren falsche Werte anzeigen, falls diese gerade zeitgleich erstmalig aktualisiert werden.

Allgemein gilt, dass die Webseite nicht automatisch aktualisiert wird, verwenden Sie bitte hierfür die entsprechende Funktion Ihres Webbrowsers.

7.9 Firmwareupdate des Gerätes

7.9.1 Firmwareupdate über die Gerätewebseite

Der ISE SMART CONNECT KNX REMOTE ACCESS bietet die Möglichkeit, Firmwareupdates über die Gerätewebseite zu installieren. Wählen Sie hierzu über die Gerätewebseite den Menüpunkt *Firmware aktualisieren*. Nun sucht der ISE SMART CONNECT KNX REMOTE ACCESS automatisch auf dem Update-Server nach einer neueren Version und zeigt die aktuelle Firmwareversion sowie ggf. die Version eines verfügbaren Updates an. Ist eine neuere Version verfügbar, so wird auch die zugehörige Beschreibung der Version angezeigt.

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 den Knopf *Firmware aktualisieren* gestartet werden. Im Falle einer möglichen Inkompatibilität muss das Update zur Sicherheit nochmals bestätigt werden.

7.9.2 Lokales Firmwareupdate ohne Internetzugang

Zusätzlich zu einem Online-Update ist ein lokales Update ohne Internetzugang möglich. Dies ist für Geräte gedacht, welche an ihrem Einbauort keine Internetanbindung haben und nur über das lokale Netzwerk zu erreichen sind. Die Firmwaredatei kann über den Knopf *Datei auswählen* lokal ausgewählt werden und anschließend über den Knopf *Firmware aktualisieren* gestartet werden. In diesem Fall ist der Anwender dafür verantwortlich sicherzustellen, dass das Update kompatibel ist (siehe Abschnitt 7.9.3 „Kompatibilität zwischen Katalogeintrag und Firmware“). Ein Downgrade auf eine ältere Version ist mit diesem Verfahren nicht möglich.

7.9.3 Kompatibilität zwischen Katalogeintrag und Firmware

Die Versionsnummern des 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 dabei keine Bedeutung für die Kompatibilität. Sie signalisiert lediglich Updates innerhalb der Version.

Wenn eine neue Firmware eine höhere Hauptnummer hat, so 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.

8 Technische Daten

KNX-Medium	TP
Inbetriebnahme Modus	S-Mode (ETS)
Versorgung KNX	DC 21…30 V SELV
Anschluss KNX	Busanschlussklemme
Externe Versorgung	
Spannung	DC 24...30V ±10%
Anschluss	Busanschlussklemme, vorzugsweise gelb (+) / weiß (-)
Leistungsaufnahme	typ. 2 W (bei DC 24 V, zwei Ethernet-Leitungen verbunden)
IP-Kommunikation	Ethernet 10 /100 BaseT (10/100 MBit/s)
Anschluss IP	2 x RJ45
Unterstützte Protokolle	ARP, ICMP, IGMP, UDP/IP, DHCP, AutoIP
	KNXnet/IP gemäß KNX System Spezifikation: Core, Device Management
microSD-Karte	max. 32 GByte microSDHC
Umgebungstemperatur	0 °C bis +45 °C
Lagertemperatur	-25 °C bis +70 °C
Einbaubreite	36 mm (2 TE)
Einbauhöhe	90 mm
Einbautiefe	74 mm
Schutzart	IP20 (nach EN60529)
Schutzklasse	III (nach IEC 61140)
Prüfzeichen	KNX, CE

9 Häufig gestellte Fragen (FAQ)

Wie finde ich die IP-Adresse meines ISE SMART CONNECT KNX REMOTE ACCESS?

Bitte lesen Sie dies im Abschnitt 7.7.2 „Über die Webseite des Gerätes“ nach.

Wieviel Internet-Datenverkehr (Traffic) entsteht, wenn ich den SDA Connector mit dem Portal verbunden habe?

Für das Aufrechterhalten der Verbindung entstehen ca. 400 Byte Datenverkehr/Minute. Dies entspricht ca. 560kB/Tag bzw. 16,5MB/Monat. Dieses Datenvolumen wird vom SDA Portal *nicht* als Nutzdaten im Sinne der Begrenzung des Datenvolumens im Lizenzvertrag zum ISE SMART CONNECT KNX REMOTE ACCESS angerechnet.

Welchen Kommunikationskanal benutzt der SDA Connector zum Portal?

Der SDA Connector kommuniziert mit dem SDA Portal 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. Falls nötig, sollte als URL *.securedeviceaccess.net eingetragen werden.

Warum muss ich Cookies aktiviert haben, um SDA zu benutzen?

Für die Absicherung der Zugriffe werden von SecureDeviceAccess Cookies benutzt. Wir verwenden Cookies ausschließlich zur Sicherung der Verbindung. Es erfolgt kein Tracking oder Austausch mit Dritten! So etwas finden wir nämlich extrem uncool.

Gibt es Software-Updates für mein ISE SMART CONNECT KNX REMOTE ACCESS-Gerät?

Informationen zu Software-Updates finden Sie im Abschnitt 7.9 „Firmwareupdate des Gerätes“.

Mit welchen Protokollen kann ich auf Geräte im entfernten Netzwerk zugreifen?

Ohne Installation der Software SDA Client 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 SDA 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 Gruppenobjekte bei der Nutzung des HTTP Zugriffs nach dem Schließen meines Browsers nicht sofort, dass keine Verbindung mehr besteht?

Sie finden eine ausführliche Beschreibung hierzu im Abschnitt 0 „

Gruppenadressen an Gruppenobjekte anbinden

In meiner ETS4 erscheinen nicht automatisch die KNX/IP Schnittstellen, die über den SDA Client veröffentlich sind. Warum ist das so?

Mit ETS4 Versionen älter als ETS4.2 kann es zu diesem Problem kommen. Lesen Sie hierzu bitte Abschnitt 4.3.1 „Zugriff auf eine KNX-Installation über KNX-IP ".

Wie kann ich die drei Physikalischen Adressen der KNX/IP ETS Schnittstellen (Tunnel ling Server) im ETS Projekt konfigurieren?

Lesen Sie hierzu bitte Abschnitt 6.2 „Projektierung Schritt 2 – Physikalische Adressen zuordnen".

Kann ich die drei KNX/IP ETS Schnittstellen für Download, Gruppen- und Busmonitor benutzen?

Ja, die Schnittstellen unterstützen alle Downloadoperationen sowie den Gruppen- und Busmonitor.

Ist die Webseite meines ISE SMART CONNECT KNX REMOTE ACCESS 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. Das ISE SMART CONNECT KNX REMOTE ACCESS benötigt die ETS ab Version 4.2 bzw. 5.0.2 oder höher.

Ist der Portalserver wirklich nötig?

Klare Antwort: Leider ja! Für uns wäre es auch einfacher, wenn wir keinen Server betreiben müssten. Es gibt heute aber keine saubere technische Lösung, die unsere Anforderungen an Stabilität und Sicherheit erfüllt. 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 von Ihnen 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 SDA Server laufen müssen (s. o.), ist eine Dauernutzung, insbesondere z.B. mit Videostreaming, sehr leistungsintensiv. Um grundsätzliche eine gute Performance zu garantieren sind daher gewisse Einschränkungen notwendig.

Solten Sie Anwendungsfälle haben, die über diese Bedingungen hinausgehen kontaktieren Sie uns bitte gerne. Lizenzmodelle mit erweitertem Umfang sind für die Zukunft nicht ausgeschlossen.

Wenn ich eine Webseite über SDA aufrufe, funktioniert diese nicht mehr richtig, obwohl sie lokal funktioniert. Was kann das sein?

Nicht alle Webseiten können aus dem entfernten Netzwerk über SDA geladen werden. Insbesondere komplexere Seiten (z.B. mit Java Implementierungen) können ggf. nicht funktionieren. Bitte senden Sie uns in solch einem Fall gerne an den Support (siehe Kapitel 10 „Fehlersuche und Support“) eine E-Mail mit der genauen Produktbeschreibung, Screenshots und einer kurzen Fehlerbeschreibung. Wir bemühen uns um Unterstützung möglichst vieler Produkte über den sicheren SDA HTTP Zugriff.

Ich habe einen partiellen Download mit der ETS4 durchgeführt und nun funktioniert die Gruppenkommunikation nicht. Warum?

In der ETS4 gibt es leider 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 Webseite des ISE SMART CONNECT KNX REMOTE ACCESS noch die vorher konfigurierten physikalischen und IP Adresse?

Die Webseite wird derzeit nach dem Entladen erst nach einem Geräteneustart aktualisiert.

10 Fehlersuche und Support

Wenn Sie ein Problem mit Ihrem ISE SMART CONNECT KNX REMOTE ACCESS haben und Support benötigen, senden Sie bitte eine E-Mail mit einer aussagekräftigen Fehlerbeschreibung sowie den Logfiles nach Auftreten des Fehlers an support@ise.de. Wie Sie die Logfiles von Ihrem ISE SMART CONNECT KNX REMOTE ACCESS herunterladen können, finden Sie im Abschnitt 10.1 „Download Logfiles im Falle eines Problems“.

10.1 Download Logfiles im Falle eines Problems

Im Falle eines Problems werden für den Support die Logfiles benötigt. Diese lassen sich über die Webseite des Gerätes (siehe Abschnitt 7.7.2 „Über die Webseite des Gerätes“) herunterladen. Gehen Sie dazu folgendermaßen vor:

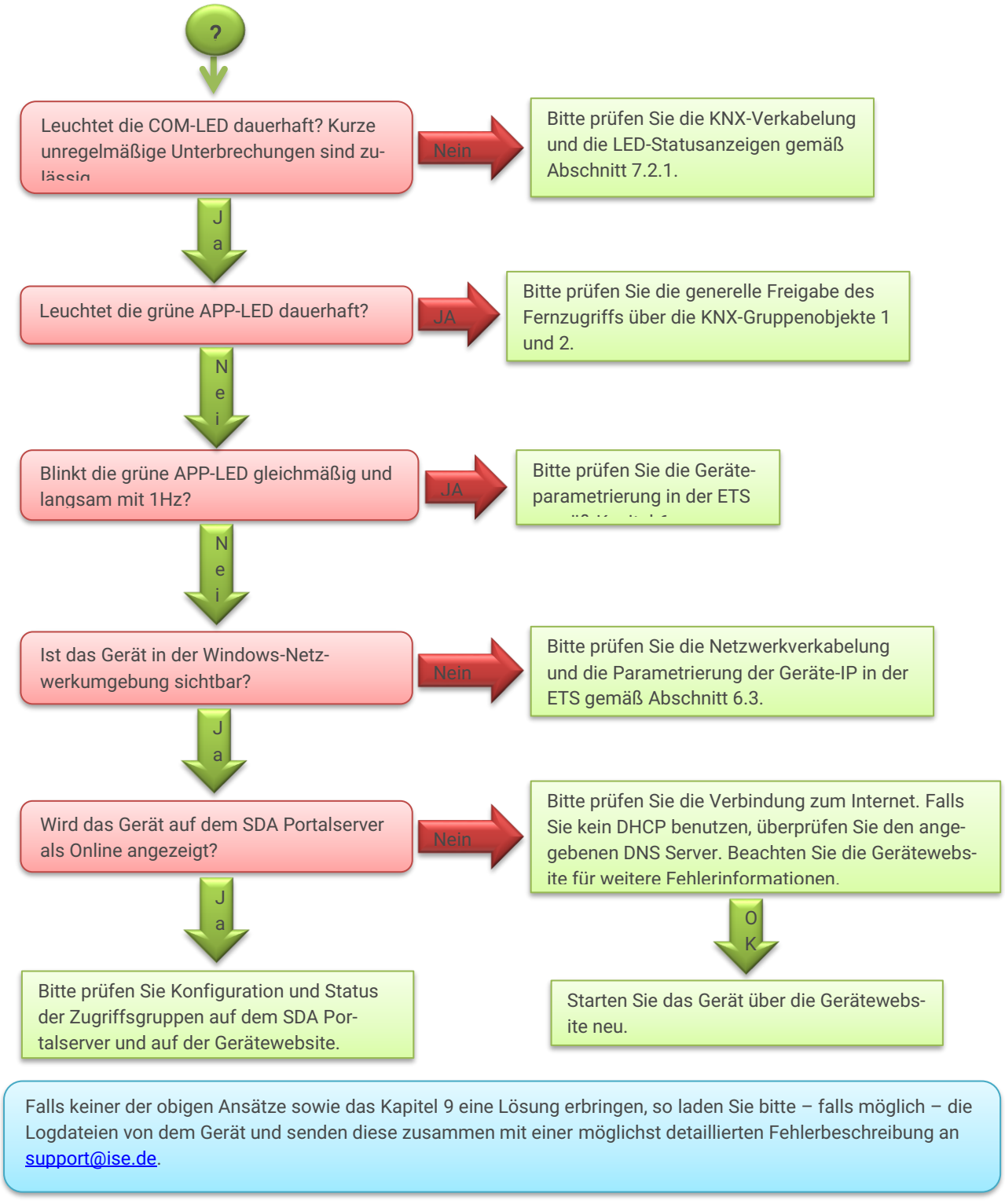
- Aufrufen der Webseite des Gerätes. Dazu in der Netzwerkumgebung auf das Icon des Gerätes im Bereich *Multimedia* doppelklicken.
- Auf der Webseite in der oberen Menüleiste *Device Status* auswählen.
- Auf der Status-Seite in der oberen Menüleiste *Download Logfile* auswählen.
- Die sich öffnende Seite startet den Download der Logfiles. Passiert dies nicht, so kann der angegebene Link verwendet werden.

10.2 Statusseite des ISE SMART CONNECT KNX REMOTE ACCESS

Auf der Webseite des ISE SMART CONNECT KNX REMOTE ACCESS (siehe Abschnitt 7.7.2 „Über die Webseite des Gerätes“) können Sie den Gerätestatus aufrufen. Dieser zeigt unter anderem die installierte Softwareversion sowie die Konfiguration und den Verbindungsstatus zum SDA Portal Server des ISE SMART CONNECT KNX REMOTE ACCESS an. Im Falle eines Fehlers senden Sie uns bitte einen Screenshot der Statusseite zu.

10.3 Der ISE SMART CONNECT KNX REMOTE ACCESS funktioniert nicht

Der folgende Fehlerbaum soll versuchen, die häufigsten Probleme zu lösen. Falls dies nicht gelingt, kontaktieren Sie uns bitte über support@ise.de.



Falls keiner der obigen Ansätze sowie das Kapitel 9 eine Lösung erbringen, so laden Sie bitte – falls möglich – die Logdateien von dem Gerät und senden diese zusammen mit einer möglichst detaillierten Fehlerbeschreibung an support@ise.de.

11 Lizenzvertrag ISE SMART CONNECT KNX REMOTE ACCESS-Software

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 ISE SMART CONNECT KNX REMOTE ACCESS-Software oder der Ingebrauchnahme des ISE SMART CONNECT KNX REMOTE ACCESS schließen Sie einen Vertrag mit der Firma ise Individuelle Software und Elektronik GmbH, und erklären sich an die Bestimmungen dieses Vertrages gebunden.

11.1 Definitionen

Lizenzgeber: ise Individuelle Software und Elektronik GmbH, Oldenburg, Osterstraße 15, Deutschland

Lizenznehmer: Der rechtmäßige Empfänger der ISE SMART CONNECT KNX REMOTE ACCESS-Software

Firmware: Software, die auf der ISE SMART CONNECT KNX REMOTE ACCESS-Hardware eingebettet ist und zum Betrieb des ISE SMART CONNECT KNX REMOTE ACCESS dient.

ISE SMART CONNECT KNX REMOTE ACCESS Software: Als ISE SMART CONNECT KNX REMOTE ACCESS-Software wird die gesamte Software inklusive der Betriebsdaten bezeichnet, die für das Produkt ISE SMART CONNECT KNX REMOTE ACCESS zur Verfügung gestellt wird. Dies sind insbesondere die Firmware und die Produktdatenbank. Außerdem enthalten sind die SDA Client Software sowie das SDA Portal.

11.2 Vertragsgegenstand

Gegenstand dieses Vertrages ist die auf Datenträger oder durch Download bereitgestellt ISE SMART CONNECT KNX REMOTE ACCESS-Software, der SDA Client Software sowie die zugehörige Dokumentation in schriftlicher oder elektronischer Form, sowie die zur Verfügungstellung des SDA Portals.

11.3 Rechte zur Nutzung der ISE SMART CONNECT KNX REMOTE ACCESS-Software

11.3.1 Firmware und SDA Client

Der Lizenzgeber räumt dem Lizenznehmer das nichtausschließliche, zeitlich unbegrenzte und nicht übertragbare Recht ein, die ISE SMART CONNECT KNX REMOTE ACCESS-Software gemäß den nachstehenden Bedingungen 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.

11.3.2 Secure Device Access Portal

Der Lizenzgeber stellt dem Lizenznehmer für die Nutzung mit der Firmware und dem SDA Client einen Secure Device Access Portalserver unter https://securedeviceaccess.net zur Verfügung. Hierzu nutzt er derzeit die Dienstleistung der ise Individuelle Software und Elektronik GmbH. Der Lizenzgeber kann aus wichtigem Grund den Betrieb des SDA Portalservers mit einer Frist von 5 Jahren kündigen. Der Lizenzgeber muss in diesem Fall auf Anfrage des Lizenznehmers die SDA Portalsoftware dem

Lizenznehmer im Quellcode zugänglich machen, um ihm ein eigenes Hosting der Serversoftware und damit eine fortlaufende Nutzung von SDA zu ermöglichen.

11.4 Beschränkung der Nutzungsrechte

11.4.1 Maximal zulässiges Übertragungsvolumen

Die Lizenz schließt die Nutzung des Fernzugriffs im Dauerbetrieb aus, z.B. für Visualisierung oder Standortvernetzung. Wir betrachten wiederholte ununterbrochene Nutzung von mehr als 12h am Stück als Dauernutzung.

Das Übertragungsvolumen ist pro Monat und SDA Connector auf maximal 2 GB beschränkt.

Wir behalten uns vor, die o.g. Nutzungsgrenzen durch technische Maßnahmen durchzusetzen.

11.4.2 Kopieren, Bearbeiten oder Übertragen

Der Lizenznehmer ist nicht berechtigt die ISE SMART CONNECT KNX REMOTE ACCESS-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.

11.4.3 Reverse-Engineering oder Umwandelungstechniken

Der Lizenznehmer ist nicht berechtigt Reverse-Engineering Techniken auf die ISE SMART CONNECT KNX REMOTE ACCESS-Software anzuwenden oder die ISE SMART CONNECT KNX REMOTE ACCESS-Software in eine andere Form umzuwandeln. Zu solchen Techniken gehört 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).

11.4.4 Die Firmware und Hardware

Die Firmware darf nur auf der vom Lizenzgeber freigegebenen Hardware (ISE SMART CONNECT KNX REMOTE ACCESS) installiert und genutzt werden.

11.4.5 Weitergabe an Dritte

Die ISE SMART CONNECT KNX REMOTE ACCESS-Software darf nicht an Dritte weitergegeben werden oder Dritten zugänglich gemacht werden.

11.4.6 Vermieten, Verleasen oder Unterlizenzen

Der Lizenznehmer ist nicht berechtigt, die ISE SMART CONNECT KNX REMOTE ACCESS-Software zu vermieten, zu verleasen oder Unterlizenzen an dem Programm zu erteilen.

11.4.7 Software-Erstellung

Der Lizenznehmer benötigt eine schriftliche Genehmigung des Lizenzgebers, um Software zu erstellen und zu vertreiben, die von der ISE SMART CONNECT KNX REMOTE ACCESS-Software abgeleitet ist.

11.4.8 Die Mechanismen des Lizenzmanagements und des Kopierschutzes

Die Mechanismen des Lizenzmanagements und des Kopierschutzes der ISE SMART CONNECT KNX REMOTE ACCESS-Software dürfen nicht analysiert, nicht publiziert, nicht umgangen und nicht außer Funktion gesetzt werden.

11.5 Eigentum, Geheimhaltung

11.5.1 Dokumentation

Die ISE SMART CONNECT KNX REMOTE ACCESS-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) sind Geschäftsgeheimnisse des Lizenzgebers und/oder Gegenstand von Copyright und/oder anderen Rechten und gehören auch weiterhin dem Lizenzgeber. Der Lizenznehmer wird diese Rechte beachten.

11.5.2 Weitergabe an Dritte

Weder die Software, noch die Datensicherungskopie, noch die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) dürfen zu irgendeinem Zeitpunkt - ganz oder in Teilen, entgeltlich oder unentgeltlich - an Dritte weitergegeben werden.

11.6 Änderungen, Nachlieferungen

Die ISE SMART CONNECT KNX REMOTE ACCESS-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) unterliegen eventuell Änderungen durch den Lizenzgeber.

11.7 Gewährleistung

Die ISE SMART CONNECT KNX REMOTE ACCESS-Software wird zusammen mit der Software von Dritten ausgeliefert, die im Kapitel 12 – *Open Source Software* aufgelistet ist. Für die Software Dritter wird keinerlei Gewährleistung übernommen.

11.7.1 Software und Dokumentation

Die ISE SMART CONNECT KNX REMOTE ACCESS-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 ISE SMART CONNECT KNX REMOTE ACCESS-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 ihrer beigefügten Dokumentation in der jeweils gültigen Fassung.
- Die Software ist auf den vom Lizenzgeber genannten Computer-Stationen ablauffähig.

Die Erfüllung der Gewährleistung erfolgt durch Ersatzlieferung.

11.7.2 Gewährleistungsbeschränkung

Im Übrigen wird für die Fehlerfreiheit der ISE SMART CONNECT KNX REMOTE ACCESS-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 ausgeschlossen.

11.8 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 ISE SMART CONNECT KNX REMOTE ACCESS-Software entstehen, selbst wenn der Lizenzgeber von der Möglichkeit eines solchen Schadens Kenntnis hat.

Diese Haftungsbeschränkung gilt für alle Schadensersatzansprüche des Lizenznehmers, gleich aus welchem Rechtsgrund. Auf jeden Fall ist die Haftung auf den Kaufpreis des Produkts beschränkt.

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

11.9 Anwendbares Recht

Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.

Gerichtsstand ist Oldenburg.

11.10 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 ISE SMART CONNECT KNX REMOTE ACCESS-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 ISE SMART CONNECT KNX REMOTE ACCESS-Software. Das Produkt ISE SMART CONNECT KNX REMOTE ACCESS muss in diesem Fall außer Betrieb genommen werden. Eine weitere Nutzung des ISE SMART CONNECT KNX REMOTE ACCESS ohne Lizenz ist ausgeschlossen.

Die Inbetriebnahme-Software und die Visualisierungs-Software muss deinstalliert und alle Kopien vernichtet oder an den Lizenzgeber zurückgegeben werden.

11.11 Nebenabreden und Vertragsänderungen

Nebenabreden und Vertragsänderungen bedürfen zu ihrer Gültigkeit der Schriftform.

11.12 Ausnahme

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

12 Open Source Software

Dieses Produkt verwendet Software aus dritten Quellen, die im Rahmen von unterschiedlichen Open Source Lizenzen veröffentlicht sind.

Die einzelnen verwendeten Software-Pakete, sowie deren Lizenzen, werden auf der Gerätewebseite dieses Produktes unter System / Lizenzen aufgeführt und beschrieben.

Der Quellcode für die in diesem Produkt verwendete Open Source-Software kann über die E-Mail-Ad-resse support@ise.de bezogen werden.

Dieses Angebot ist für 3 Jahre nach Auslauf des Service für dieses Produkt gültig.