

Stand der Dokumentation:
14.07.2015
Druck: 23.07.2015

Produkthandbuch

ise smart connect KNX Secure

Best.-Nr. 1-0003-004

Gültig für Applikations-Software v2.1, Firmwareversion v2.2 und SDA Client v1.1



Inhaltsverzeichnis

1	<u>Produktbeschreibung</u>	<u>5</u>
1.1	Funktionen	5
1.2	Wie funktioniert Secure Device Access?	6
1.2.1	ise smart connect KNX Secure, allgemein "SDA Connector"	6
1.2.2	Quick Connect.....	7
1.2.3	SDA-Portalserver	7
1.2.4	HTTPS-Proxy httpaccess.net	7
1.2.5	Kommunikation – sicher, zuverlässig und einfach zu handhaben	7
1.2.6	Clientsoftware (SDA Client)	8
1.3	Definitionen und Begriffsklärungen.....	8
2	<u>Anwendungsszenarien</u>	<u>11</u>
2.1	Wichtige allgemeine Informationen.....	11
2.1.1	Quick Connect vs. SDA Portal.....	11
2.1.2	Einschränkungen und Freigaben von Zugriffsrechten über KNX Kommunikationsobjekte.....	11
2.2	Zugriff auf Webseiten im entfernten Netzwerk.....	11
2.3	Zugriff auf KNX Installationen.....	12
2.4	Konfiguration des Gira HomeServer	13
2.5	Zugriff über andere TCP Protokolle	13
2.6	Benutzerrechte und Zugriffsgruppen	14
3	<u>Nutzung des SDA-Portalservers</u>	<u>16</u>
3.1	Startseite.....	16
3.2	HTTP Zugriff über Quick Connect	16
3.3	Benutzerregistrierung	17
3.4	SDA Connector Verwaltung.....	18
3.5	HTTP Zugriff über Portal Connect	19
3.6	Erweiterte Informationen zu einem SDA Connector.....	19
3.7	Eigenschaften eines SDA Connectors anzeigen und ändern.....	19
3.8	Zugriffsrechte für Benutzer verwalten	20
3.8.1	Die Rolle eines Benutzers an einem SDA Connector	21
3.8.2	Die Zugriffsgruppen eines Benutzers an einem SDA Connector.....	21
3.9	Eigentümer und Übertragung der Eigentümerschaft.....	22
4	<u>Nutzung des SDA Clients</u>	<u>23</u>
4.1	Allgemeine Einstellungen	23
4.2	Über den SDA Client mit einem SDA Connector verbinden.....	24
4.2.1	Verbindung via Quick Connect herstellen	24
4.2.2	Verbindung via Portal Connect herstellen.....	24
4.3	Konfiguration der Zugriffsoptionen eines SDA Connectors	25
4.3.1	Zugriff auf eine KNX Installation über KNX-IP.....	25
4.3.2	Softwareaktualisierung von ise smart connect Geräten	27
4.3.3	Fernkonfiguration Gira HomeServer und Nutzung von Eiblib/IP	27
4.3.4	Nutzung weitere TCP Protokolle über SDA	28
4.4	Starten der SDA Verbindung und Statusanzeige.....	29
4.5	Messung der Kommunikationsgeschwindigkeit	30
4.6	Beenden einer SDA Verbindung.....	30

5	<u>Montage, elektrischer Anschluss und Bedienung</u>	<u>31</u>
5.1	Geräteaufbau	31
5.2	Sicherheitshinweise.....	32
5.3	Montage und elektrischer Anschluss	32
6	<u>Projektierung in der ETS.....</u>	<u>34</u>
6.1	Projektierung Schritt 1 – ise smart connect KNX Secure als Gerät in der ETS anlegen.....	35
6.2	Projektierung Schritt 2 – Physikalische Adressen zuordnen	35
6.3	Projektierung Schritt 3 – IP-Adresse, Subnetzmaske und Adresse des Standardgateways einstellen.....	36
6.4	Allgemeine Parameter einstellen.	38
6.4.1	Parameter-Seite <i>Allgemein</i>	38
6.5	Gruppenadressen an Gruppenobjekte anbinden.	39
7	<u>Inbetriebnahme</u>	<u>43</u>
7.1	Bedienung.....	43
7.2	LED-Statusanzeigen	44
7.2.1	LED-Statusanzeige beim Gerätestart	44
7.2.2	LED-Statusanzeige im Betrieb.....	45
7.3	Übertragung beschleunigen: Übertragungsweg <i>KNX-TP</i> oder <i>IP</i> wählen	46
7.4	Physikalische Adresse des Geräts programmieren	46
7.5	Applikationsprogramme und Projektierungsdaten übertragen	47
7.6	Werksreset.....	47
7.6.1	Über die Programmier Taste am Gerät	47
7.6.2	Über die Webseite des Gerätes.....	47
7.7	Information Anzeigen über die Webseite	48
8	<u>Technische Daten.....</u>	<u>49</u>
9	<u>Häufig gestellte Fragen (FAQ)</u>	<u>50</u>
10	<u>Fehlersuche und Support</u>	<u>52</u>
10.1	Download Logfiles im Falle eines Problems	52
10.2	Statusseite des ise smart connect KNX Secure.....	52
10.3	Der ise smart connect KNX Secure funktioniert nicht	53
11	<u>Lizenzvertrag ise smart connect KNX Secure-Software.....</u>	<u>54</u>
11.1	Definitionen	54
11.2	Vertragsgegenstand	54
11.3	Rechte zur Nutzung der ise smart connect KNX Secure-Software	54
11.3.1	Firmware und SDA Client	54
11.3.2	Secure Device Access Portal	54
11.4	Beschränkung der Nutzungsrechte	54
11.4.1	Maximal zulässiges Übertragungsvolumen.....	54
11.4.2	Kopieren, Bearbeiten oder Übertragen	55
11.4.3	Reverse-Engineering oder Umwandlungstechniken	55
11.4.4	Die Firmware und Hardware	55
11.4.5	Weitergabe an Dritte.....	55
11.4.6	Vermieten, Verleasen oder Unterlizenzen	55
11.4.7	Software-Erstellung	55
11.4.8	Die Mechanismen des Lizenzmanagements und des Kopierschutzes	55

11.5	Eigentum, Geheimhaltung	55
11.5.1	Dokumentation	55
11.5.2	Weitergabe an Dritte.....	55
11.6	Änderungen, Nachlieferungen.....	55
11.7	Gewährleistung	56
11.7.1	Software und Dokumentation	56
11.7.2	Gewährleistungsbeschränkung.....	56
11.8	Haftung	56
11.9	Anwendbares Recht.....	56
11.10	Beendigung	56
11.11	Nebenabreden und Vertragsänderungen	56
11.12	Ausnahme.....	57
<u>12</u>	<u>Open Source Software</u>	<u>58</u>
<u>13</u>	<u>GNU GENERAL PUBLIC LICENSE</u>	<u>60</u>
<u>14</u>	<u>OpenSSL Lizenzen</u>	<u>65</u>
14.1	OpenSSL License	65
14.2	Original SSLeay License	66

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 zu Hause 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
- KNX/TP Anschluss mit integriertem IP Interface (Tunnelling 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 Secure 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 Secure oder anderen KNXnet/IP Geräten über direkte KNX-IP Verbindung.
- Die Konfiguration des ise smart connect KNX Secure erfolgt über 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 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.

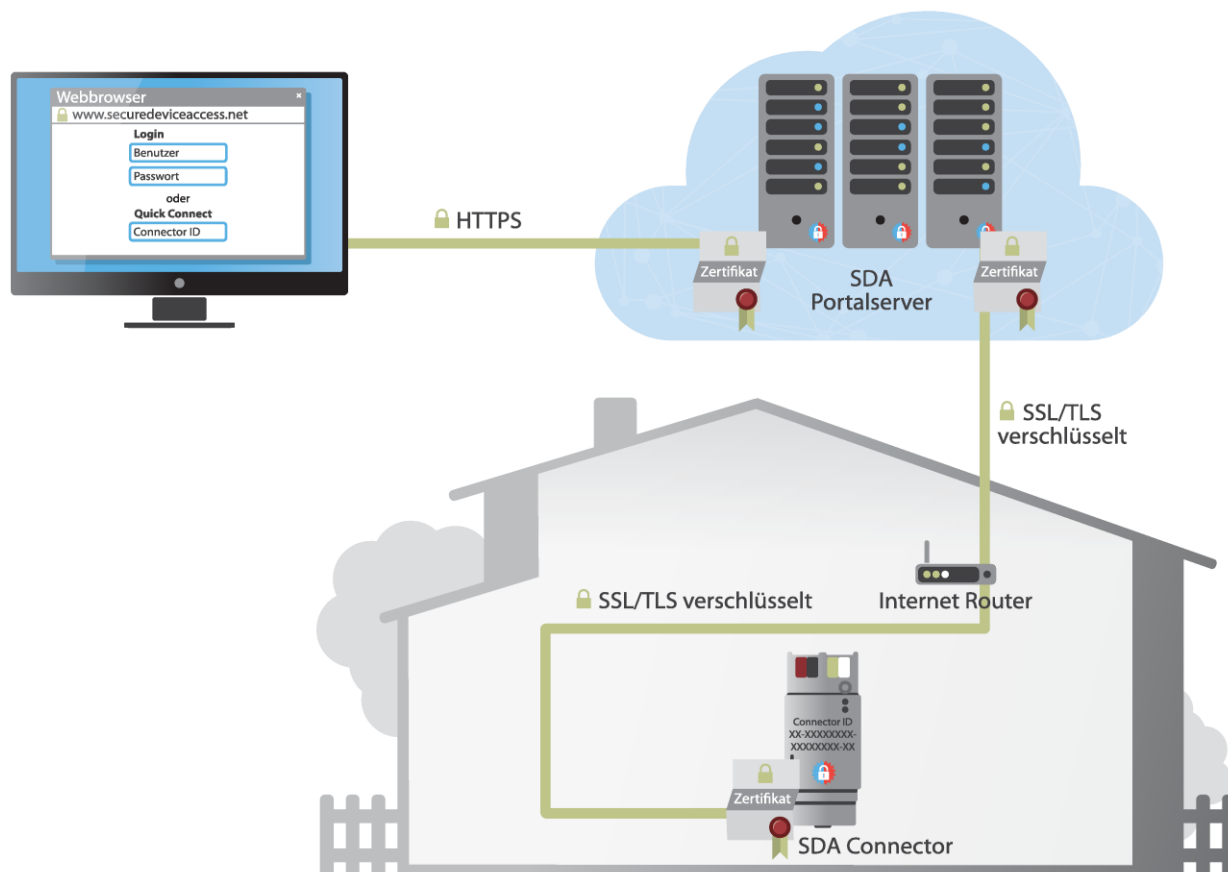


Abbildung 1 – Übersicht über den sicheren Zugriff mit „Secure Device Access“

1.2.1 ise smart connect KNX Secure, allgemein „SDA Connector“

Der ise smart connect KNX Secure (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 1.2.4).

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 1.2.6).

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

1.2.2 Quick Connect

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

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

Die Connector ID hat einen zufälligen Anteil und kann daher nicht geraten werden. Jeder, der die Connector 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.

1.2.3 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.

1.2.4 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 SDA 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.

1.2.5 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-Tunnelling.

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.

1.2.6 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. 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.

1.3 Definitionen und Begriffsklärungen

- **Secure Device Access, SDA**
Bezeichnet das komplette System, welches den sicheren Zugriff über das Internet auf Ihr Zuhause bereitstellt. Siehe 1.2.
- **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 1.2.3.
- **SDA Connector, ise smart connect KNX secure**
Der SDA Connector ist ein kleines elektronisches Gerät, das an Ihr Heimnetzwerk angeschlossen wird und dieses mit dem Portalserver verbindet. Siehe 1.2.1.
- **Connector ID**
Jeder SDA Connector hat eine eindeutige ID, welche auf dem Gerät aufgedruckt ist. Diese ID dient folgenden Zwecken:
 - Sicherer Zugriff ohne Portalanmeldung (Quick Connect)
 - Verknüpfung eines SDA Connectors mit einem Portalkonto
 Die Connector ID ist zufällig und kann nicht geraten werden.
- **Quick Connect**
Zugriff auf Geräte hinter einem SDA Connector ohne Portalanmeldung, nur durch Eingabe der Connector ID. Siehe 1.2.2. Der Quick Connect ist das Gegenstück zum Portal Connect
- **Portal Connect**
Zugriff auf Geräte hinter einem SDA Connector mit Portalanmeldung. Siehe 1.2.3. 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 Netzwerkanschluss oder KNX-Anschluss, auf das über SDA zugegriffen werden soll
- **httpaccess.net**
Teil des SDA-Portalserver 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 Datenvolumen, 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 Portalserver, 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“
- **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 (s. a. 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 Connector ID (s. auch 1.2.2), 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 Secure 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 Secure 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 (s. Abbildung) über eine verschlüsselte SSL/TLS Verbindung zum SDA-Portalserver transportiert und wiederum über eine HTTPS Verbindung zum Internet Browser.

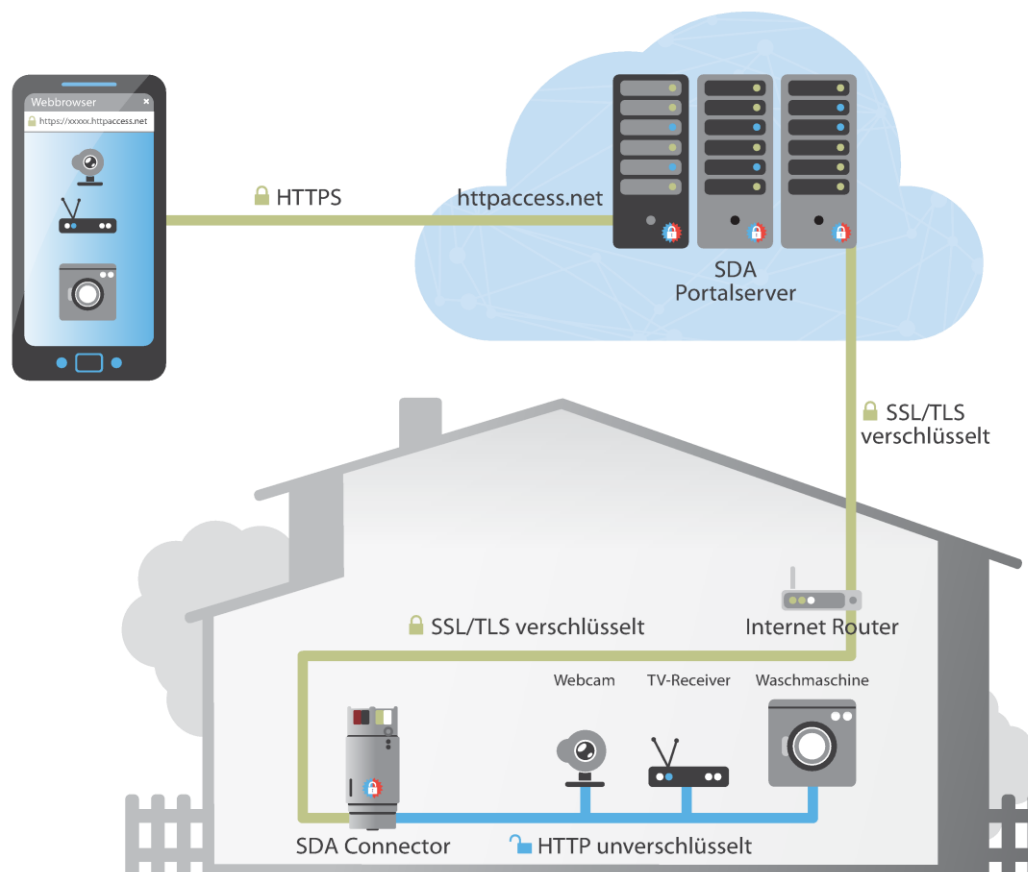


Abbildung 2 – Sicherer Zugriff auf Webseiten mit „Secure Device Access“

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 Kapiteln 3.2 - HTTP Zugriff über Quick Connect sowie 3.5 - HTTP Zugriff über Portal Connect.

2.3 Zugriff auf KNX Installationen

Der SDA Client ermöglicht 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.

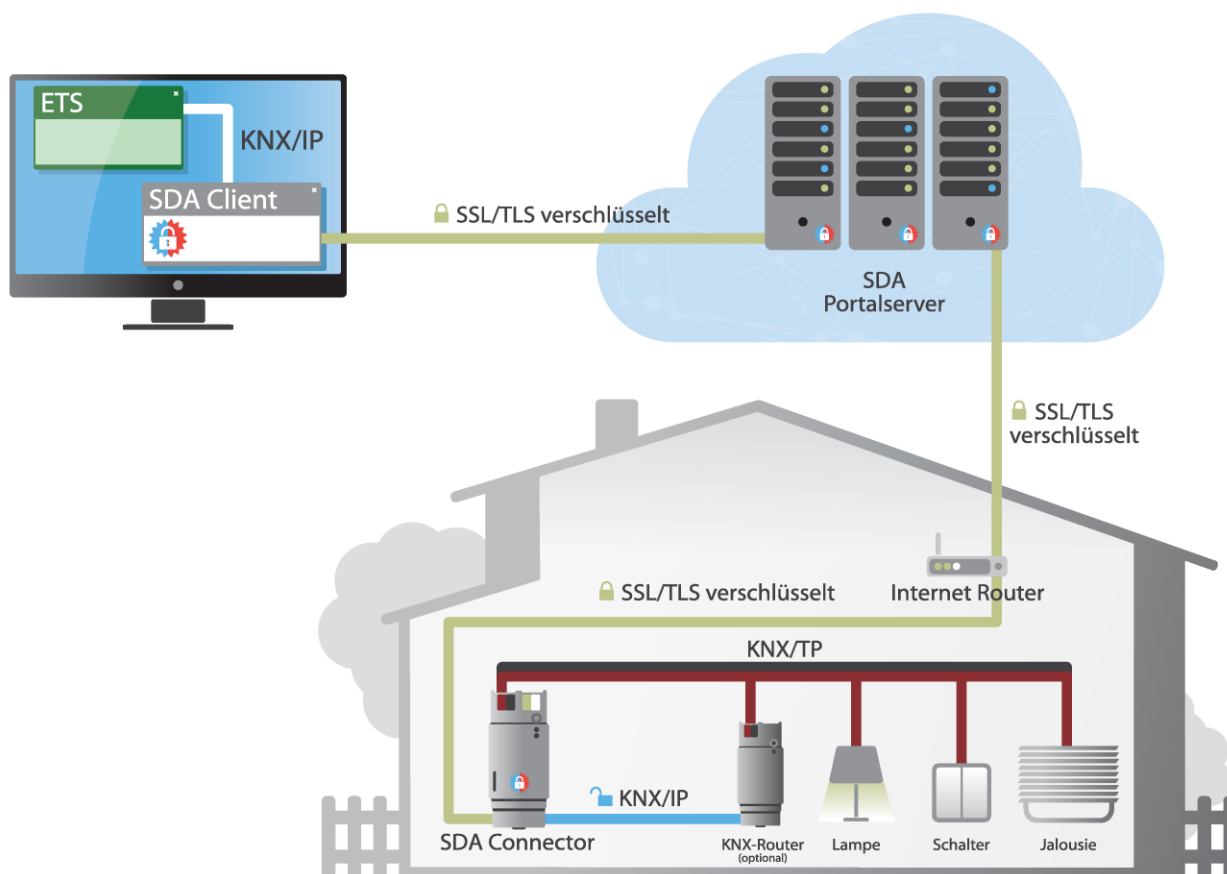


Abbildung 3 – Sicherer Zugriff auf die KNX Installation mit „Secure Device Access“

Nachdem mit dem SDA Client eine Verbindung zu einem bestimmten SDA Connector hergestellt wurde (s. Abschnitt 4.2), 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 (s. Abschnitt 7.3), der ETS bekannt gemacht, so dass auch diese beschleunigten Downloads über SDA funktionieren. Weitere Informationen finden Sie hierzu auch in Abschnitt 4.3.

2.4 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 wird die Konfiguration mit dem Experten unterstützt. Auch hierbei werden alle Daten beim Transport über das Internet verschlüsselt.

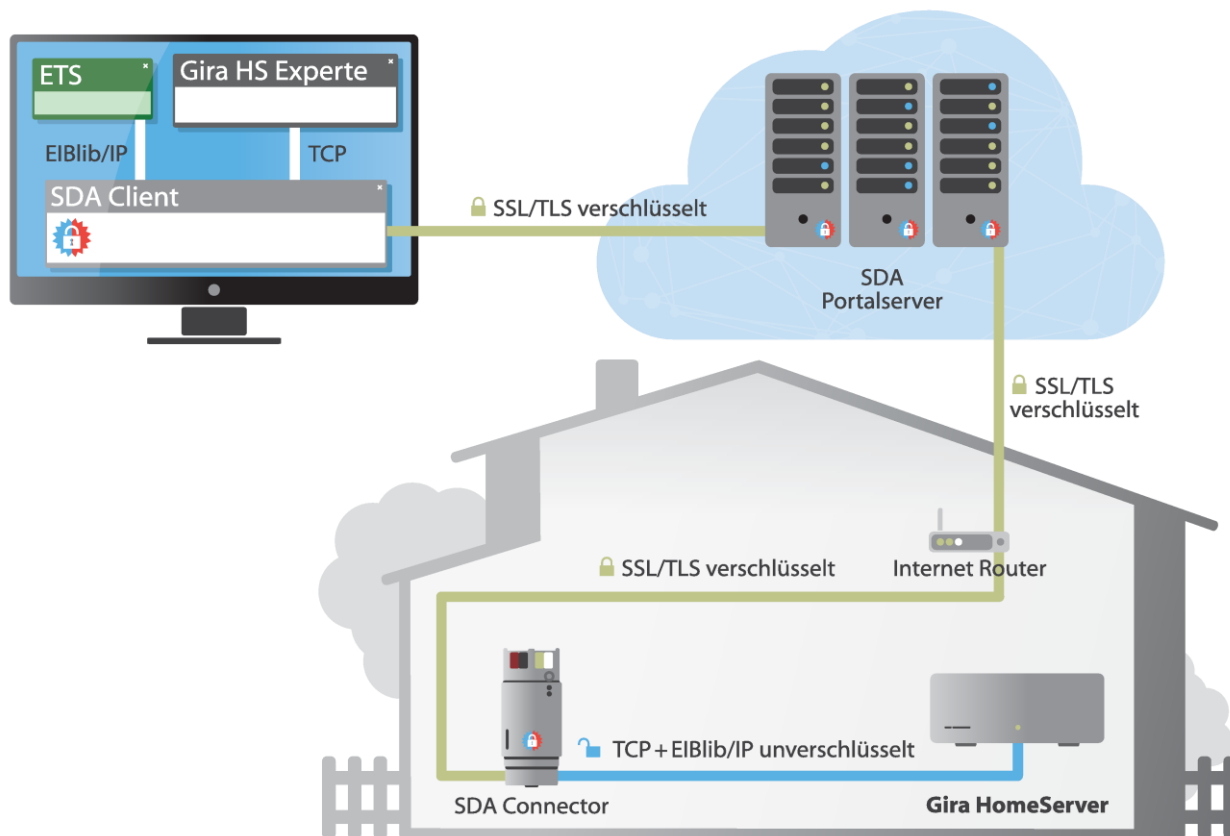


Abbildung 4 – Sichere Konfiguration des Gira HomeServer mit „Secure Device Access“

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 4.3.2.

2.5 Zugriff über andere TCP Protokolle

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

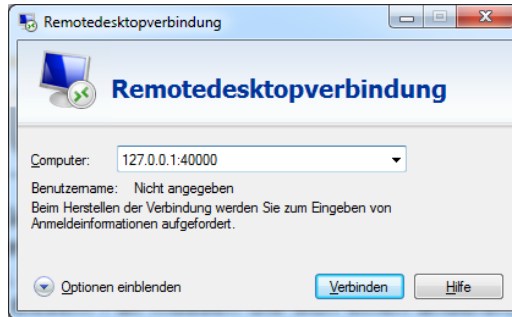
Weit verbreitet ist u.a. das Remote Desktop Protokoll (RDP), welches Microsoft für den Fernzugriff auf Windows Rechner definiert hat. Über eine einzelne TCP Verbindungskonfiguration wird der Zugriff möglich:

IP Adresse oder DNS Name im entfernten Netzwerk	TCP Port im entfernten Netzwerk	Lokaler TCP Port	Kommentar
computename	RDP (3389)	40000	

Als TCP Port sind Werte zwischen 1 und 65535 erlaubt, oder folgende vordefinierte Abkürzungen:
HTTP (80), HTTPS (443), SSH (22), Telnet (21), RDP (3389)

Beachten Sie hierbei: 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 „csd-i7“) herstellen wollen, müssen Sie den Port noch extra angeben, wenn er nicht dem Standard-Port entspricht. In unserem Beispiel kann die Verbindung wie folgt aufgebaut werden:



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

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

Weitere Informationen finden Sie im Abschnitt 4.3.4.

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.

2.6 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.

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 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 Connector ID

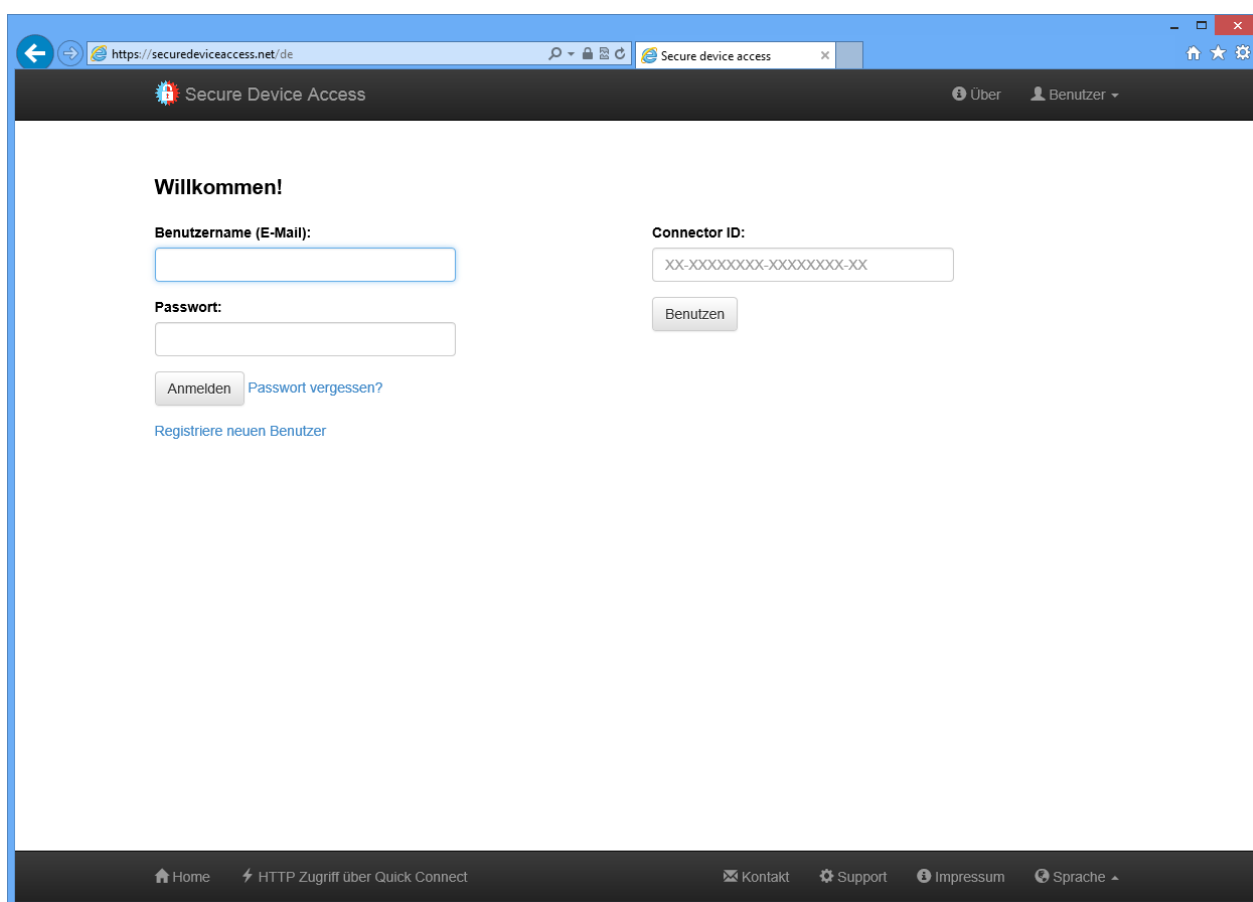


Abbildung 5 - SDA Portal – Startseite

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 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 uvm. werden dabei erfasst. Technisch wird hier das (Simple Service Discovery Protocol (kurz SSDP) benutzt.

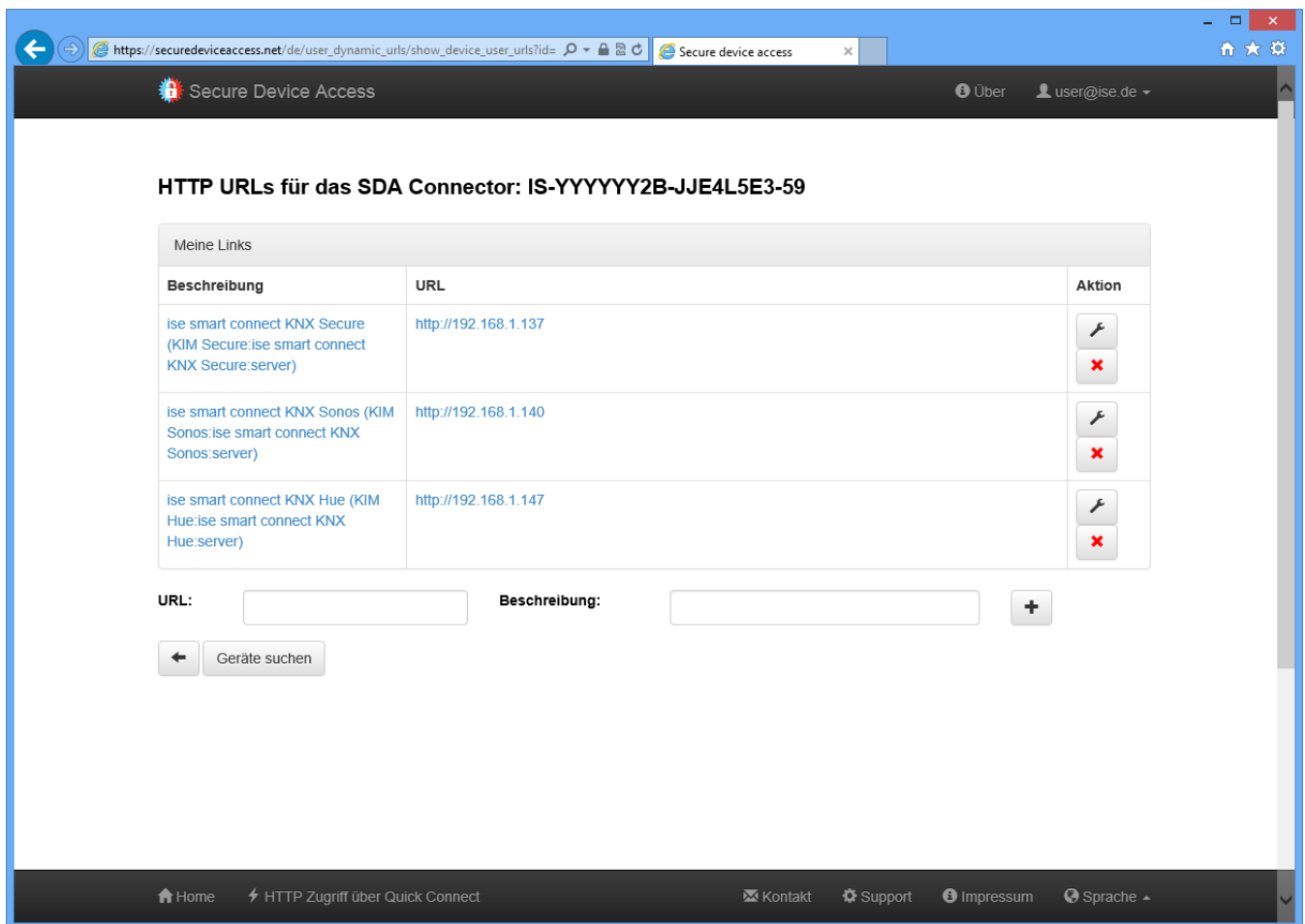


Abbildung 6 - Zugriff auf HTTP Webseiten über Quick Connect

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.

Wichtiger Hinweis: 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 (s. Kapitel 10) eine E-Mail mit der genauen Produktbeschreibung, Screenshots und einer kurzen Fehlerbeschreibung.

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 Secure auf Ihr Netzwerk zugreifen wollen, ist dies notwendig bzw. sehr hilfreich.

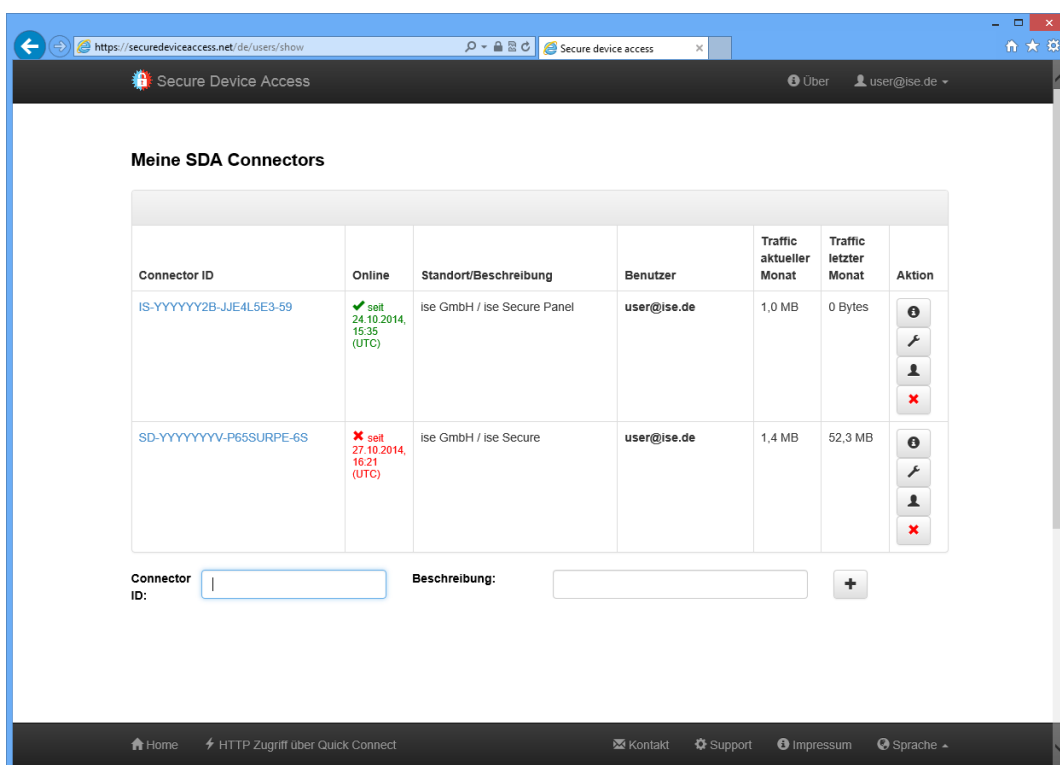
Die Registrierung erfolgt nach dem heute üblichen Standard zur Verifikation der E-Mail Adresse. Die Bestätigung eines Links in einer automatisch nach Start der Registrierung an die angegebene E-Mail Adresse gesendete Verifikationsmail ist zwingend erforderlich. Damit ist sichergestellt, dass eine Anmeldung 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 Bedienelemente unter der Liste Ihrer Geräte einen neuen SDA Connector über die Connector ID hinzu und werden damit der Eigentümer (wichtige Hinweise s. Abschnitt 3.9)
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 s. Abschnitt 3.9)



Connector ID	Online	Standort/Beschreibung	Benutzer	Traffic aktueller Monat	Traffic letzter Monat	Aktion
IS-YYYYY2B-JJE4L5E3-59	✓ seit 24.10.2014, 15:35 (UTC)	ise GmbH / ise Secure Panel	user@ise.de	1,0 MB	0 Bytes	
SD-YYYYYYYV-P65SURPE-6S	✗ seit 27.10.2014, 16:21 (UTC)	ise GmbH / ise Secure	user@ise.de	1,4 MB	52,3 MB	

Connector ID: Beschreibung:

Abbildung 7 – SDA Connectors des angemeldeten Benutzers

In der Liste der mit Ihrem Benutzer verbundenen SDA Connectors können Sie über die Spalte „Connector ID“ über den entsprechenden SDA Connector 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 dieses der Eigentümer (s. Abschnitt 3.9). 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 s. Kapitel 11.

Als Aktionen können (je nach Benutzerrechten) bis zu vier zur Verfügung stehen:

- Anzeigen von erweiterten Informationen zu einem SDA Connector (s. Abschnitt 3.6)
- Eigenschaften eines SDA Connectors anzeigen und ändern (s. Abschnitt 3.7)
- Zugriffsrechte für andere Benutzer verwalten (s. Abschnitt 3.8)
- Verbindung mit SDA Connector löschen (Hinweis: dies ist nicht möglich, so lange Sie der Eigentümer des SDA Connectors sind! S. auch Abschnitt 3.9)

3.5 HTTP Zugriff über Portal Connect

Der Zugriff auf entfernte Webseiten über SDA mit angemeldetem Benutzer (Portal Connect) entspricht von der Funktionsweise dem Zugriff über Quick Connect, s. Abschnitt 3.2.

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 IP Adresse des 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 Firmware Version genannt), die aktuell auf dem SDA Connector läuft

3.7 Eigenschaften eines SDA Connectors anzeigen und ändern

Die Seite ermöglicht zum einen das Ändern der für den angemeldeten Benutzer geltenden Beschreibung und Zugriffsgruppen. Zum anderen kann allgemein für den SDA Connector der Standort sowie der Quick Access Zugriff geändert werden, insofern der angemeldete Benutzer die Zugriffsrechte hierfür hat.

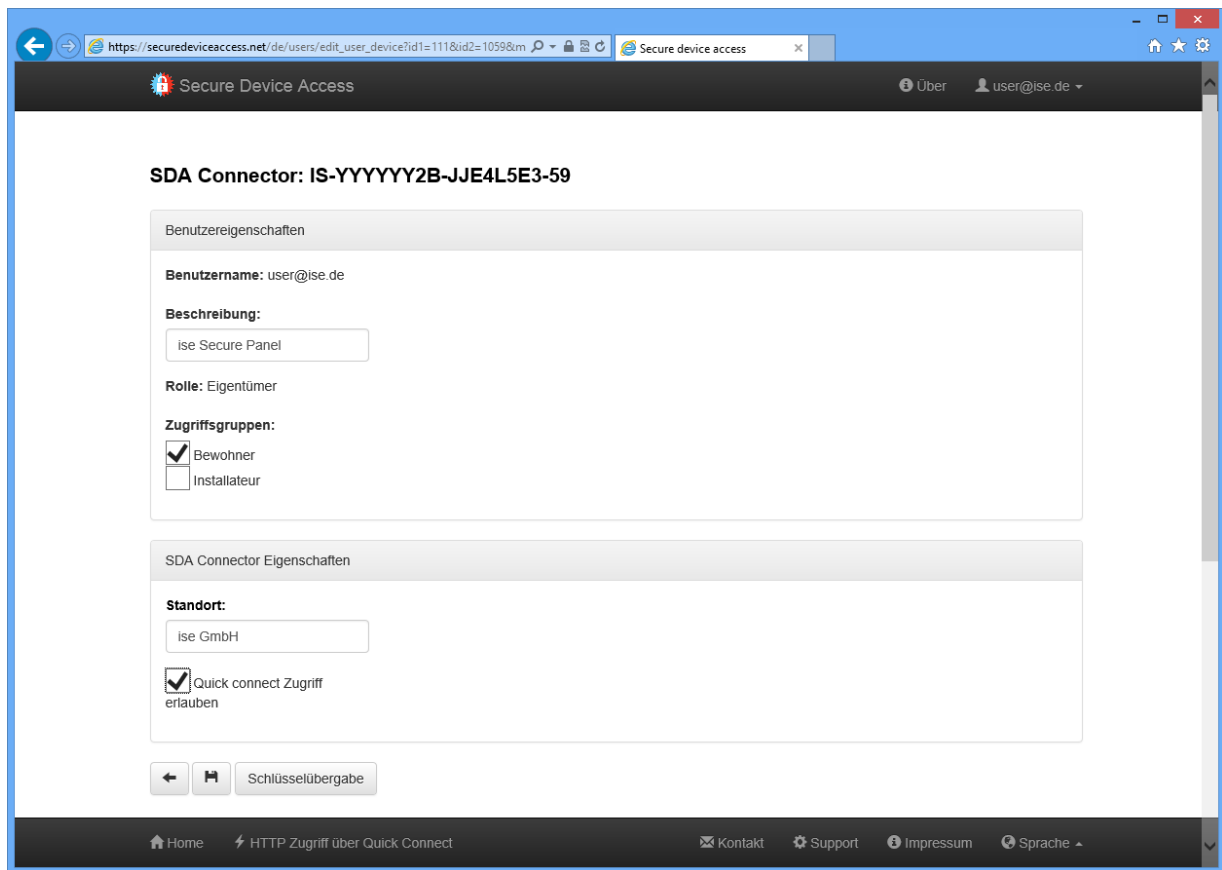


Abbildung 8 – Eigenschaften eines SDA Connectors anzeigen und ändern

3.8 Zugriffsrechte für Benutzer verwalten

Der Secure Device Access erlaubt die differenzierte Konfiguration von Zugriffsrechten auf Basis von Benutzern.

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

- Rolle: möglich sind hier „Eigentümer“, „Administrator“ und „Benutzer“, wobei der Eigentümer ein Administrator mit einer Sonderstellung ist (s. Abschnitt 3.9), 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.

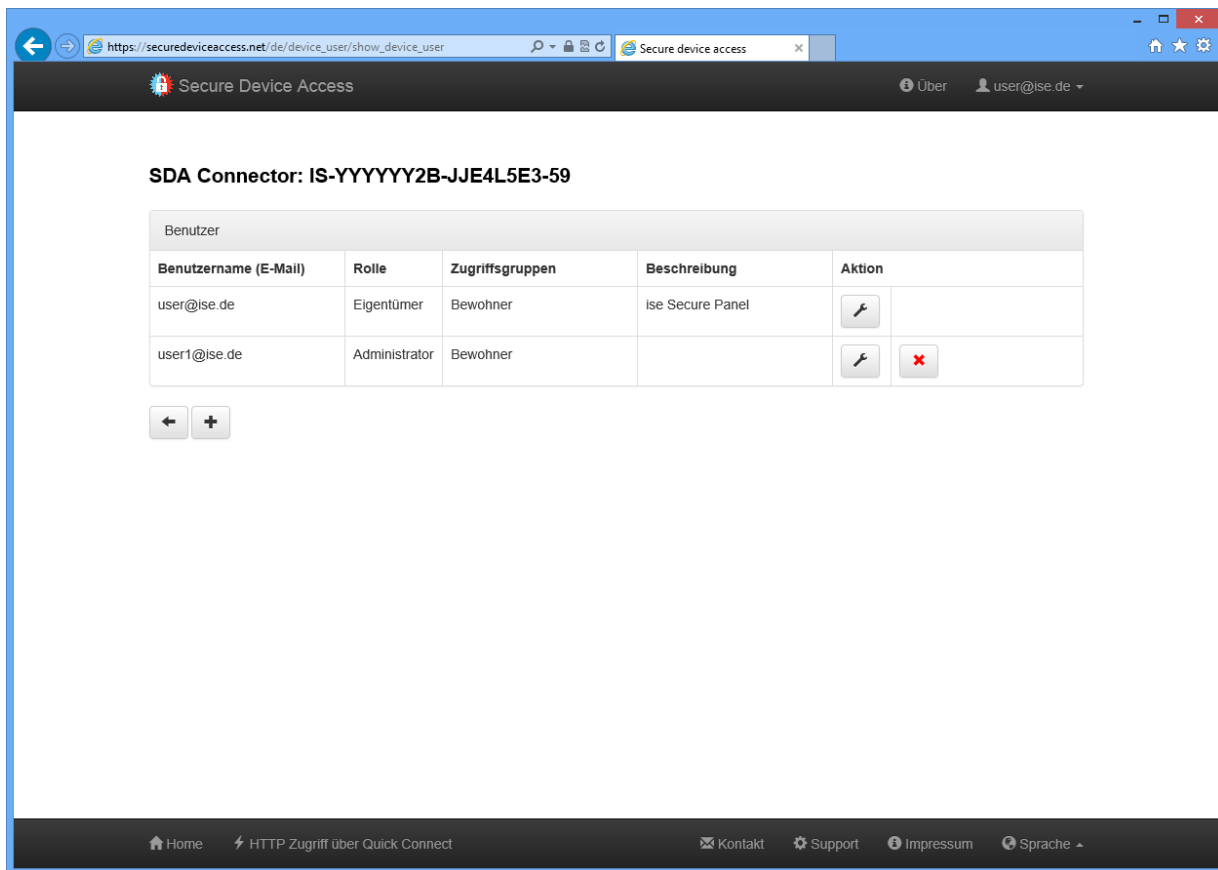


Abbildung 9 – Zugriffsrechte für andere Benutzer verwalten

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.

Wichtig: 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 (s. Abschnitt 3.8.2)!

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 den Abschnitt 6.

Wichtig: 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 (s. Abschnitt 3.8.1)!

3.9 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 (s. 3.7). 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 noch mal 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, Abschnitt 2.2.

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 Service/Downloads.

4.1 Allgemeine Einstellungen

Über die Schaltfläche für allgemeine Einstellungen oben rechts (s. Abbildung) können Sie das erweiterte Logging für die Fehlersuche bei Problemfällen aktivieren und können die Logfiles löschen sowie ein ZIP Archiv erzeugen, dass 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 und ob Sie standardmäßig für neue SDA Connector Konfigurationen (s. folgende Abschnitte) die Gira HomeServer Unterstützung aktiviert haben möchten. Dies ist dann sinnvoll, falls Sie in Ihren Projekten regelmäßig den Gira HomeServer nutzen.

Darüber hinaus können Sie das Verbindungs-Timeout für die Verbindung zum SDA Portal konfigurieren. Drei Sekunden sind ein guter Wert 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, ist dies durch Erhöhung des Timeouts problemlos möglich.

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. S. hierzu auch Abschnitt 4.3.1.

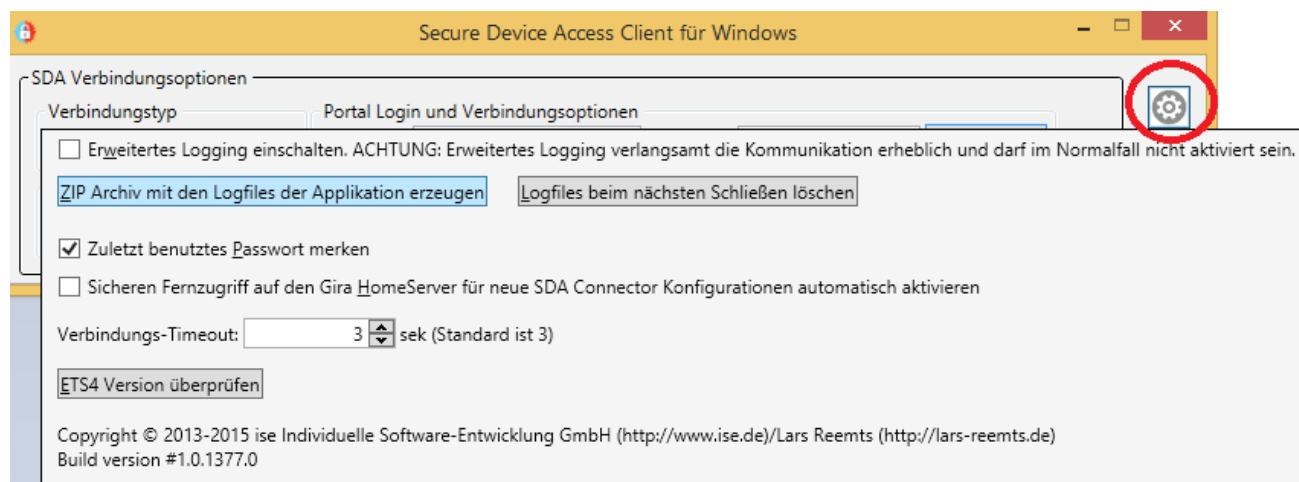


Abbildung 10 – Allgemeine Einstellungen im SDA Client

4.2 Über den SDA Client mit einem SDA Connector verbinden

Für den Verbindungsaufbau zu einem SDA Connector gibt es wie bereits beschrieben zwei Möglichkeiten, den Quick Connect und den Portal Connect.

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

4.2.1 Verbindung via Quick Connect herstellen

Wählen Sie „Quick Connect“ als Verbindungstyp (s. Abbildung). Danach geben Sie in das Feld daneben die Connector 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.

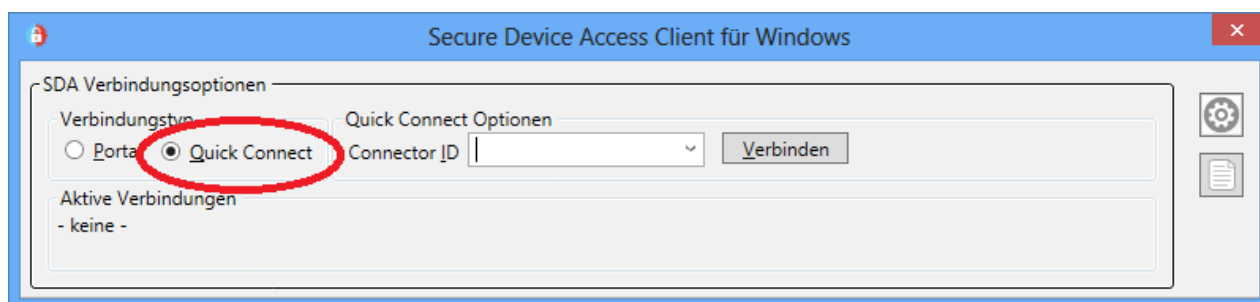


Abbildung 11 – SDA Connector über Quick Connect verbinden

Nach Eingabe einer gültigen SDA Connector 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 (s. Abschnitt 4.3 ff.), können Sie die Verbindung über die Schaltfläche „Verbinden“ aufbauen.

4.2.2 Verbindung via Portal Connect herstellen

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

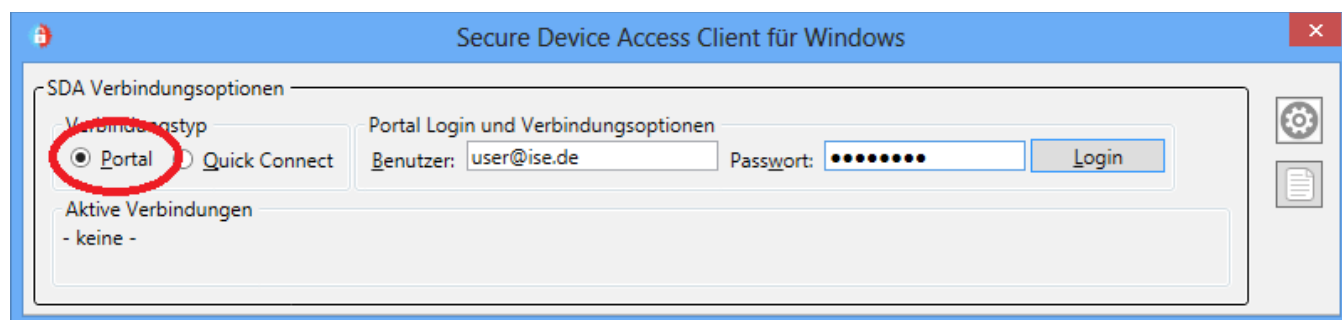


Abbildung 12 – Login beim SDA Portal Server

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.

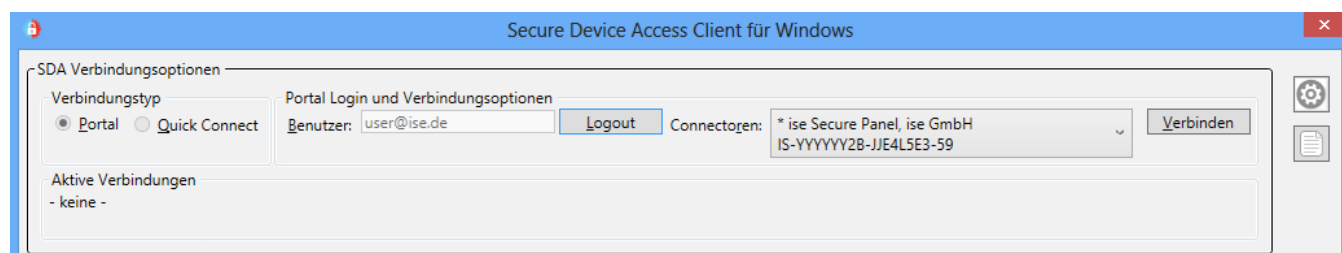


Abbildung 13 – SDA Connector über Portal Connect benutzen

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 (s. Abschnitt 4.3 ff.), können Sie die Verbindung über die Schaltfläche „Verbinden“ aufbauen.

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 Secure 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 HomeServer. Hier kann zum einen ein Projekt über den HomeServer Experten aktualisiert werden, zum anderen über das Eiblib/IP Protokoll eine Busverbindung hergestellt werden.

Darüber hinaus 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 (s. Abbildung) an- bzw. abschaltbar.

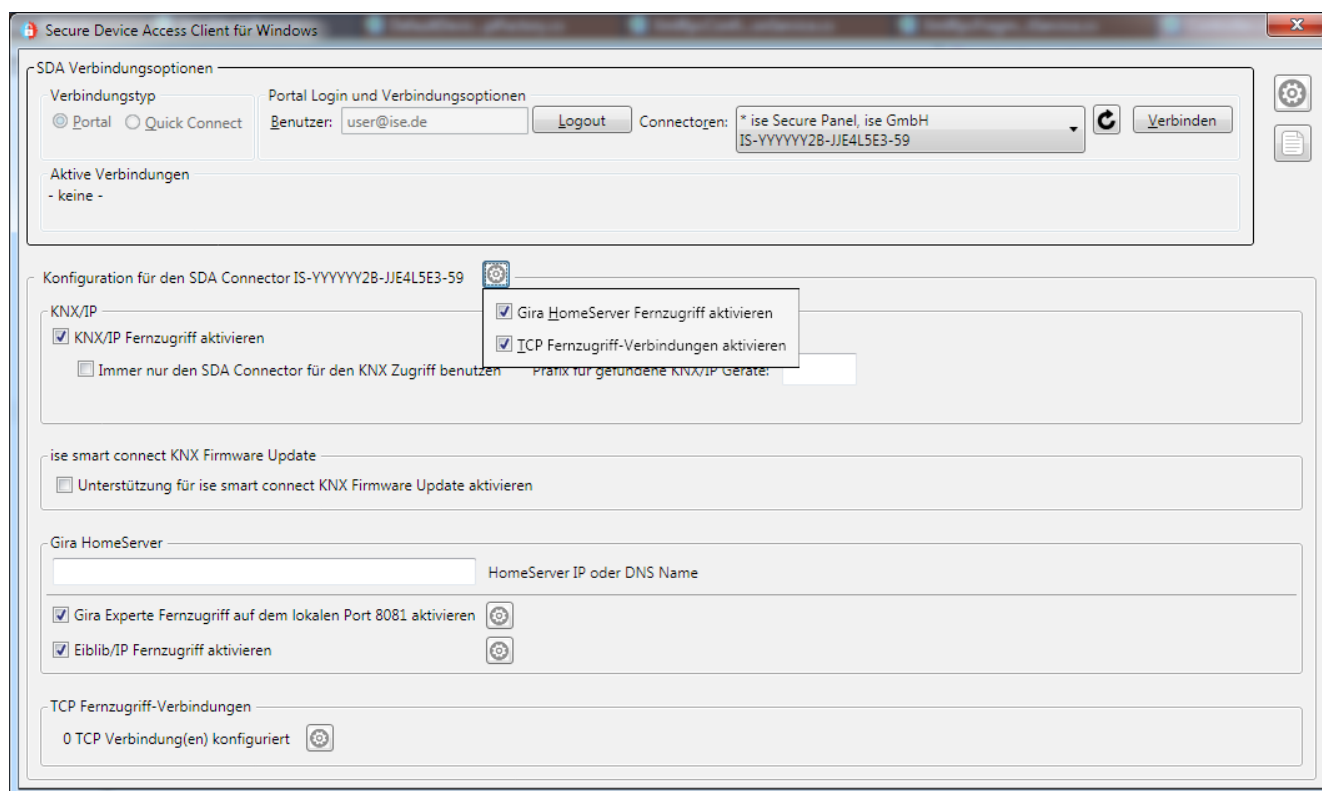


Abbildung 14 – SDA Connector Konfigurationsoptionen

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 (s. 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 Kapitels). 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 Secure über SDA zugänglich machen.

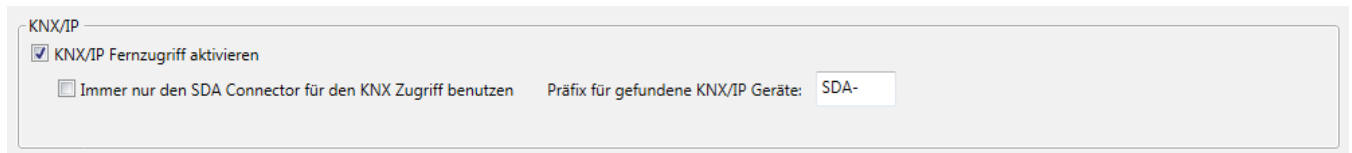


Abbildung 15 – KNX/IP Fernzugriffskonfiguration

Wichtiger Hinweis: Bei der Benutzung von **ETS4 Versionen älter als ETS4.2** können Probleme beim automatischen Erkennen der KNX/IP Interfaces in der ETS4 auftreten, so dass diese nicht erscheinen. In diesem 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, in dem Schaltflächen angeboten werden, um die entsprechenden Werte in die Zwischenablage zu kopieren. Beachten Sie hierzu die folgende Abbildung.

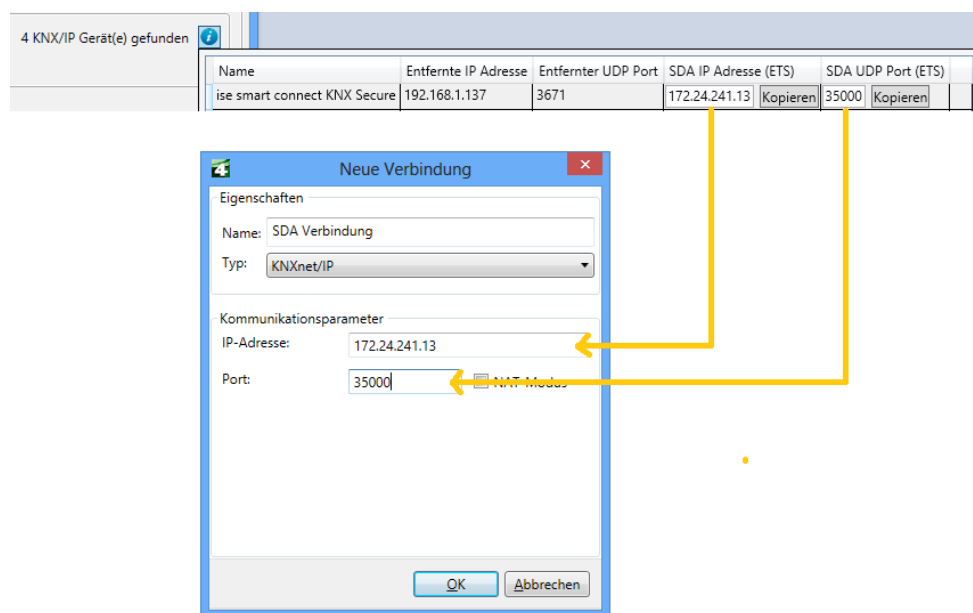


Abbildung 16 – Manuelle KNX/IP Interfacekonfiguration für ETS kleiner ETS4.2

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 hierbei 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.

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.

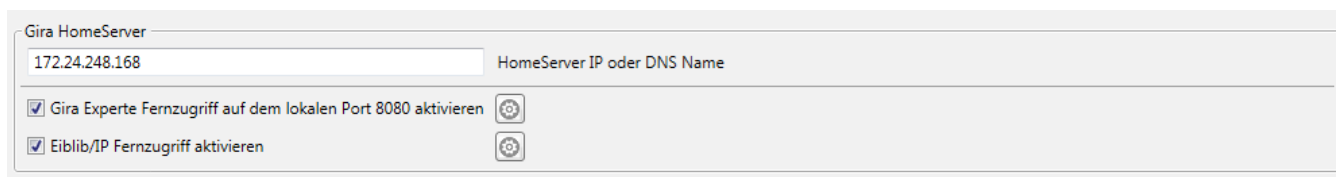


Abbildung 17 – Gira HomeServer Fernzugriffskonfiguration

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).

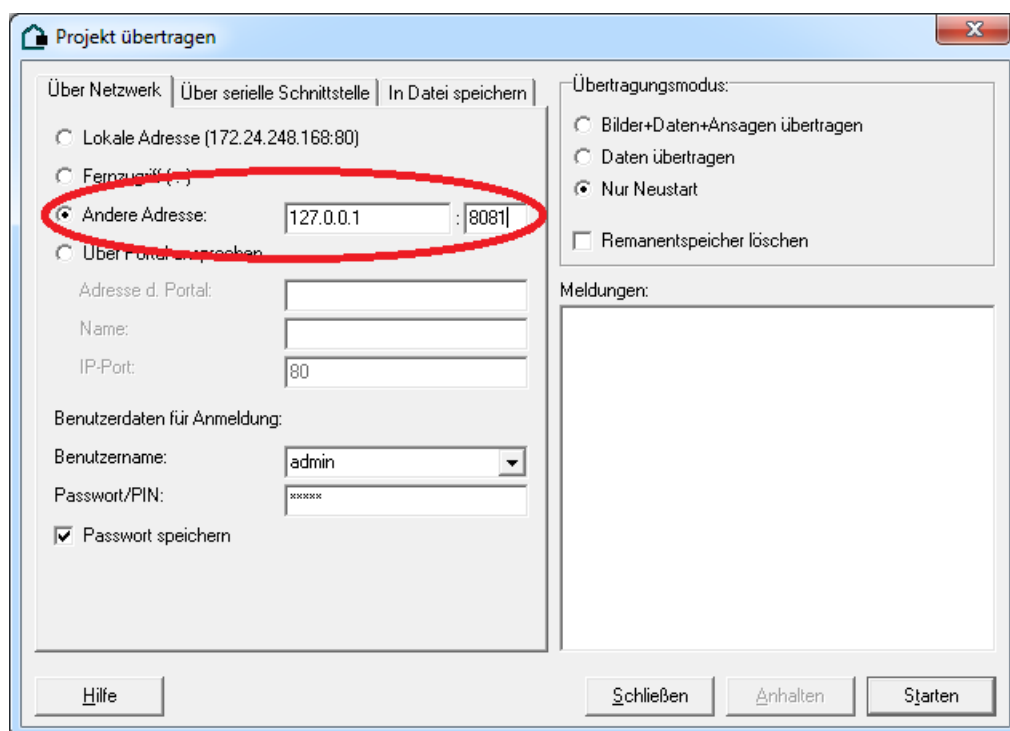


Abbildung 18 – Projekt mit Experte über SDA übertragen

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.

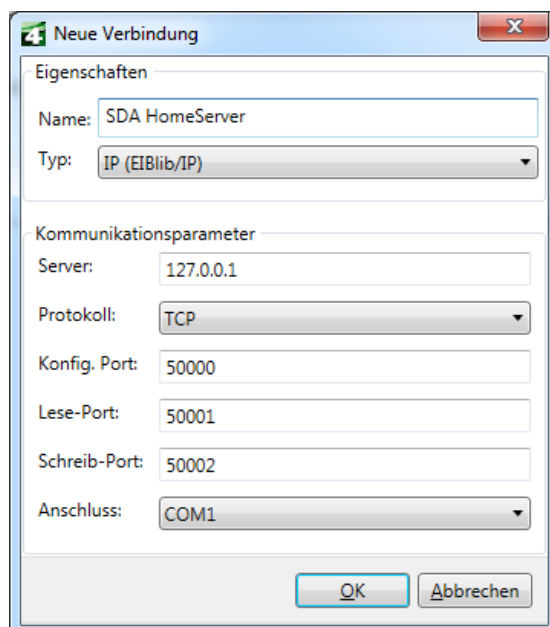


Abbildung 19 – HomeServer mit Eiblib/IP über SDA für KNX Anbindung nutzen

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.

Hinzufügen Löschen			
IP Adresse oder DNS Name im entfernten Netzwerk	TCP Port im entfernten Netzwerk	Lokaler TCP Port	Kommentar
computername	RDP (3389)	40000	Fernzugriff Windows Rechner

Als TCP Port sind Werte zwischen 1 und 65535 erlaubt, oder folgende vordefinierte Abkürzungen:
HTTP (80), HTTPS (443), SSH (22), Telnet (21), RDP (3389)

Abbildung 20 – TCP Fernzugriffskonfiguration

Bitte lesen Sie hierzu auch Abschnitt 2.5.

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.

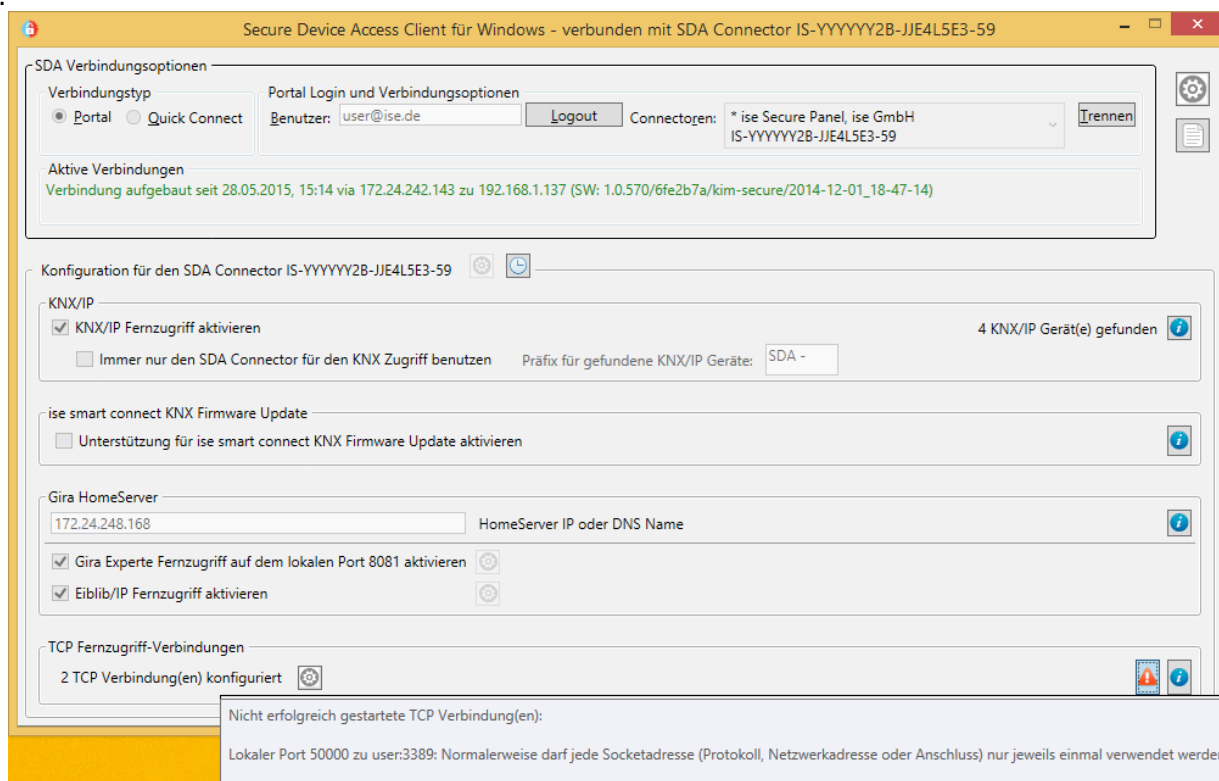


Abbildung 21 – Statusinformationen im SDA Client nach Verbindungsaufbau

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.

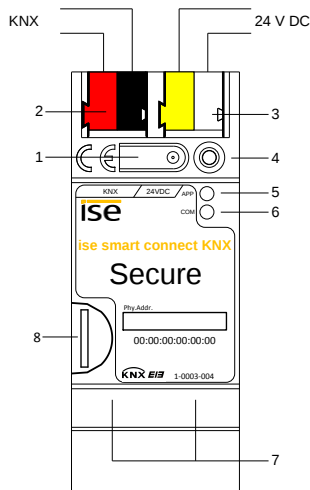
Wichtiger Hinweis: Bei einer Dauer es Kommunikations-Roundtrips von durchschnittlich über fünf Sekunden wird die KNX Kommunikation problematisch.

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 22: ise smart connect KNX Secure

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 gelb: Start- bzw. Diagnosecode, siehe 7.2.1 / 7.2.2	
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	Te-
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 beigelegten Bedienungsanleitung.

5.3 Montage und elektrischer Anschluss

Gerät montieren

- Aufsnappen 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 beigelegter KNX-Bus-Anschlussklemme. 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 23A).
- Abdeckkappe entfernen: Die Abdeckkappe wird entfernt, indem sie seitlich leicht eingedrückt und nach vorne abgezogen wird (vgl. Abbildung 23B).

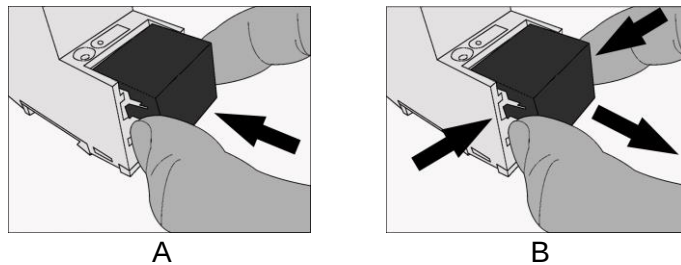


Abbildung 23: Abdeckkappe anbringen / entfernen.

6 Projektierung in der ETS

Hinweis: Der ise smart connect KNX Secure 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 physikalischen Adressen für den Tunneling Server haben alle die Adresse 15.15.254.

Die Projektierung des ise smart connect KNX Secure 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 Secure 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 Secure 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. | |
|---|--|

Wichtiger Hinweis: Der ise smart connect KNX Secure 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 Secure 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 Secure einstellen. | → Abschnitt 6.4.1 |
|---|-------------------|

- | | |
|--|-----------------|
| 5 Gruppenadressen an Gruppenobjekte wie üblich anbinden. | → Abschnitt 6.5 |
|--|-----------------|

- | | |
|---|--|
| 6 Der ise smart connect KNX Secure ist nun bereit zur Inbetriebnahme mittels „ETS Programmieren“ und zum Test der Funktionen. | |
|---|--|

6.1 Projektierung Schritt 1 – ise smart connect KNX Secure als Gerät in der ETS anlegen

Wenn noch nicht geschehen, importieren Sie die ETS-Geräte-Applikation zum ise smart connect KNX Secure 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.

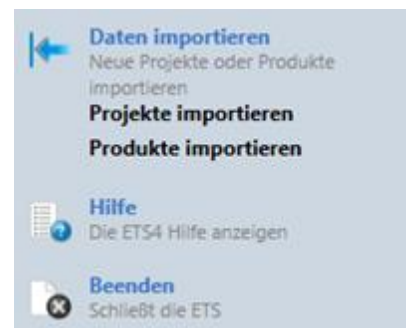


Abbildung 24: Produktimport über die ETS4-Startseite.

Die weiteren Erläuterungen in diesem Dokument beziehen sich auf

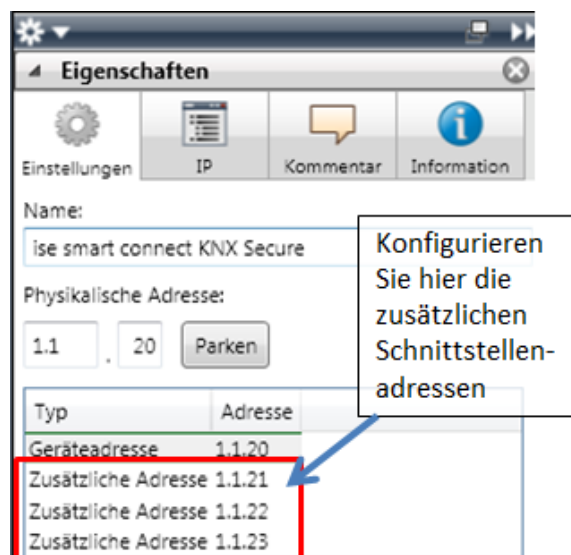
Hardware	Applikations-Software
Gerät: ise smart connect KNX Secure	Applikation: ise smart connect KNX Secure
Hersteller: ise GmbH	Version: V2.1
Bestell-Nr. 1-0003-004	
Version: V1.0	
Bauform: REG (Reiheneinbau)	

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 Secure verfügt über drei Tunneling Server (KNX/IP Interfaces). Diese Interfaces können für den Download als auch im Gruppen- und-Busmonitor-Modus genutzt werden. Neben der physikalischen Adresse des Geräts besitzt das Gerät daher noch (bis zu) drei weitere physikalische Schnittstellen. Diese können wie bei vielen Produkten heute üblich nach Öffnen der KNX/IP Verbindung in der ETS über die Einstellungen der Schnittstelle konfiguriert werden. In diesem Fall muss man selbst genau darauf achten, dass die Adressen nicht bereits anderweitig benutzt sind. Ab der ETS4 ist es möglich bei Produkten die Anzahl der zusätzlichen Adressen anzugeben, so dass diese in der ETS konfigurierbar sind. Hierzu erscheint unter dem Eingabefenster für die physikalische Adresse bei den Geräteeigenschaften in der ETS eine Liste mit den zusätzlichen Adressen. In diesem Fall stellt die ETS die Eindeu-



tigkeit 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 Secure 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 25 gezeigt.



Abbildung 25: Geräte-Eigenschaftendialog der ETS

3. Wählen Sie den Reiter „IP“ entsprechend Abbildung 26. 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 (s. Kapitel 6.4)!

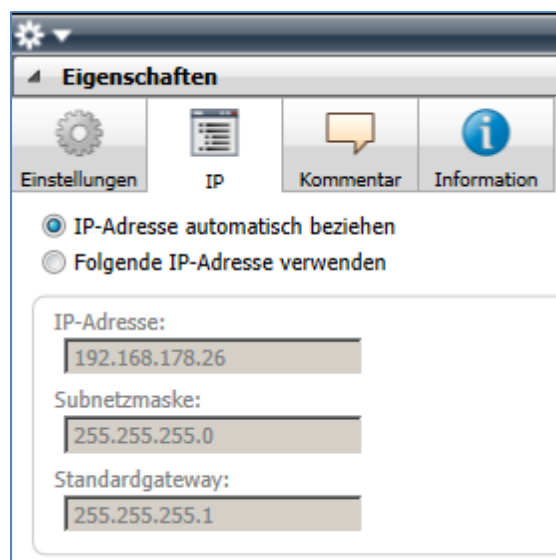


Abbildung 26: Einstellung der IP-Adressdaten des Geräts unter dem Reiter „IP“ im Sidebar der ETS

Bei der Einstellung ⊙ *IP-Adresse automatisch beziehen* muss ein DHCP-Server dem ise smart connect KNX Secure eine gültige IP-Adresse zuteilen.

Steht bei dieser Einstellung kein DHCP-Server zur Verfügung, so startet das Gerät nach einer Wartezeit mit einer Auto IP-Adresse (Adressbereich von 169.254.1.0 bis 169.254.254.255).

Sobald ein DHCP Server zur Verfügung steht, wird dem Gerät automatisch eine neue IP-Adresse zugewiesen.

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.

6.5 Gruppenadressen an Gruppenobjekte anbinden.

Am ise smart connect KNX Secure 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: Freigegeben

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= Verboten

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSÜA)
 2	Fernzugriff zulassen – Status	Lesen	1 Bit	1.003	KL-Ü-

Rubrik: Fernzugriff Datentyp: Freigegeben

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: Freigegeben

Funktion: Erlaubt oder verbietet den Fernzugriff jeweils für Mitglieder der Gruppe bzw. über „Quick Connect“.

Beschreibung: 1 = Erlauben, 0= Verboten

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: Freigegeben

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 Secure Geräts.				

Beschreibung: 1 = Alarm, 0= Kein Alarm

Objekt	Name	Richtung	Datenbreite	DP-Typ	Flags (KLSUA)
 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 (KLSUA)
 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.

7 Inbetriebnahme

7.1 Bedienung

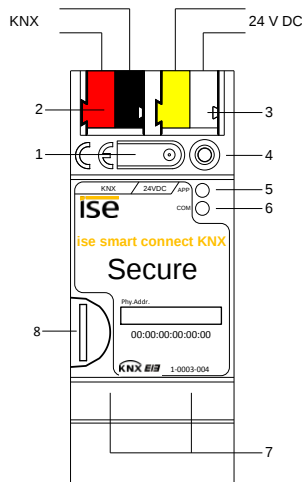


Abbildung 27: ise smart connect KNX Secure.

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 gelb: Start- bzw. Diagnosecode, siehe 7.2.1 / 7.2.2	
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	Te-
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	Als 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	<u>Fehler:</u> Keine Versorgungsspannung: Bitte Anschlüsse und Spannungsversorgung prüfen.	x
 aus	 gelb	Gerät startet.	✓
  grün blinken langsam (ca. 1 Hz)	 gelb	<u>Hinweis:</u> Das Gerät ist komplett hochgefahren, aber noch unparametriert. Ein ETS Download ist notwendig.	x
  grün blinken schnell	 aus	<u>Fehler:</u> Bitte kontaktieren Sie den Support. Die Firmware kann nicht gestartet werden.	x
      grün       gelb blinken langsam im Wechsel (ca. 1Hz)		<u>Fehler:</u> Bitte kontaktieren Sie den Support. Die neu geladene Firmware kann nicht gestartet werden. Das System versucht, die bisherige Firmware zu aktivieren (Ungültige Firmware).	x

7.2.2 LED-Statusanzeige im Betrieb

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

LED „APP“ (grün)	Bedeutung
 grün	<u>Normalbetrieb:</u> Der Fernzugriff ist generell erlaubt, das Gerät verbindet sich mit dem Portalserver, allerdings ist kein Fernzugriff derzeit aktiv.
 aus	<u>Gerät im Startvorgang oder außer Betrieb:</u> Warten Sie bis Startvorgang abgeschlossen ist bzw. prüfen Sie die Spannungsversorgung
 Einmal blinken langsam, mit 1 Hz, dann 2 s Pause	<u>Hinweis:</u> 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	<u>Hinweis:</u> 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	<u>Normalbetrieb:</u> KNX-Verbindung ist hergestellt, kein KNX-Telegrammverkehr.
 schnelles gelbes Blinken mit kurzen Dunkelphasen	<u>Normalbetrieb:</u> KNX-Verbindung ist hergestellt, KNX-Telegrammverkehr.
 aus	<u>Fehler:</u> 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.

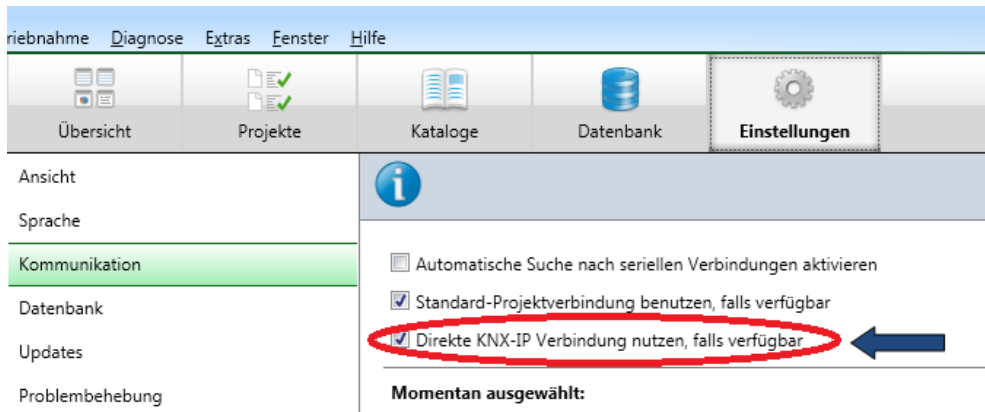


Abbildung 28: Die Einstellung „*Direkte KNX-IP-Verbindung nutzen, falls verfügbar*“ beschleunigt die Übertragung von der ETS zum Gerät.

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.
- Programmierertaste (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 Secure 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.

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

7.6 Werksreset

Werksseitig voreingestellt ist folgende physikalische KNX-Adresse:15.15.255

Nach dem Werksreset verhält sich das Gerät wie im Auslieferungszustand. Das Gerät ist unprojektiert. Dies ist nach dem Hochfahren des Gerätes an der langsam blinkenden grünen APP-LED (5) zu erkennen.

7.6.1 Über die Programmiertaste am Gerät

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

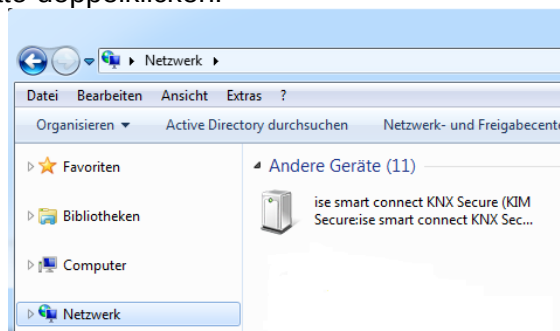
- Sicherstellen, dass das Gerät ausgeschaltet ist.
- Programmiertaste (1) drücken, gedrückt halten und das Gerät einschalten.
- Programmiertaste (1) gedrückt halten bis die Programmier-LED (4), die RUN-LED (5) und die KNX-LED (6) gleichzeitig langsam blinken.
- Programmiertaste (1) kurz loslassen, erneut 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.

7.6.2 Über die Webseite des Gerätes

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

- Aufrufen der Webseite des Gerätes. Dazu in der Netzwerkumgebung auf das Icon des Gerätes im Bereich *Andere Geräte* doppelklicken.

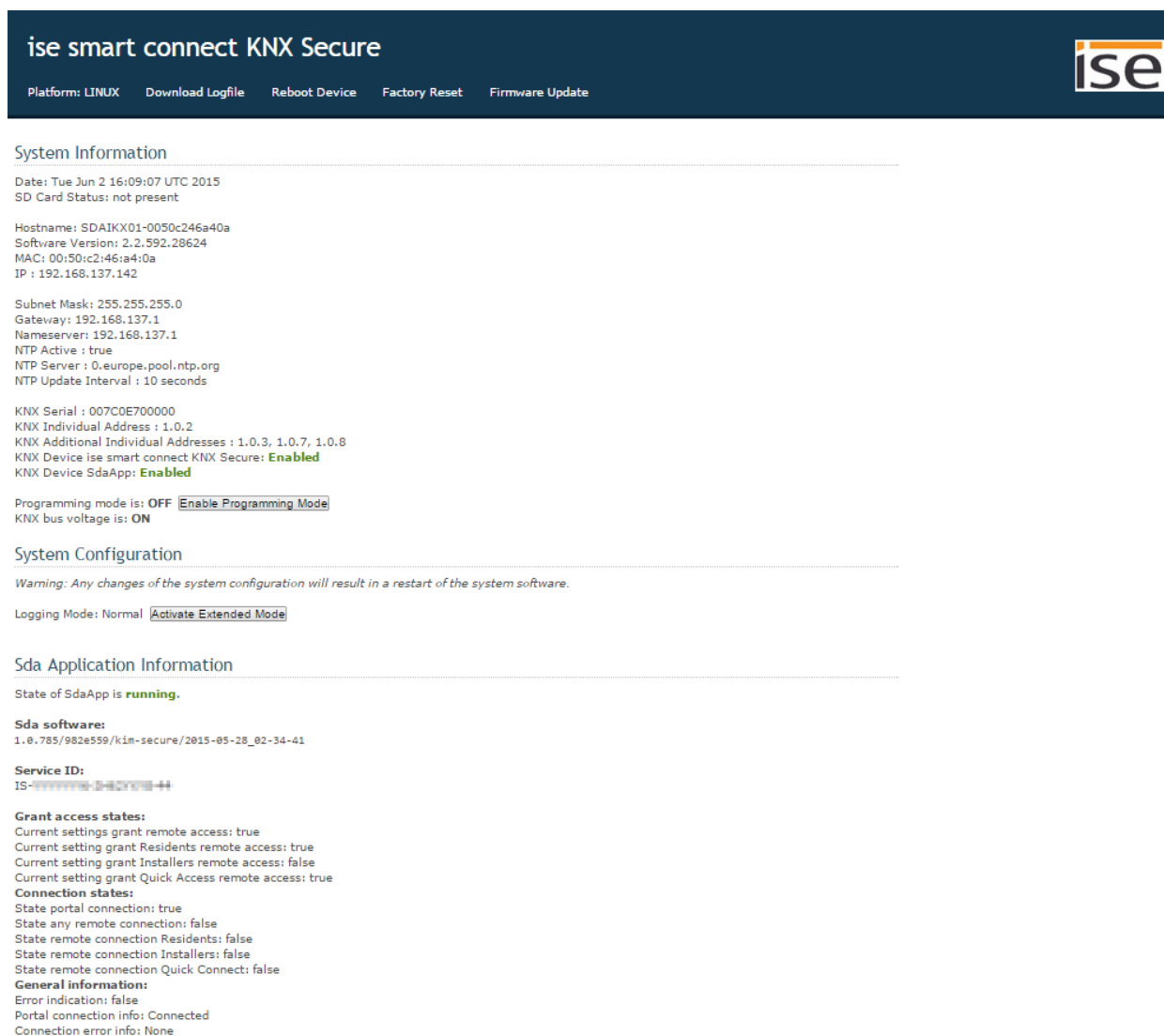


- Alternativ können Sie auch die IP-Adresse des Gerätes in Ihrem Browser eingeben.
- Auf der Webseite in der oberen Menüleiste *Device Status* auswählen.
- Auf der Status-Seite in der oberen Menüleiste *Factory Reset* auswählen.
- Bei der Sicherheitsabfrage den Werksreset bestätigen.
- Die nachfolgend angezeigte Seite *Factory Reset* zeigt die Durchführung des Werksresets an. Sobald dieser abgeschlossen ist, wird wieder die Startseite geladen.

7.7 Information Anzeigen über die Webseite

Der Aufruf der Webseite ist im Kapitel 7.6.2 – *Über die Webseite des Gerätes* beschrieben.

Die Startseite des Geräts zeigt die System Information, die System Configuration und die Application Information



ise smart connect KNX Secure

Platform: LINUX Download Logfile Reboot Device Factory Reset Firmware Update

System Information

Date: Tue Jun 2 16:09:07 UTC 2015
SD Card Status: not present

Hostname: SDAIKX01-0050c246a40a
Software Version: 2.2.592.28624
MAC: 00:50:c2:46:a4:0a
IP : 192.168.137.142

Subnet Mask: 255.255.255.0
Gateway: 192.168.137.1
Nameserver: 192.168.137.1
NTP Active : true
NTP Server : 0.europe.pool.ntp.org
NTP Update Interval : 10 seconds

KNX Serial : 007C0E700000
KNX Individual Address : 1.0.2
KNX Additional Individual Addresses : 1.0.3, 1.0.7, 1.0.8
KNX Device ise smart connect KNX Secure: **Enabled**
KNX Device SdaApp: **Enabled**

Programming mode is: **OFF** [Enable Programming Mode](#)
KNX bus voltage is: **ON**

System Configuration

Warning: Any changes of the system configuration will result in a restart of the system software.

Logging Mode: Normal [Activate Extended Mode](#)

Sda Application Information

State of SdaApp is **running**.

Sda software:
1.0.785/982e559/kin-secure/2015-05-28_02-34-41

Service ID:
IS-*****-*****-44

Grant access states:
Current settings grant remote access: true
Current setting grant Residents remote access: true
Current setting grant Installers remote access: false
Current setting grant Quick Access remote access: true

Connection states:
State portal connection: true
State any remote connection: false
State remote connection Residents: false
State remote connection Installers: false
State remote connection Quick Connect: false

General information:
Error indication: false
Portal connection info: Connected
Connection error info: None

Abbildung 29: Gerätewebseite für die die System Information, die System Configuration und die Application Information

Wichtiger Hinweis: Falls das ise smart connect KNX Secure Gerät 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.

8 Technische Daten

KNX-Medium	TP
Inbetriebnahme Modus	S-Mode (ETS)
Versorgung KNX	DC 21...30 V SELV
Anschluss KNX	Bus-Anschlussklemme
Externe Versorgung	
Spannung	DC 24...30V $\pm 10\%$
Anschluss	Bus-Anschlussklemme, 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 Secure?**
Bitte lesen Sie dies in Abschnitt 7.6.2 – *Über die Webseite des Gerätes* nach.
- **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 Secure noch die vorher konfigurierten physikalischen und IP Adresse?**
Die Webseite wird derzeit nach dem Entladen erst nach einem Geräteneustart aktualisiert.
- **Gibt es Software-Updates für mein ise smart connect KNX Secure-Gerät?**
Verfügbare Software-Updates finden Sie auf der Firmenwebseite. Bitte besuchen Sie den Produktbereich auf www.ise.de für weitere Informationen.
- **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 6.5 – *Gruppenadressen an Gruppenobjekte anbinden*.
- **In meiner ETS4 erscheinen nicht automatisch die KNX/IP Schnittstellen, die über den SDA Client veröffentlicht 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 (Tunneling 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 Secure 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 Secure 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.

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

- **Wenn 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 (s. Kapitel 10) 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.

10 Fehlersuche und Support

Wenn Sie ein Problem mit Ihrem ise smart connect KNX Secure 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 Secure 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 7.6.2) herunterladen. Gehen Sie dazu folgendermaßen vor:

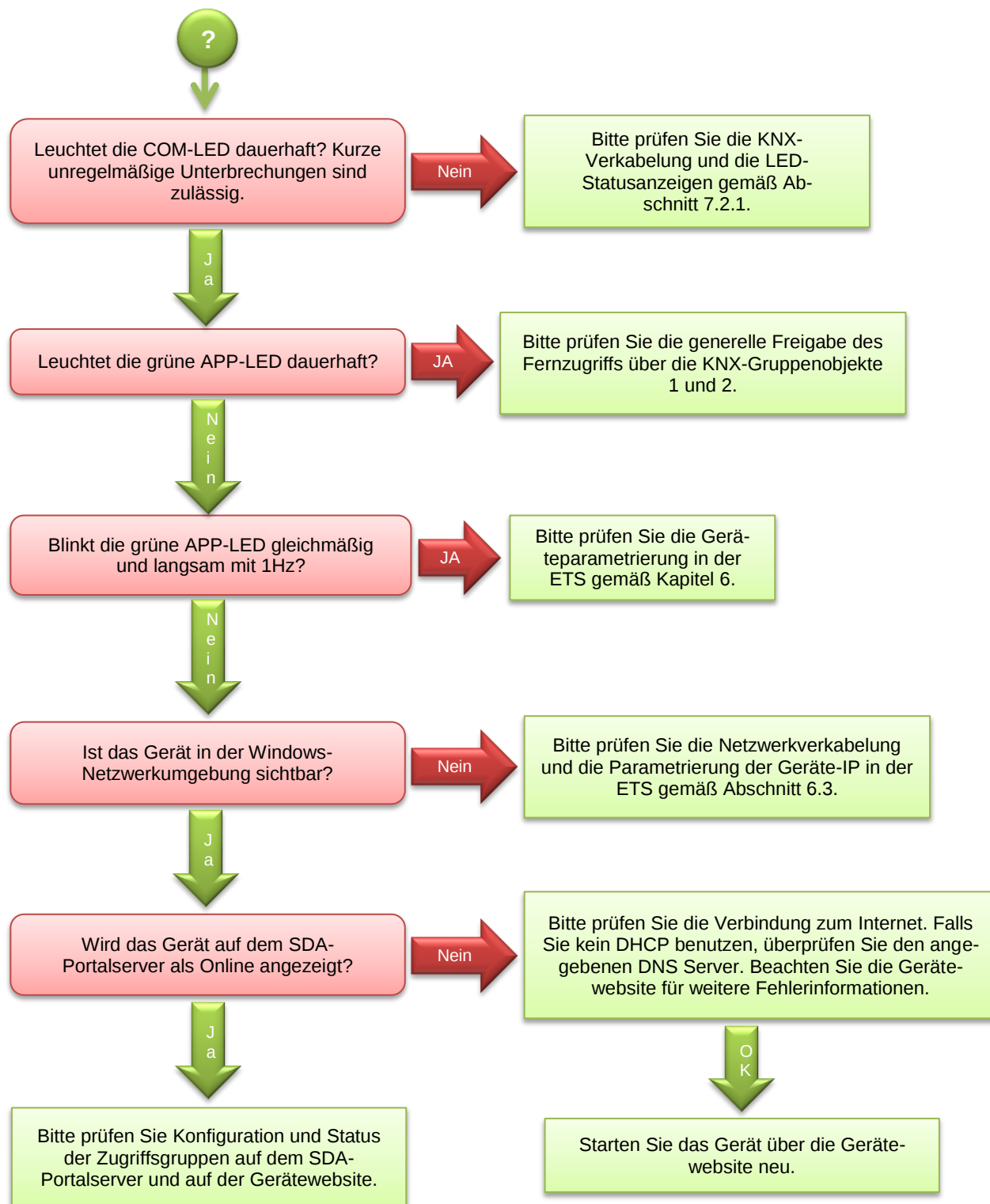
- Aufrufen der Webseite des Gerätes. Dazu in der Netzwerkumgebung auf das Icon des Gerätes im Bereich *Multimedia* doppelklicken.
- Auf der Webseite in der oberen Menüleiste *Device Status* auswählen.
- Auf der Status-Seite in der oberen Menüleiste *Download Logfile* auswählen.
- Die sich öffnende Seite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

10.2 Statusseite des ise smart connect KNX Secure

Auf der Webseite des ise smart connect KNX Secure (siehe Abschnitt 7.6.2) können Sie den Gerätstatus aufrufen. Dieser zeigt unter anderem die installierte Softwareversion sowie die Konfiguration und den Verbindungsstatus zum SDA Portal Server des ise smart connect KNX Secure an. Im Falle eines Fehlers senden Sie uns bitte einen Screenshot der Statusseite zu.

10.3 Der ise smart connect KNX Secure 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 Secure-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 Secure-Software oder der Ingebrauchnahme des ise smart connect KNX Secure schließen Sie einen Vertrag mit der Firma ise Individuelle Software-Entwicklung GmbH, und erklären sich an die Bestimmungen dieses Vertrages gebunden.

11.1 Definitionen

Lizenzgeber: ise Individuelle Software-Entwicklung GmbH, Oldenburg, Kaiserstraße 14, Deutschland

Lizenznehmer: Der rechtmäßige Empfänger der ise smart connect KNX Secure-Software

Firmware: Software, die auf der ise smart connect KNX Secure-Hardware eingebettet ist und zum Betrieb des ise smart connect KNX Secure dient.

ise smart connect KNX Secure Software: Als ise smart connect KNX Secure-Software wird die gesamte Software inklusive der Betriebsdaten bezeichnet, die für das Produkt ise smart connect KNX Secure 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 Secure-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 Secure-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 Secure-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 securedeviceaccess.net GbR. Der Lizenzgeber kann aus wichtigem Grund den Betrieb des SDA Portalserver 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 500 MB 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 Secure-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 Umwandlungstechniken

Der Lizenznehmer ist nicht berechtigt Reverse-Engineering Techniken auf die ise smart connect KNX Secure-Software anzuwenden oder die ise smart connect KNX Secure-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 Secure) installiert und genutzt werden.

11.4.5 Weitergabe an Dritte

Die ise smart connect KNX Secure-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 Secure-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 Secure-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 Secure-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 Secure-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 Secure-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 Secure-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 Secure-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 Secure-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 beigelegten 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 Secure-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 Secure-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 Secure-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 Secure-Software. Das Produkt ise smart connect KNX Secure muss in diesem Fall außer Betrieb genommen werden. Eine weitere Nutzung des ise smart connect KNX Secure 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 der GNU General Public License (GPL), bzw. Lesser GNU General Public License LGPL verwendet werden, sowie im Rahmen der Berkeley Software Distribution (BSD) und der MIT Lizenz.

Die in diesem Produkt verwendeten Software-Pakete, die in den genannten Rahmen lizenziert sind, werden im Folgenden beschrieben.

Software-Paket	U-Boot
Version der Software	2012.07
Bezugsquelle	http://www.denx.de/wiki/U-Boot/WebHome
Lizenz	GNU GPL, Version 2, June 1991
Copyright-Vermerk	Copyright © 2000-2012 by Wolfgang Denk et al.

Software-Paket	GNU/Linux
Version der Software	3.2.20
Bezugsquelle	http://kernel.org
Lizenz	GNU GPL, Version 2, June 1991
Copyright-Vermerk	Copyright © 1992-2013 by Linus Torvalds et al.

Software-Paket	Buildroot
Version der Software	2012.11
Bezugsquelle	http://buildroot.org
Lizenz	GNU GPL, Version 2, June 1991
Copyright-Vermerk	Copyright © 1999-2005 Erik Andersen, 2006-2012 The Buildroot developers

Software-Paket	GNU C Library (GLIBC)
Version der Software	2.30.3
Bezugsquelle	http://www.gnu.org/s/libc/
Lizenz	GNU LGPL, Version 2.1, February 1999
Copyright-Vermerk	Copyright © 1996-2012 by Roland McGrath et al.

Software-Paket	Boost C++ Libraries
Version der Software	1.49.0 (Firmware) und 1.55.0 (SDA Client)
Bezugsquelle	http://www.boost.org
Lizenz	Boost Software Licence, Version 1.0
Copyright-Vermerk	Copyright 2012 Boost.org

Software-Paket	libupnp
Version der Software	1.6.17
Bezugsquelle	http://sourceforge.net/projects/pupnp/files/pupnp/
Lizenz	BSD
Copyright-Vermerk	Copyright (c) 2000-2003, Intel Corporation. All rights reserved.

Software-Paket	Websocketpp
Version der Software	0.3.x
Bezugsquelle	http://www.zaphoyd.com/websocketpp
Lizenz	BSD
Copyright-Vermerk	Copyright (c) 2013, Peter Thorson. All rights reserved.

Software-Paket	jQuery
Version der Software	1.11.1
Bezugsquelle	https://jquery.org
Lizenz	MIT Licence
Copyright-Vermerk	Copyright 2014 The jQuery Foundation

Software-Paket	openssl
Version der Software	1.0.0 (Firmware) und 1.0.1 (SDA Client)
Bezugsquelle	https://www.openssl.org
Lizenz	OpenSSL License und SSLeay License
Copyright-Vermerk	Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved. Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

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

Der Quellcode für diese Software kann über die E-Mail-Adresse info@ise.de bezogen werden.

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

13 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

- a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasona-

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

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

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

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

- a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

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

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

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modi-

fy, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

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

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

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

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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

case, this License incorporates the limitation as if written in the body of this License.

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

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

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

NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

14 OpenSSL Lizenzen

LICENSE ISSUES
=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

14.1 OpenSSL License

```
/* =====
 * Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * =====
 *
```

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

14.2 Original SSLeay License

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

* [including the GNU Public Licence.]
*/