Produkthandbuch

SMART CONNECT KNX Remote Access

1-0003-004

Dokumentation gilt für:

Produktdatenbankeintrag:	v6.1
Firmware:	v6.1
SDA-Client:	ab v1.6
Stand der Dokumentation:	25.05.2021

© 2021 ise Individuelle Software und Elektronik GmbH

Inhaltsverzeichnis

© 2021 ise Individuelle Software und Elektronik GmbH

© 2021 ise Individuelle Software und Elektronik GmbH

Rechtliche Hinweise

SMART CONNECT KNX Remote Access Produkthandbuch
Stand: 25.05.2021

ise Individuelle Software und Elektronik GmbH
Osterstraße 15
26122 Oldenburg, Deutschland
© Copyright 2021 ise Individuelle Software und Elektronik GmbH

Alle Rechte vorbehalten. Kein Teil dieses Dokuments darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne vorherige schriftliche Genehmigung von ise Individuelle Software und Elektronik GmbH bearbeitet, vervielfältigt, verbreitet oder öffentlich zugänglich gemacht werden.

Produkte, auf die sich in diesem Dokument bezogen wird, können entweder Marken oder eingetragene Marken der jeweiligen Rechteinhaber sein. Ise Individuelle Software und Elektronik GmbH und der Autor erheben keinen Anspruch auf diese Marken. Die Nennung der Marken dient lediglich der notwendigen Beschreibung.

Warenzeichen

KNX ist ein eingetragenes Warenzeichen der KNX Association.

Feedback und Informationen zu Produkten

Bei Fragen zu unseren Produkten, kontaktieren Sie uns bitte per E-Mail an vertrieb@ise.de. Gerne nehmen wir Anregungen, Verbesserungsvorschläge und Kritik per E-Mail über support@ise.de entgegen.

1 Über diese Dokumentation

Diese Dokumentation begleitet Sie durch alle Phasen des Produktlebenszyklus Ihres SMART CONNECT KNX Remote Access. Sie erfahren u. a. wie Sie das Gerät montieren, installieren, in Betrieb nehmen und projektieren.

Alle Beschreibungen in dieser Dokumentation zur Projektierung in der ETS beziehen sich auf die Variante „ETS Professional“ in der Version 5.

Erläuterungen zu den Konzepten von KNX sind nicht Bestandteil dieser Dokumentation.

1.1 Zielgruppe

Diese Dokumentation richtet sich an Elektrofachkräfte und KNX Verarbeiter.

Der SMART CONNECT KNX Remote Access darf ausschließlich von Elektrofachkräften montiert und installiert werden. Fachkenntnisse zu KNX werden vorausgesetzt.

Der SMART CONNECT KNX Remote Access darf von jedermann projektiert werden. Wir empfehlen die Projektierung von einem Systemintegrator durchführen zu lassen. Sie benötigen solide Fachkenntnisse zu KNX und im Umgang mit der ETS.

1.2 Symbole und typografische Konventionen

Symbol / Auszeichnung	Bedeutung
	Warnung vor möglichen Sachschäden
	Allgemeine Warnung
	Warnung vor elektrischer Spannung

Tabelle 1: Symbole und Sicherheitshinweise

Symbol / Auszeichnung	Bedeutung
[F1]	PC-Taste
<<Beschriftung>>	Text auf Softwareoberfläche
	Tipp, Fehlerbehandlung
	Wichtige zusätzliche Information

Tabelle 2: Besondere Symbole und Schriftkonventionen

© 2021 ise Individuelle Software und Elektronik GmbH

2 Über SMART CONNECT KNX Remote Access

2.1 Bestimmungsgemäßer Gebrauch

Der SMART CONNECT KNX Remote Access ermöglicht einen sicheren Fernzugriff auf Ihre KNX Installation. Zusätzlich lässt sich eine VPN-Verbindung mit Ihrem Ethernet-basierten Heimnetzwerk herstellen. Um die Fernwartung mit der ETS durchzuführen, haben Sie mit dem SDA-Client für Windows Zugriff auf:

- die in der KNX Installation vorhandenen IP-Schnittstellen,
- die im entfernten Netzwerk befindlichen Geräte.

Der SMART CONNECT KNX Remote Access ist ein Gerät des KNX Systems und entspricht den KNX Richtlinien.

Achtung

Ise Individuelle Software und Elektronik GmbH haftet nicht für Schäden, die durch unsachgemäße oder bestimmungsfremde bzw. bestimmungswidrige Verwendung entstehen.

Projektierung: Kompatible ETS-Versionen

Einfache Einbindung in das KNX-System (komplett über die ETS programmierbar):

- ETS5 oder höher,
- Produktdatenbankeintrag: Laden Sie den Produktdatenbankeintrag von unserer Webseite unter www.ise.de oder aus dem Online-Katalog der ETS kostenlos herunter.

KNX Secure

SMART CONNECT KNX Remote Access ist KNX Secure.

Das Gerät ist KNX Secure kompatibel. KNX Secure bietet Schutz vor Manipulation in der Gebäudeautomation und kann im ETS-Projekt konfiguriert werden.

- Das notwendige KNX Secure-Zertifikat bzw. der darin enthaltene FDSK (Factory-Default Setup-Key, Fabrikschlüssel) befindet sich seitlich als Aufkleber auf dem Gerät und liegt zusätzlich dem Gerät bei.
- Für maximale Sicherheit empfehlen wir, den Aufkleber auf dem Gerät zu entfernen.
- Bewahren Sie das Zertifikat sicher auf.
- Das Zertifikat können Sie selbst nicht wiederherstellen.
- Falls Sie das Zertifikat trotz aller Sorgfalt verlieren sollten, kontaktieren Sie unseren Support.

© 2021 ise Individuelle Software und Elektronik GmbH

2.2 System

Der SMART CONNECT KNX Remote Access wird mit der KNX Installation über KNX/TP verbunden. Das Gerät wird über IP mit dem Internet verbunden, um den Zugriff auf das KNX System zu ermöglichen. Die Konfiguration des Fernzugriffs erfolgt über Secure Device Access (SDA) im SDA-Portal auf https://securedeviceaccess.net.
Die Kommunikation zwischen dem SMART CONNECT KNX Remote Access und dem SDA-Portalserver ist per AES verschlüsselt und mit digitalen Zertifikaten gesichert.

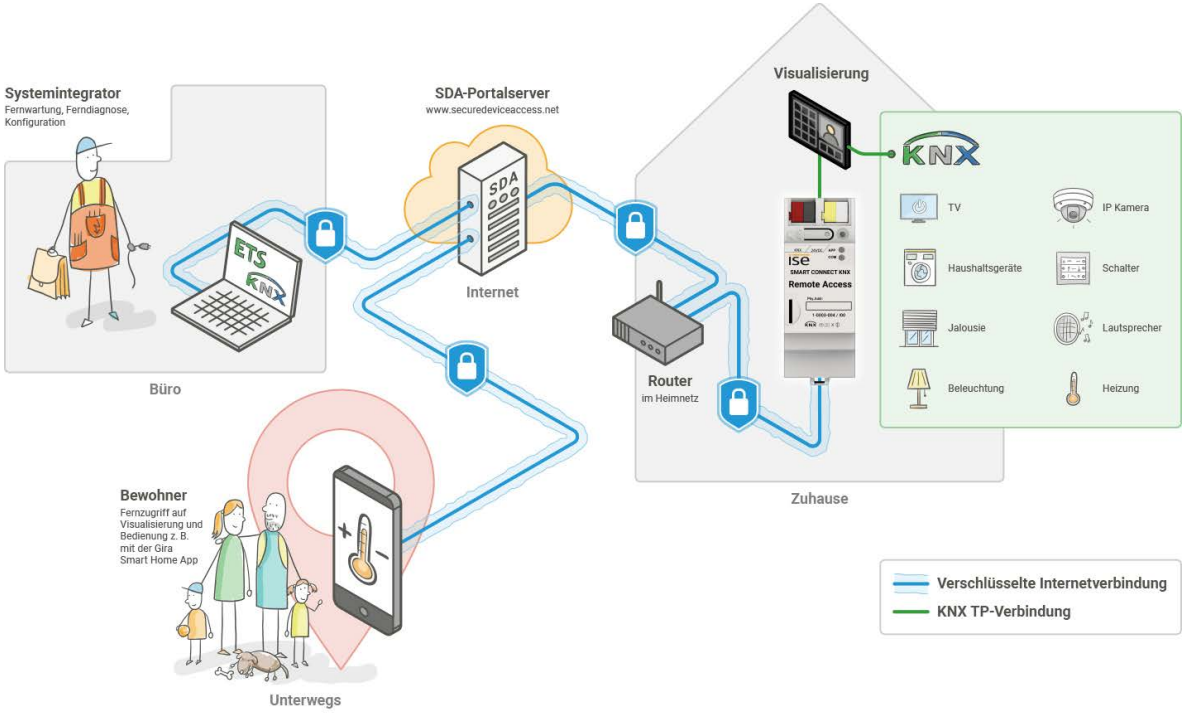


Abbildung 1: Remote Access Systemgrafik

2.3 Funktionen und Anwendungsfälle

- Um per Fernzugriff auf die KNX Geräte zuzugreifen, verbinden Sie den SMART CONNECT KNX Remote Access mit der KNX Installation.
- Der SMART CONNECT KNX Remote Access wird per Ethernet an das Heimnetzwerk angeschlossen. Er verbindet sich automatisch über Ihren vorhandenen Internetzugang mit dem SDA-Portalserver https://securedeviceaccess.net ► siehe Nutzung des SDA-Portalservers, S. 8
- Einsatz als Datenlogger. Der SMART CONNECT KNX Remote Access besitzt einen Kartenleser für microSDHC-Karten bis 32 GB. Auf der Karte können die KNX Telegramme in einem ETS5-konformen Format für Analysen aufgezeichnet werden. Der Kartenspeicher kann als Ringspeicher oder als Festspeicher verwendet werden.
- Einsatz als Zeitgeber. Der SMART CONNECT KNX Remote Access kann Zeit und Datum in konfigurierbaren Intervallen auf den Bus senden. Es ist möglich, über einen Trigger das Senden der aktuellen Zeit und des aktuellen Datums auszulösen.
- VPN-Netzkopplung (wahlweise Layer 2 oder Layer 3) ermöglicht u. a. den Zugriff auf KNX Installationen, Visualisierungsoberflächen und Dateien im Heimnetz. Auch für Smartphone-Apps ist somit ein unkomplizierter Zugang zum KNX System und weiteren Anwendungen gewährleistet. Der VPN-Zugriff lässt sich über KNX Kommunikationsobjekte steuern und überwachen.

© 2021 ise Individuelle Software und Elektronik GmbH

- Verwaltung von Fernzugriffsoptionen und Zugriffsrechten im SDA-Portal ► siehe Funktionen des SDA-Portals, S. 9
- Zugriff auf die HTML-Seiten von jedem Netzwerk-Endgerät ► siehe Zugriff auf Webseiten im entfernten Netzwerk, S. 10
- KNX Kommunikation mit der ETS per KNXnet/IP, IP-Direkt-Download und Eiblib/IP über den SDA-Client ► siehe Fernzugriffsoptionen des SDA-Clients, S. 16
- Konfigurationszugriff auf den Gira HomeServer mit dem HomeServer Experten über den SDA-Client.
- Zugriff auf Windows-Rechner über die Remotedesktopverbindung über den SDA-Client.
- Frei konfigurierbare TCP-Portweiterleitungen über den SDA-Client für Windows.
- Benachrichtigungen lassen sich über KNX Telegramme auslösen, auf dem SDA-Portalserver speichern und z. B. per E-Mail, Sprachanruf oder SMS weiterleiten.
- KNX/TP Anschluss mit integriertem IP-Interface (Tunneling Server) für den KNX Zugriff über die ETS oder andere Software. Es lassen sich drei gleichzeitige Verbindungen für die Nutzung des Downloads, des Gruppen- und Busmonitors einrichten.
- Statussignalisierung und Zugriffsmanagement der gesicherten Verbindungen über KNX Kommunikationsobjekte.
- Secure Device Access funktioniert zudem über einen Mobilfunkzugang, auch wenn dieser nicht über eine eindeutige von außen erreichbare IP-Adresse verfügt wie z. B. bei UMTS oder LTE üblich.
- Für Ihren Internetrouter unterscheidet sich die Kommunikation des SMART CONNECT KNX Remote Access nicht von einer verschlüsselten Verbindung Ihres Browsers z. B. beim Onlinebanking.

Funktionserweiterungen durch Aktualisierungen

Funktionserweiterungen für den SMART CONNECT KNX Remote Access erhalten Sie über eine neue Version der Firmware. Die jeweils aktuelle Firmware und das passende Produkthandbuch laden Sie einfach von unserer Webseite www.ise.de herunter.

► siehe Firmware über die Gerätewebseite aktualisieren, S. 45

© 2021 ise Individuelle Software und Elektronik GmbH

2.4 Nutzung des SDA-Portalservers

Der SDA-Portalserver und damit das SDA-Portal sind unter https://securedeviceaccess.net erreichbar. Der SDA-Portalserver dient als Vermittlungsstelle während des Fernzugriffs auf Endgeräte in Ihrem Gebäude.
Der SMART CONNECT KNX Remote Access verwendet zur Kommunikation mit dem SDA-Portalserver die Standardprotokolle HTTPS, TLS/SSL und Websockets. Der SDA-Portalserver speichert die übertragenen Daten nicht, sondern leitet diese nur weiter. Der Server wird in Deutschland unter Einhaltung der strengen europäischen Datenschutzrichtlinien betrieben.

Hinweis auf Cookies

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

Um den SDA-Portalserver nutzen zu können, stehen Ihnen die folgenden Möglichkeiten zur Verfügung:

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

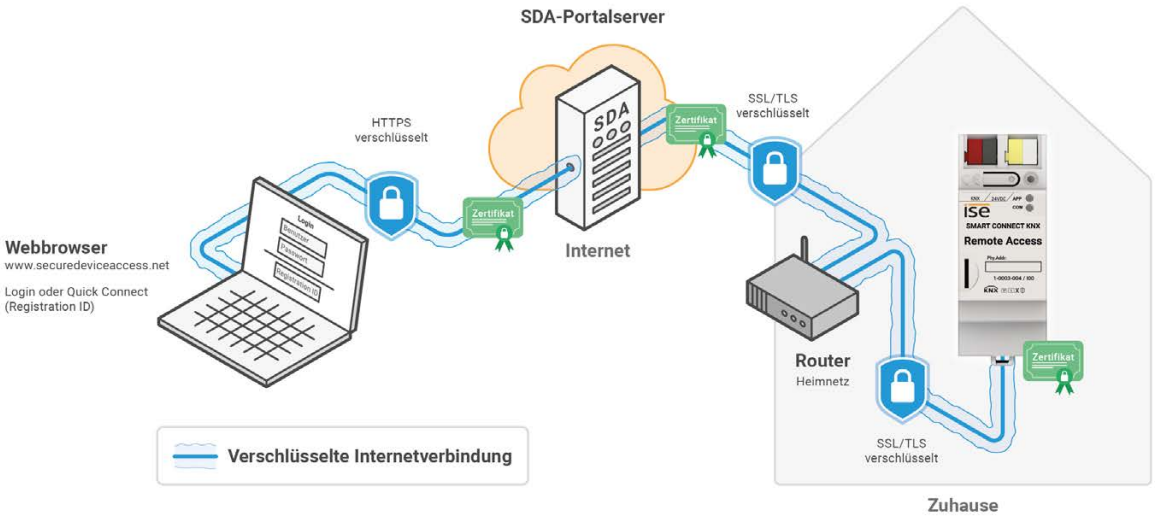


Abbildung 2: Sicherer Zugriff mit Secure Device Access

© 2021 ise Individuelle Software und Elektronik GmbH

Quick Connect vs. Portal-Login

Bei Quick Connect wird ausschließlich über Eingabe der Registration ID auf die Installation aus der Ferne zugegriffen. Dies hat den Vorteil, dass man keine Benutzer im SDA-Portal anmelden muss. Ein Anwendungsfall ist z. B. ein SMART CONNECT KNX Remote Access auf einer Baustelle in Verbindung mit einem UMTS/LTE Router, der für jeden Kollegen schnell und unkompliziert nutzbar sein soll.

Dagegen können einem Benutzerkonto im SDA-Portal beliebig viele SMART CONNECT KNX Remote Access zugeordnet werden.

Um den Zugriff per Quick Connect zu verhindern, können Sie jederzeit Ihren SMART CONNECT KNX Remote Access 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.

Unabhängig vom Einsatz von Quick Connect oder Portal-Login stehen jeweils alle Zugriffsmöglichkeiten (ETS, HTTP, Gira HomeServer etc.) zur Verfügung.

Funktionen des SDA-Portals

Im SDA-Portal stehen Ihnen die folgenden Funktionen zur Verwaltung Ihres SMART CONNECT KNX Remote Access zur Verfügung:

- Einrichten von Benutzern und Zugriffsgruppen und verwalten der Zugriffsrechte
- Hinzufügen weiterer SDA-Geräte
- Abrufen von Gerätedaten
- Konfigurieren des VPN-Zugangs
- Erstellen von Weiterleitungsregeln von SDA-Benachrichtigungen
- Aufrufen eingegangener SDA-Benachrichtigungen
- Hinzufügen von Links zum Aufrufen von Web-Oberflächen im entfernten Netzwerk
- Einrichten von Applikationszugängen zur Nutzung von unterstützten Apps

© 2021 ise Individuelle Software und Elektronik GmbH

Zugriff auf Webseiten im entfernten Netzwerk

Netzwerkgeräte mit einem integrierten Webserver (z. B. Kameras oder Netzwerkdrucker) sind über den SMART CONNECT KNX Remote Access erreichbar und bekommen automatisch einen eigenen Namen unterhalb der Domain httpaccess.net.
Unter diesem Namen können Sie mit einem Webbrowser das entsprechende Netzwerkgerät erreichen. Die Kommunikation über das Internet ist verschlüsselt und es erfolgt eine Benutzerauthentifizierung gemäß der für Ihren SMART CONNECT KNX Remote Access auf dem SDA-Portalserver eingestellten Zugriffsfreigaben. Die Konfiguration erfolgt im SDA-Portal.

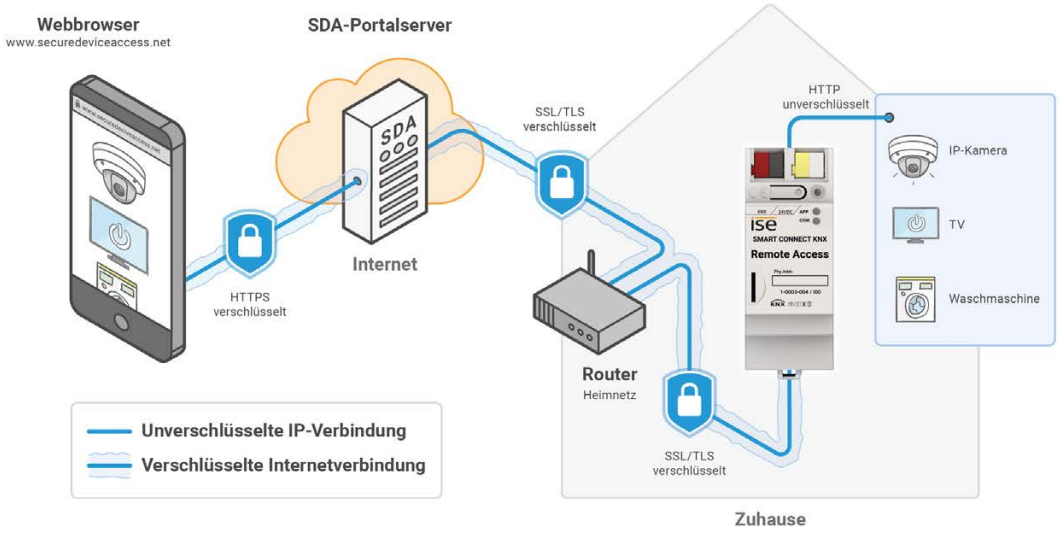


Abbildung 3: Sicherer Zugriff auf Webseiten mit Secure Device Access

© 2021 ise Individuelle Software und Elektronik GmbH

2.5 SDA-Client

Der SDA-Client ist eine Applikation, die den sicheren Zugriff auf Geräte im entfernten Netzwerk über das Internet ermöglicht. Dafür wird der SDA-Client auf dem gleichen PC wie die ETS installiert und gestartet.

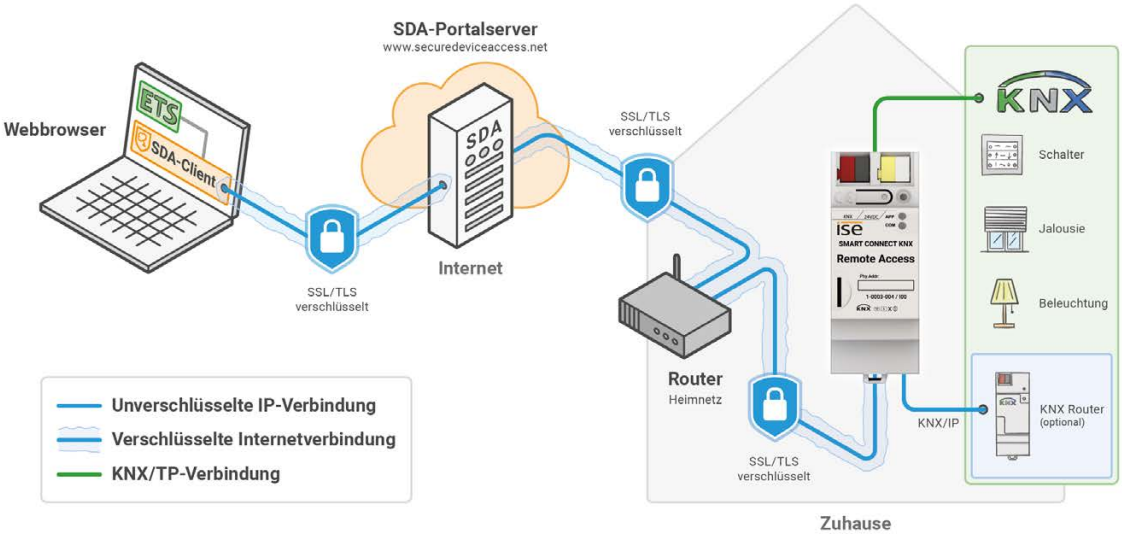


Abbildung 4: Sicherer Zugriff auf die KNX Installation mit Secure Device Access

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

Für einen Zugriff auf die Geräte über HTTP ist kein SDA-Client erforderlich, Sie können direkt das SDA-Portal verwenden.

Der SDA-Client ist derzeit für Microsoft Windows ab der Version 8 verfügbar.

Anwendungsfälle

Der SDA-Client kommt in folgenden Anwendungsfällen zum Einsatz:

- Fernzugriff auf KNX Installation über das KNX/IP-Protokoll
- Fernkonfiguration eines Gira HomeServers mit dem HomeServer Experten
- Fernzugriff über andere TCP-Protokolle (z. B. Remotedesktopverbindung RDP)

Verbindungsoptionen

Es gibt zwei Optionen eine Verbindung zum SMART CONNECT KNX Remote Access herzustellen:

- Portal Login (siehe Verbindung über Portal Login herstellen, S. 13)

© 2021 ise Individuelle Software und Elektronik GmbH

- Quick Connect (siehe Verbindung über Quick Connect herstellen, S. 15)

SDA-Client installieren

1. Scrollen Sie auf der Produktseite zum Downloadbereich.
2. Laden Sie die passende Installationsdatei für Windows (x86) oder (x64) herunter.
3. Führen Sie die Installationsdatei auf dem gleichen PC wie die ETS aus.

2.5.1 Allgemeine Einstellungen des SDA-Clients

1. Starten Sie den SDA-Client.
2. Öffnen Sie die allgemeinen Einstellungen über das Zahnrad  . Informationen zu spezifischen Einstellungen entnehmen Sie der folgenden Tabelle.

Einstellung	Beschreibung
ETS Zugriff für das gesamte lokale Netzwerk (LAN) aktivieren (ansonsten nur für diesen PC)	• Aktiviert: Alle im gleichen lokalen Netzwerk laufenden Clients haben Zugriff auf die KNX/IP-Geräte. • Deaktiviert: Die KNX/IP-Geräte sind nur für den aktuellen Client verfügbar. Der Client ist der PC, auf dem Ihre ETS läuft. Der PC wird anhand seiner IP-Adresse identifiziert. Die KNX/IP-Geräte werden in der ETS unter <<Gefundene Schnittstellen>> angezeigt.
Sicheren Fernzugriff auf den Gira HomeServer für neue SDA-Connector Konfigurationen automatisch aktivieren	Setzen Sie diese Einstellung, wenn Sie in Ihren Projekten regelmäßig den Gira HomeServer nutzen.
ETS4 Version prüfen	Ermöglicht eine Kompatibilitätsprüfung der ETS4, weil die automatische Suche der KNX/IP-Verbindungen mit ETS-Versionen älter als ETS4.2 möglicherweise eingeschränkt ist.

Tabelle 3: SDA-Client Einstellungen

© 2021 ise Individuelle Software und Elektronik GmbH

2.5.2 Verbindung über Portal Login herstellen

Voraussetzung: Sie sind im SDA-Portal als Benutzer registriert.

1. Starten Sie den SDA-Client.
2. Wählen Sie den Verbindungstyp <<Portal>>.

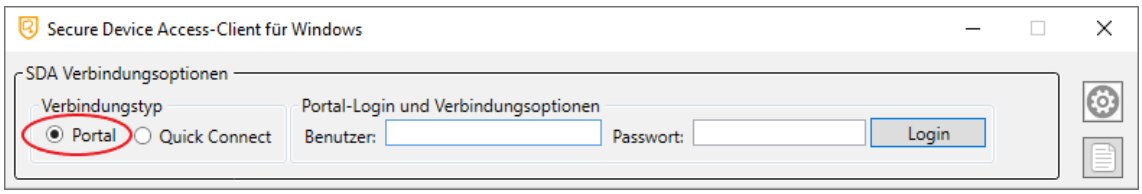


Abbildung 5: Verbindungstyp Portal

3. Melden Sie sich mit den gleichen Benutzerdaten wie im SDA-Portal an.
4. Wählen Sie das gewünschte Gerät.

Nutzen Sie den Filter, wenn Sie mit mehreren Geräten arbeiten. Geben Sie entweder einen Text ein oder begrenzen Sie mit der Funktion <<Nur online>> die Auswahl auf die derzeit im SDA-Portal angemeldeten Geräte.

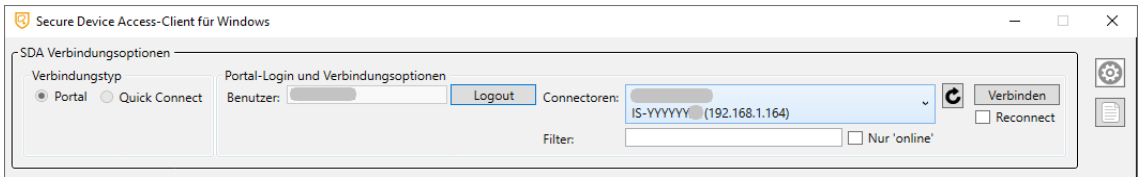


Abbildung 6: Geräteauswahl für Portal Login

5. Wählen Sie den Fernzugriff entsprechend Ihrem Anwendungsfall. Der Fernzugriff über KNX/IP ist standardmäßig aktiviert (siehe Fernzugriffsoptionen des SDA-Clients, S. 16).
6. Definieren Sie bei Bedarf externe Kommandos, die nach Herstellung oder nach Abbruch einer Verbindung ausgeführt werden sollen.
   In das linke Eingabefeld tragen Sie den Namen des Kommandos oder des Programms mit dem Pfad ein. Das Eingabefeld <<Argumente>> füllen Sie mit allen Parametern, die zur Ausführung übergeben werden sollen.

Abbildung 7: Externe Kommandos

Kombinieren Sie externe Kommandos mit der Funktion <<Reconnect>> unter der Schaltfläche <<Verbinden>>. Mit dieser Funktion versucht der SDA-Client die Verbindung nach einem Verbindungsabbruch automatisch wiederherzustellen.

© 2021 ise Individuelle Software und Elektronik GmbH

7. Klicken Sie auf <<Verbinden>>, nachdem Sie alle gewünschten Einstellungen definiert haben.

   Bei einer aktiven Verbindung können Sie die Kommunikationsgeschwindigkeit messen  .
   Das heißt, gemessen wird die Zeit ab Versenden einer Anfrage in das Zielnetzwerk des SMART CONNECT KNX Remote Access bis zum Erhalt einer Antwort vom SMART CONNECT KNX Remote Access.

    Detaillierte Verbindungsinformationen entnehmen Sie dem Logbuch  .

   Eine aktive Verbindung trennen Sie über die Schaltfläche <<Trennen>> oder, indem Sie den SDA-Client schließen.

© 2021 ise Individuelle Software und Elektronik GmbH

2.5.3 Verbindung über Quick Connect herstellen

Aus Sicherheitsgründen wird der Dauerbetrieb über Quick Connect nicht empfohlen. Die Verbindung über Quick Connect ist nur in Ausnahmesituationen zu nutzen, z. B. bei einem dringenden Fernzugriff direkt nach der Installation des Geräts.

1. Starten Sie den SDA-Client.
2. Wählen Sie den Verbindungstyp <<Quick Connect>>.

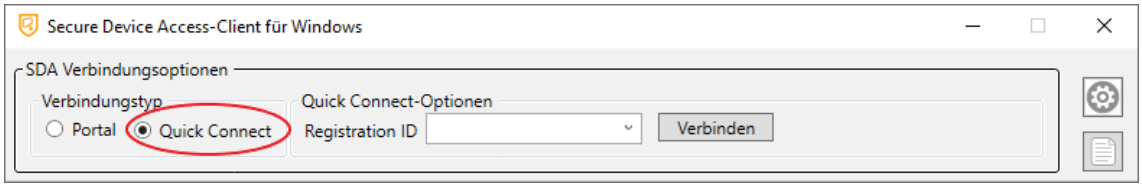


Abbildung 8: Verbindungstyp Quick Connect

3. Geben Sie die Registration ID des Geräts ein oder wählen Sie ein bereits genutztes Gerät aus der Auswahlliste. Die Optionen für den Fernzugriff werden erst eingeblendet, wenn die Eingabe korrekt ist.
4. Wählen Sie den Fernzugriff entsprechend Ihrem Anwendungsfall. Der Fernzugriff über KNX/IP ist standardmäßig aktiviert. Siehe Fernzugriffsoptionen des SDA-Clients, Seite 16.
5. Definieren Sie bei Bedarf externe Kommandos, die nach Herstellung oder nach Abbruch einer Verbindung ausgeführt werden sollen.

   In das linke Eingabefeld tragen Sie den Namen des Kommandos oder des Programms mit dem Pfad ein. Das Eingabefeld <<Argumente>> füllen Sie mit allen Parametern, die zur Ausführung übergeben werden sollen.

   Kombinieren Sie externe Kommandos mit der Funktion <<Reconnect>> unter der Schaltfläche <<Verbinden>>. Mit dieser Funktion versucht der SDA-Client die Verbindung nach einem Verbindungsabbruch automatisch wiederherzustellen.

© 2021 ise Individuelle Software und Elektronik GmbH

6. Klicken Sie auf <<Verbinden>>, nachdem Sie alle gewünschten Einstellungen definiert haben.

   Bei einer aktiven Verbindung können Sie die Kommunikationsgeschwindigkeit messen  . Das heißt, gemessen wird die Zeit ab Versenden einer Anfrage in das Zielnetzwerk des SMART CONNECT KNX Remote Access bis zum Erhalt einer Antwort vom SMART CONNECT KNX Remote Access.

   Detaillierte Verbindungsinformationen entnehmen Sie dem Logbuch  .

   Eine aktive Verbindung trennen Sie über die Schaltfläche <<Trennen>> oder, indem Sie den SDA-Client schließen.

2.5.4 Fernzugriffsoptionen des SDA-Clients

Fernzugriff über KNX/IP

Beim Fernzugriff über KNX/IP erscheinen im Connection Manager der ETS alle im entfernten Netzwerk gefundenen KNX/TP Tunneling Server sowie KNX/IP-Geräte.

Um Verwechslungen mit anderen Geräten im eigenen Netzwerk zu vermeiden, kennzeichnen Sie gefundene KNX/IP-Geräte mit einem Präfix, z. B. SDA-.

Fernzugriff über TCP

Wenn Sie beispielsweise per Remotedesktop auf einen PC zugreifen möchten, gehen Sie auf das Zahnrad und geben die IP oder DNS des Zielrechners im entfernten Netzwerk ein. Es ist sehr wahrscheinlich, dass der TCP Port im entfernten Netzwerk (Standard-Port RDP 3389) auf Ihrem PC bereits belegt ist. In diesem Fall müssen Sie einen anderen freien, lokalen TCP Port als den Standard-Port RDP verwenden. Empfohlen sind Ports ab 40000.

Wenn Sie für den lokalen TCP Port einen anderen als den Standard-Port RDP gewählt haben, ist die Eingabe für die Remotedesktopverbindung wie folgt:

Beispiel: 127.0.0.1:40000

© 2021 ise Individuelle Software und Elektronik GmbH

Fernkonfiguration Gira HomeServer

Für den Fernzugriff auf den Gira HomeServer ist entweder die IP-Adresse des HomeServers oder der lokale DNS-Name des HomeServers im entfernten Netzwerk einzugeben.

Für den Gira Experten können Sie die vorgegebenen Standardwerte verwenden. Wenn Sie die Angabe des Ports allerdings ändern möchten, klicken Sie auf das Zahnrad. Ports kleiner 1023 sind in der Regel vergeben und zur Nutzung nicht empfohlen.

Gira HomeServer ab Version 4.7.0 verwenden Port 443.

Sobald die Verbindung über das SDA-Portal hergestellt wurde, können Sie das Projekt auf den HomeServer übertragen. Starten Sie dafür den Gira Experten und wählen Sie im Dialog <<Projekt übertragen>> die Option <<Andere Adresse>>. Geben Sie die IP-Adresse 127.0.0.1 sowie den konfigurierten Port ein.

Beim Eiblib/IP-Protokoll können Sie die vorgegebenen Standardwerte verwenden.

In der ETS legen Sie eine Verbindung vom Typ <<Eiblib/IP>> an und vergeben als Server-Adresse die 127.0.0.1 sowie die konfigurierten lokalen Ports.

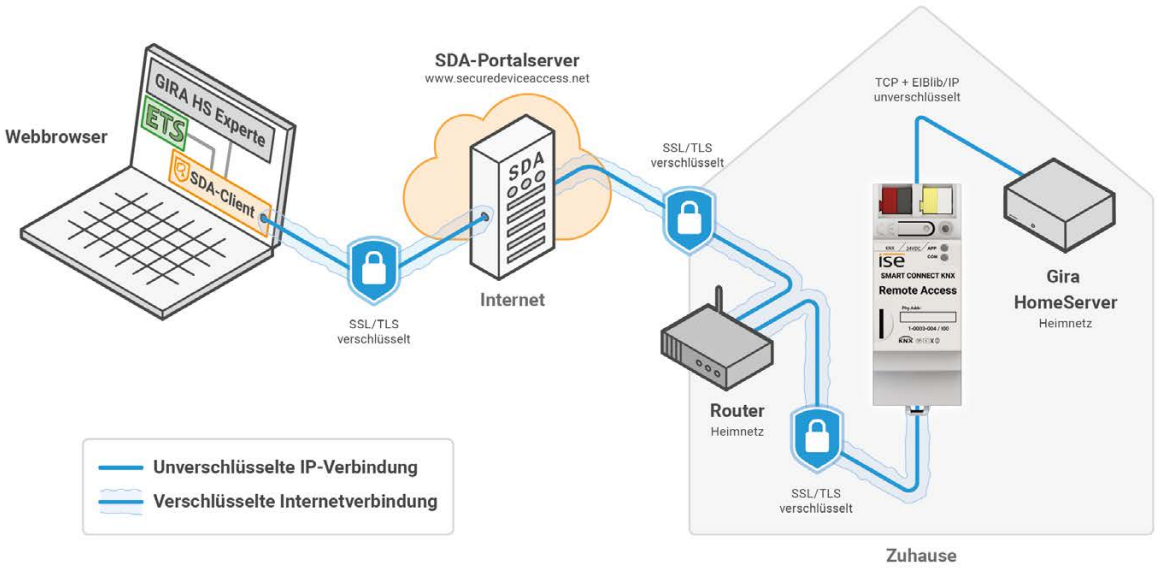


Abbildung 9: Sichere Konfiguration des Gira HomeServers mit Secure Device Access

© 2021 ise Individuelle Software und Elektronik GmbH

3 Wichtige Hinweise

3.1 Allgemeine Sicherheitshinweise

Warnung

Gefahr durch unsachgemäße Verwendung

Bei unsachgemäßer Verwendung können Schäden am Gerät, Brand oder andere Gefahren entstehen.

- Einbau und Montage elektrischer Geräte nur durch Elektrofachkräfte.
- Beachten Sie die Anleitungen in diesem Produkthandbuch.
- Dieses Produkthandbuch ist Bestandteil des Produkts und muss beim Kunden verbleiben.

3.2 Lagerung und Transport

Lagern Sie das Gerät in der Originalverpackung. Die Originalverpackung bietet beim Transport den optimalen Schutz. Lagern Sie das Gerät im Temperaturbereich von -25 °C bis +70 °C.

3.3 Reinigung und Wartung

Der SMART CONNECT KNX Remote Access ist wartungsfrei.

Reinigen Sie das Gerät bei Bedarf mit einem trockenen Tuch.

Achtung

Geräteschaden durch unsachgemäße Öffnung

- Öffnen Sie niemals das Gehäuse.
- Sollten Sie den Verdacht eines Geräteschadens haben, kontaktieren Sie unseren Support.
- Wir leisten Gewähr im Rahmen der gesetzlichen Bestimmungen.
- Bitte schicken Sie das Gerät nur nach Aufforderung durch unseren Support, portofrei mit einer aussagekräftigen Fehlerbeschreibung an uns zurück.

© 2021 ise Individuelle Software und Elektronik GmbH

4 Technische Daten

Spannungsversorgung und Anschlüsse	
Nennspannung:	DC 24 bis 30 V Versorgung über externe DC
Leistungsaufnahme:	2 W
Anschlüsse:	• KNX: Busanschlussklemme (schwarz/rot) • Externe Spannungsversorgung: Spannungsversorgungsklemme (weiß/gelb) • IP: 2x RJ45 (integrierter Switch)
microSD-Kartenslot	microSD-Karten bis 32 GB (SDHC)

Umgebungsbedingungen	
Temperatur Einbauumgebung	0 °C bis +45 °C

Geräteabmessungen	
Einbaubreite:	36 mm (2 TE)
Einbauhöhe:	90 mm
Einbautiefe:	74 mm (REG Plus)

KNX	
Kommunikation:	• KNX: KNX/TP • IP: Ethernet 10/100 BaseT (10/100 MBit/s)
Installationsmethode:	S-Mode

Zulassungen und Schutzart	
Zulassungen / Zertifizierungen:	CE, KNX
Schutzart:	IP20 (nach EN 60529)
Schutzklasse:	III (nach IEC 61140)

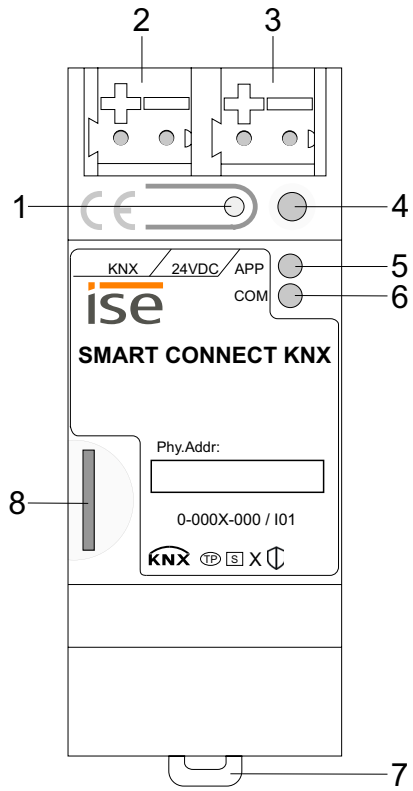
Unterstützte Webbrowser
Aktuelle Versionen von Mozilla Firefox, Microsoft Edge, Apple Safari und Google Chrome.

© 2021 ise Individuelle Software und Elektronik GmbH

5 Geräteaufbau

Bei Richtungsangaben gehen wir immer vom Gerät in Einbaulage aus.

5.1 Vorderseite

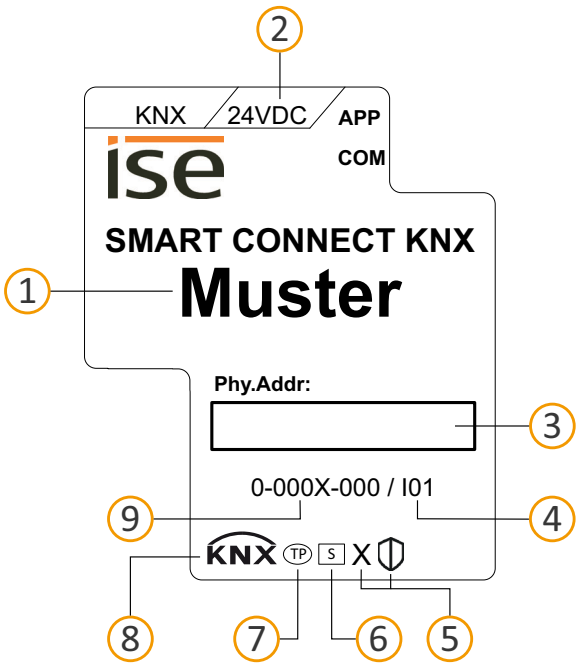


Nr.	Beschreibung	
1	Taste:	Programmiertaste
2	Anschluss:	KNX/TP
3	Anschluss:	Externe Spannungsversorgung
4	LED:	„Programmierung“ (rot)
5	LED:	„APP“: Betriebsanzeige (grün)
6	LED:	„COM“: Kommunikation KNX/TP (gelb)
7	Haltevorrich-tung:	Lösehebel der Hutschienen-klemme
8	Anschluss:	microSD-Kartenslot Verwendung von microSD-Karten bis 32 GB (SDHC)

Abbildung 10: Vorderseite

© 2021 ise Individuelle Software und Elektronik GmbH

5.2 Daten auf Geräteaufkleber

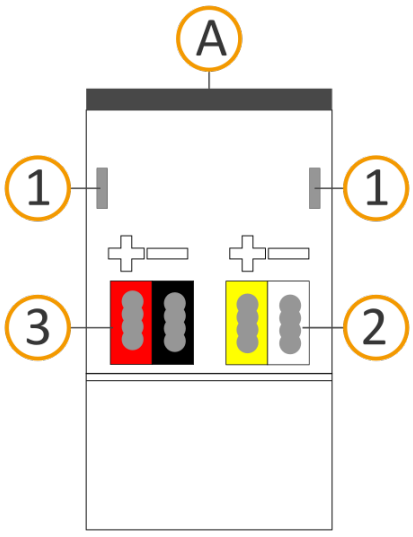


Nr.	Beschreibung
1	Produktname
2	Nennspannung
3	Physikalische Adresse: Tragen Sie in das Feld die zugeordnete physikalische Adresse mit einem abriebfesten Marker ein.
4	Index
5	KNX Secure
6	Installationsmethode, hier „S-Mode“
7	Übertragungsmedium, hier „TP“
8	KNX Zertifizierung
9	Bestellnummer

Abbildung 11: Geräteaufkleber

5.3 Oberseite

Auf der Geräteoberseite befinden sich die Öffnungen zur Befestigung der Abdeckkappe.

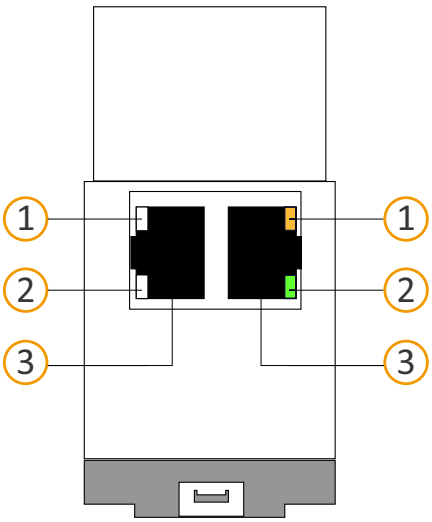


Nr. / Index	Beschreibung
1	Öffnung zur Befestigung der Abdeckkappe
2	Aufgesteckte Spannungsanschlussklemme
3	Aufgesteckte Busanschlussklemme
A	Geräterückseite

Abbildung 12: Geräteoberseite

© 2021 ise Individuelle Software und Elektronik GmbH

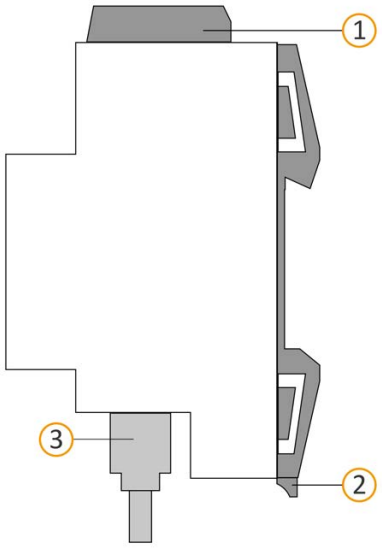
5.4 Unterseite



Nr.	Beschreibung
1	LED „Kommunikation“
2	LED „Verbindungsgeschwindigkeit“
3	IP: 2x RJ45 (integrierter Switch)

Abbildung 13: Netzwerkanschlüsse

5.5 Geräteseite



Nr.	Beschreibung
1	Aufgesteckte Abdeckkappe
2	Lösehebel für Hutschienenklemme
3	RJ45-Kabel (nicht im Lieferumfang enthalten) an RJ45-Buchse angeschlossen.

Abbildung 14: Geräteseite

© 2021 ise Individuelle Software und Elektronik GmbH

6 Montage

6.1 Lieferumfang

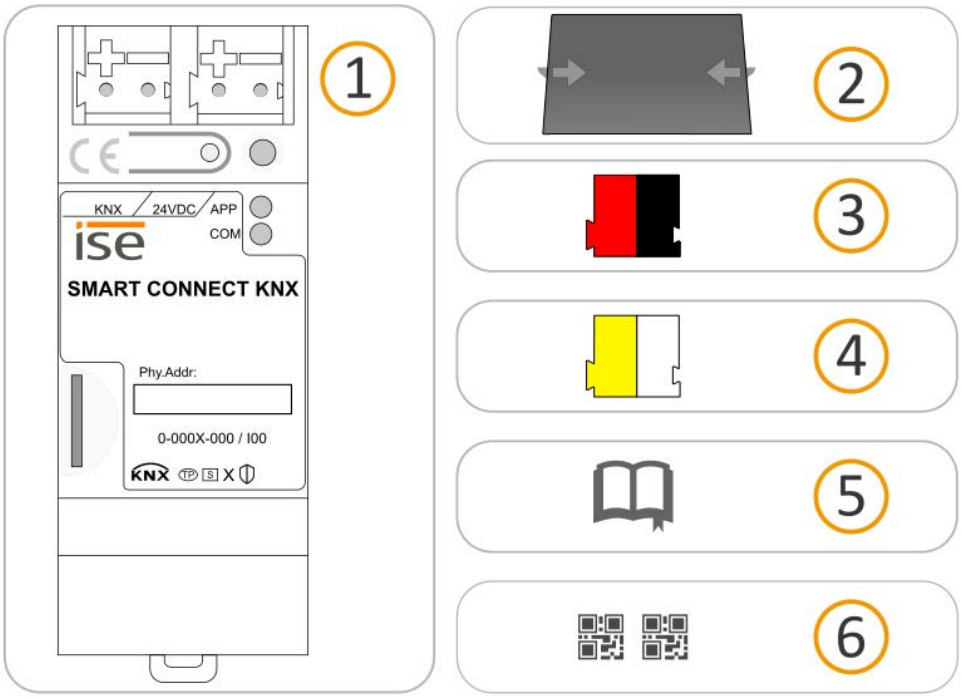


Abbildung 15: Lieferumfang

Nr.	Liefergegenstände	Erklärung
1	Gerät	SMART CONNECT KNX Remote Access
2	Abdeckkappe	Zum Schutz der Anschlüsse vor gefährlichen Spannungen.
3	Busanschlussklemme	Zum Anschluss der KNX/TP-Busleitungen.
4	Spannungsanschlussklemme	Zum Anschluss der externen Spannungsversorgung.
5	Installationsanleitung	Das vorliegende Produkthandbuch bietet Ihnen auch die Informationen der Installationsanleitung, jedoch mit zusätzlichen Details, Anwendungsbeispielen und Hinweisen zur Projektierung.
6	Aufkleber-Satz	Zusätzlicher Satz Aufkleber mit Daten für KNX Secure, Initial Device Passwort und Registration ID. Die gleichen Aufkleber sind auch auf der Geräteseite angebracht.

Die Installationsanleitung ist Bestandteil des Produkts.
Händigen Sie diese Anleitung Ihrem Kunden aus.

© 2021 ise Individuelle Software und Elektronik GmbH

6.2 Einbaubedingungen prüfen

Bevor Sie mit der Montage beginnen, prüfen Sie, ob die Voraussetzungen für die geplante Einbauumgebung erfüllt sind.

Achtung

Funktionsstörung des Geräts durch falsche Umgebungstemperatur in der Einbauumgebung

- Beachten Sie die Temperatur der Einbauumgebung: Mind. 0 °C bis max. +45 °C.
- Montieren Sie den SMART CONNECT KNX Remote Access nicht oberhalb von Wärme abgebenden Geräten.
- Sorgen Sie für ausreichende Lüftung/Kühlung.

Beachten Sie die Gerätetiefe (siehe Abbildung 16, Pos.1): REG-Plus, 74 mm.

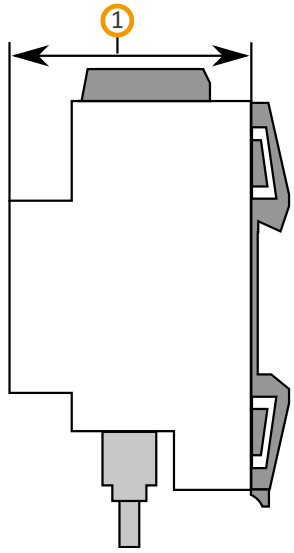


Abbildung 16: Gerätetiefe

© 2021 ise Individuelle Software und Elektronik GmbH

6.3 Gerät montieren

Der SMART CONNECT KNX Remote Access darf ausschließlich von Elektrofachkräften montiert und installiert werden.
Fachkenntnisse zu Installationsvorschriften werden vorausgesetzt.

Warnung

Gefahr durch unsachgemäße Verwendung

Bei unsachgemäßer Verwendung können Schäden am Gerät, Brand oder andere Gefahren entstehen.

- Einbau und Montage elektrischer Geräte nur durch Elektrofachkräfte.
- Beachten Sie die Anleitungen in diesem Produkthandbuch.
- Dieses Produkthandbuch ist Bestandteil des Produkts und muss beim Kunden verbleiben.

Warnung

Gefahr durch elektrischen Schlag

Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung.
Elektrischer Schlag kann zum Tod führen.
Beachten Sie die Installationsvorschriften:

- Führen Sie die KNX/TP-Busleitung mit intaktem Mantel bis nahe an die Busanschlussklemme.
- Schieben Sie die KNX/TP-Busleitung mit Druck bis zum Anschlag in die Busanschlussklemme.
- Installieren Sie Busleitungsadern ohne Mantel (SELV) sicher getrennt von allen Nicht-Schutzkleinspannungsleitungen (PELV/FELV).
- Halten Sie den vorgeschriebenen Abstand ein.
- Stecken Sie die mitgelieferte Abdeckkappe auf.
- Weitere Informationen siehe auch VDE-Bestimmungen zu SELV (DIN VDE 0100-410/ „Sichere Trennung“, KNX Installationsvorschriften).

© 2021 ise Individuelle Software und Elektronik GmbH

Gerät montieren und anschließen

1. Lassen Sie das Gerät auf der Hutschiene vertikal aufschnappen (Einbaulage: Netzwerkanschlüsse unten).

2. Verbinden Sie die KNX/TP-Busleitung (nachfolgend Busleitung genannt) mit dem KNX Anschluss des Geräts (siehe Abbildung 17, Pos. 1) mittels beigefügter Busanschlussklemme (siehe Abbildung 17, Pos. 2). Polung: links/rot: „+“, rechts/schwarz „-“.

   a. Stecken Sie die Busanschlussklemme (siehe Abbildung 17, Pos. 2) auf.

   b. Führen Sie die Busleitung mit intaktem Mantel bis nahe an die Busanschlussklemme.

   c. Schieben Sie die Busleitung mit Druck bis zum Anschlag in die Busanschlussklemme.

   d. Führen Sie die Busleitung nach hinten.

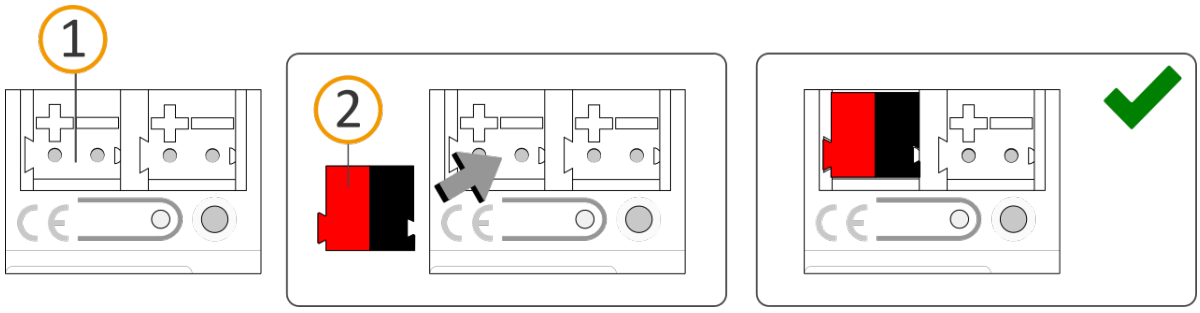


Abbildung 17: Busleitung anschließen

3. Verbinden Sie die externe Spannungsversorgung mit dem Spannungsversorgungsanschluss (siehe Abbildung 18, Pos. 1) mittels beigefügter Spannungsanschlussklemme (siehe Abbildung 18, Pos. 2). Polung: links/gelb: „+“, rechts/weiß: „-“.

   a. Stecken Sie die Spannungsanschlussklemme (siehe Abbildung 18, Pos. 2) auf.

   b. Führen Sie die Spannungsleitung mit intaktem Mantel bis nahe an die Spannungsanschlussklemme.

   c. Schieben Sie die Spannungsleitung mit Druck bis zum Anschlag in die Spannungsanschlussklemme.

   d. Führen Sie die Spannungsversorgungsleitung nach hinten.

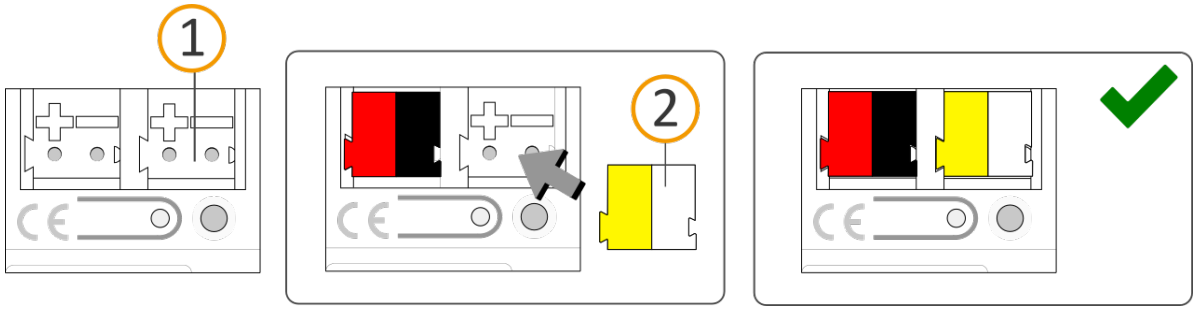


Abbildung 18: Spannungsversorgung anschließen

© 2021 ise Individuelle Software und Elektronik GmbH

Achtung

Funktionsstörung aller Geräte einer Linie durch falsch dimensionierte Spannungsversorgung

Wenn Sie als zusätzliche Spannungsversorgung den unverdrosselten Hilfsspannungsausgang einer KNX Spannungsversorgung nutzen, gilt:
Die Betriebsströme aller KNX/TP-Geräte am Liniensegment dürfen nicht den Bemessungsstrom der Spannungsversorgung überschreiten.

4. Stecken Sie die Abdeckkappe auf:

   a. Führen Sie alle Kabel nach hinten. Die Öffnungen zur Befestigung der Abdeckkappe (siehe Abbildung 19, Pos. 1) müssen frei sein. Alle Kabel müssen sich zwischen den Öffnungen befinden.

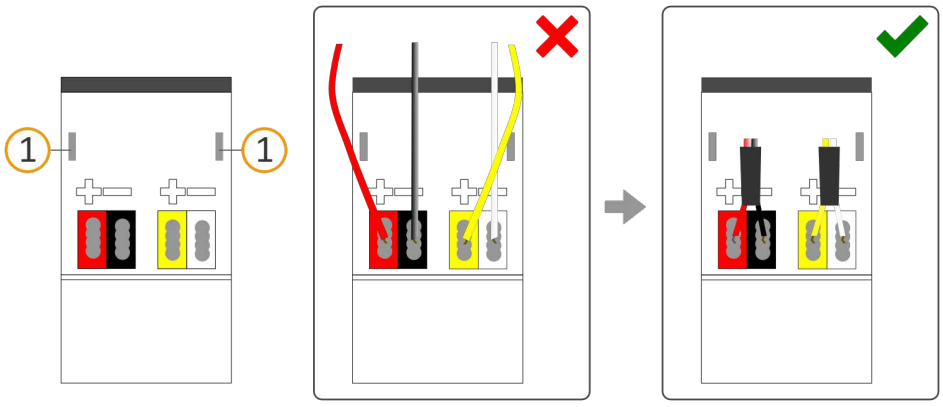


Abbildung 19: Kabelführung

   b. Stecken Sie die Abdeckkappe über die Anschlussklemmen.

   c. Drücken Sie die Abdeckkappe leicht zusammen.

   d. Führen Sie die Befestigungskrallen der Abdeckkappe in die Öffnungen, bis die Abdeckkappe spürbar einrastet.

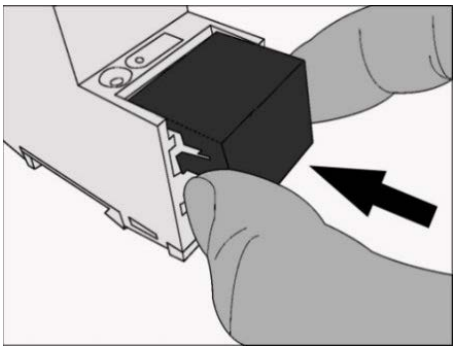


Abbildung 20: Abdeckkappe aufstecken

© 2021 ise Individuelle Software und Elektronik GmbH

5. Netzwerk anschließen:

   a. Stellen Sie sicher, dass Ihre Netzwerkinfrastruktur (Router, DNS-Server) in Betrieb ist.

   b. Die Netzwerkanschlüsse befinden sich auf der Geräteunterseite.

   c. Verbinden Sie die IP-Netzwerkleitung (RJ45-Kabel) mit dem Netzwerkanschluss des Geräts (RJ45-Buchse).

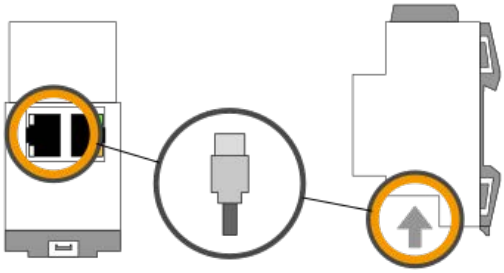


Abbildung 21: IP-Netzwerkleitung anschließen

© 2021 ise Individuelle Software und Elektronik GmbH

7 Gerätewebseite

Über die Applikation „Gerätewebseite“ können Sie auf den SMART CONNECT KNX Remote Access zugreifen.

Die Gerätewebseite bietet u. a. die folgenden Funktionen:

- Gerätestatus prüfen ▶ siehe Fehlersuche, S. 77.
- Netzwerkeinstellungen konfigurieren ▶ siehe Netzwerkeinstellungen über die Gerätewebseite vornehmen, S. 43.
- Firmware aktualisieren ▶ siehe Firmware über die Gerätewebseite aktualisieren, S. 45.
- Auf Werkseinstellungen zurücksetzen ▶ siehe Gerät über die Gerätewebseite auf Werkseinstellungen zurücksetzen, S. 45.
- Logdateien generieren ▶ siehe Logdateien generieren, S. 78.

Die Gerätewebseite wird in Ihrem installierten Browser ausgeführt. Sie benötigen keine zusätzliche Software.

Auf die Gerätewebseite können Sie zugreifen, sobald das Gerät über IP im Netzwerk verfügbar ist.

7.1 Gerätewebseite: Startseite aufrufen

Rufen Sie die Gerätewebseite über einen der nachfolgenden Wege auf:

- Geben Sie die IP-Adresse des Geräts in die Adresszeile Ihres Browsers ein.
- Bei der Nutzung von Microsoft Windows wählen Sie alternativ das Gerät in der Netzwerkumgebung in der Kategorie <<Andere Geräte>> (siehe Abbildung 22, Pos. 1): Doppelklicken Sie auf das Icon des Geräts (siehe Abbildung 22, Pos. 2).

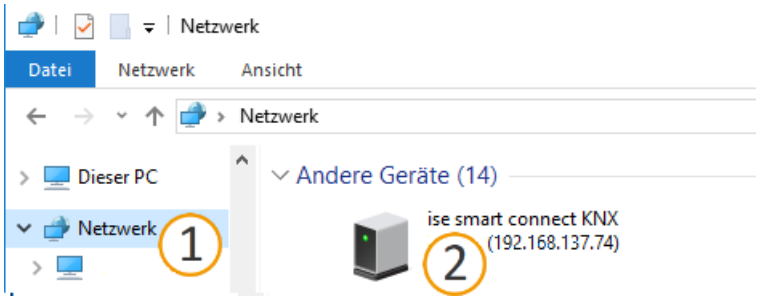


Abbildung 22: Aufruf der Gerätewebseite über Netzwerkumgebung

Die Gerätewebseite ist passwortgeschützt. Als Initialpasswort auch nach einem Werksreset dient die Registration ID. Nach erfolgreicher Anmeldung können Sie das Passwort unter <<Benutzer>> ändern.

© 2021 ise Individuelle Software und Elektronik GmbH

7.2 Oberfläche der Gerätewebseite kennenlernen

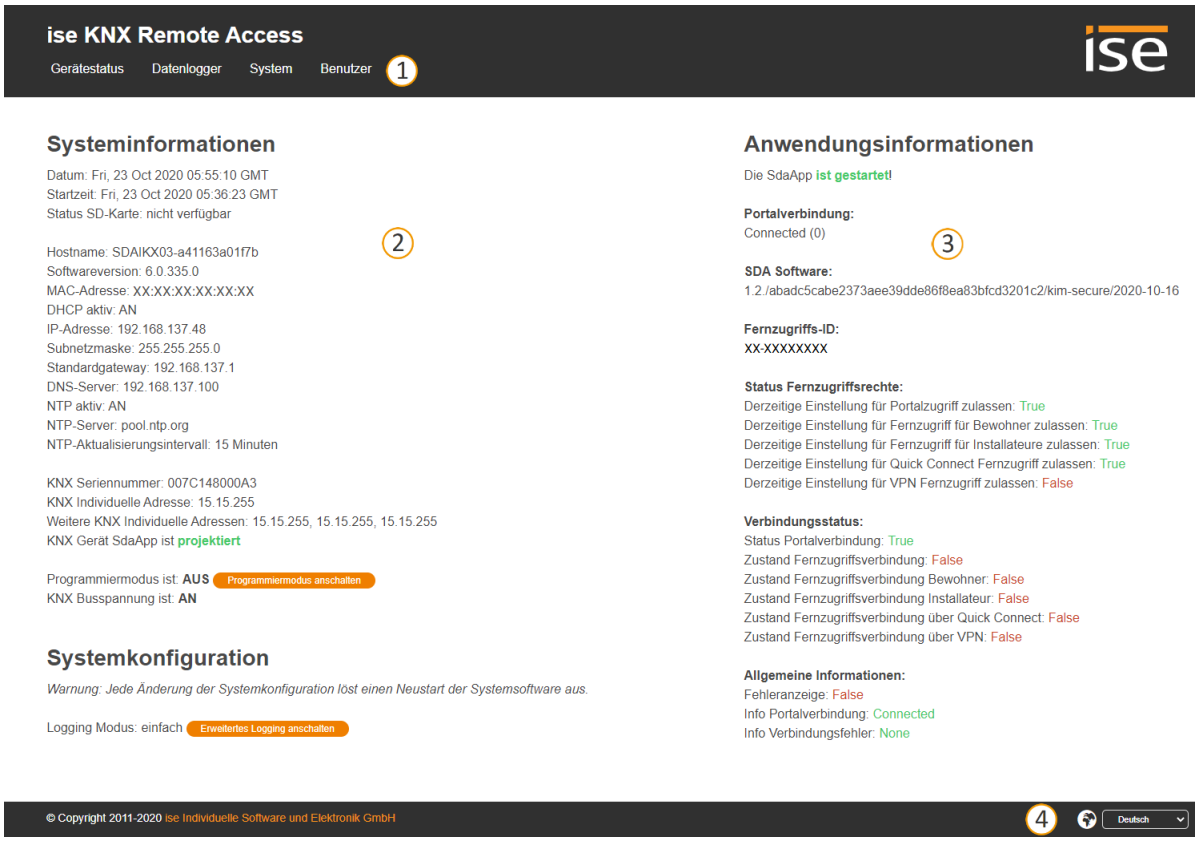


Abbildung 23: Startseite der Gerätewebseite

Pos.	Element	Funktion
1	Menüleiste	Weitere Seiten aufrufen oder Funktionen ausführen.
2	Seite	Abgebildet ist die Seite <<Gerätestatus>>.
3	Informationen	Darstellung spezifischer Informationen.
4	Statusleiste	Sprache wechseln.

© 2021 ise Individuelle Software und Elektronik GmbH

Menü	Beschreibung
Gerätestatus	Informationen: • Systeminformationen • Systemkonfiguration • Anwendungsinformationen Funktionen: • ▶ Logging-Modus umstellen, S. 78 • Gerät in Programmiermodus schalten
Datenlogger	Zugriff auf das Datenlogger-Archiv
System	Funktionen: • ▶ Netzwerkeinstellungen konfigurieren, S. 43 • ▶ Logdateien generieren, S. 78 • Gerät neu starten • ▶ Auf Werkseinstellungen zurücksetzen, S. 43 • ▶ Firmware aktualisieren, S. 45 Informationen: • Haftungshinweis • Lizenzen
Benutzer	• Passwort ändern • Abmelden von der Gerätewebseite

Tabelle 4: Überblick

Nach einem Neustart des SMART CONNECT KNX Remote Access kann der Verbindungsstatus mit dem SDA-Portalserver für einen kurzen Moment falsche Werte anzeigen.
Die Webseite wird nicht automatisch aktualisiert. Verwenden Sie hierfür die entsprechende Funktion Ihres Browsers.

© 2021 ise Individuelle Software und Elektronik GmbH

8 Inbetriebnahme und Projektierung

Nach der Montage des Geräts und dem Anschluss von Bus, Spannungsversorgung und Netzwerk können Sie das Gerät in Betrieb nehmen.

8.1 Schnelleinstieg

Wenn Sie mit KNX und der Installation von KNX Gateways bereits vertraut sind, können Sie diesen Schnelleinstieg zum erstmaligen Einrichten des SMART CONNECT KNX Remote Access nutzen.

Im SDA-Portal anmelden

1. Im SDA-Portal https://securedeviceaccess.net registrieren.
2. <<SDA-Connector hinzufügen>> anklicken.
3. Registration ID (siehe beiliegenden Aufkleber) eingeben.
4. Namen und Beschreibung zur einfacheren Identifizierung vergeben.

SDA-Client herunterladen

Nicht im selben Netzwerk wie der SMART CONNECT KNX Remote Access?
SDA-Client nutzen:

5. Produktseite aufrufen und zum Downloadbereich scrollen.
6. Passenden SDA-Client für Windows (x86) oder (x64) herunterladen.
7. Installationsdatei auf dem gleichen Rechner wie die ETS ausführen.

Gerät über SDA-Client verbinden

8. SDA-Client über Windows Startmenü starten.
9. Mit den gleichen Benutzerdaten wie im SDA-Portal anmelden.
10. In der Auswahlliste den SMART CONNECT KNX Remote Access auswählen und verbinden.

Gerät in ETS einbinden

11. In der ETS den Reiter <<Bus>> anklicken.
12. Physikalische Adresse eingeben. Physikalische Adresse im Auslieferungszustand: 15.15.255.
13. Eingabe testen, indem Sie <<Test>> anklicken.

© 2021 ise Individuelle Software und Elektronik GmbH

8.2 Gerätestatus anhand der LEDs ablesen

Auf der Vorderseite finden Sie die folgenden Statusindikatoren (LEDs).

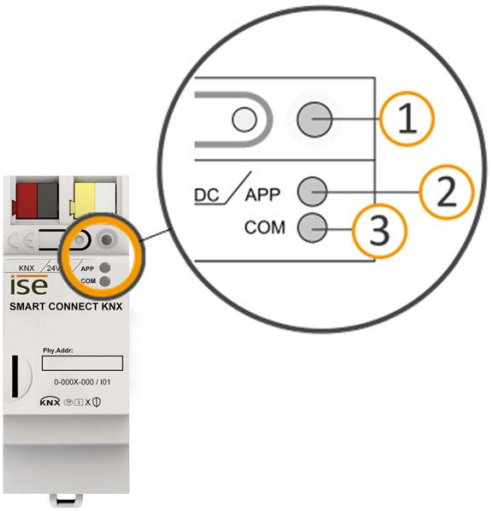


Abbildung 24: Statusindikatoren (LEDs) auf der Vorderseite des Geräts

Nr.	Element	Beschreibung
1	LED „Programmierung“ (rot)	Anzeige Programmiermodus aktiv/inaktiv
2	LED „APP“ (grün)	Anzeige als Statusindikator der Anwendung
3	LED „COM“ (gelb)	Anzeige Kommunikationsverkehr von KNX/TP

Tabelle 5: Statusindikatoren

Die LED „Programmierung“ zeigt unabhängig vom Betriebsmodus an, ob das Gerät im Programmiermodus ist.

Farbe	Beschreibung
● (rot, dauerhaft an)	Programmiermodus ist aktiv. ► Physikalische Adresse zuordnen, S. 41
○ (aus)	Programmiermodus ist deaktiviert.

Tabelle 6: Status des Geräts – Programmiermodus

© 2021 ise Individuelle Software und Elektronik GmbH

Auf der Geräteunterseite finden Sie die Statusindikatoren für das Netzwerk.

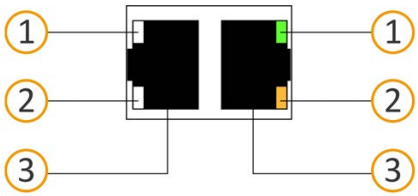


Abbildung 25: Netzwerk LEDs

Nr.	Element	Beschreibung
1	LED „Verbindungsgeschwindigkeit“	• LED leuchtet grün: 100 MBit/s • LED ist aus: 10 MBit/s (Falls LED 2 auch aus ist, besteht keine Verbindung. Prüfen Sie dann, ob das Kabel korrekt angeschlossen ist.)
2	LED „Kommunikation“	• LED leuchtet gelb-orange: Verbunden, aber aktuell kein Telegrammverkehr • LED blinkt gelb-orange: Telegrammverkehr
3	IP-Anschluss	2x RJ45 (integrierter Switch)

Tabelle 7: Status des Geräts – Netzwerk

© 2021 ise Individuelle Software und Elektronik GmbH

8.2.1 LEDs beim Gerätestart

Die LEDs „APP“ und „COM“ haben unterschiedliche Bedeutungen je nach Phase im Betriebsmodus. Nach Einschalten der Spannungsversorgung oder nach Spannungsrückkehr zeigt das Gerät den Status mit folgenden LED-Kombinationen:

APP	COM	Beschreibung
Ordnungsgemäßer Betrieb		
○ (aus)	● (gelb)	Gerät startet.
● (grün)	● (gelb)	Gerät funktionsbereit hochgefahren.
Fehler		
○ (aus)	○ (aus)	Keine Spannungsversorgung. • Prüfen Sie die Anschlüsse und die Spannungsversorgung.
○ ... ● ... ○ ... ● ... (aus)...(grün)...(aus)...(grün)... Langsames Blinken (ca. 1 Hz)	● (gelb)	Das Gerät ist komplett hochgefahren, aber noch nicht konfiguriert. Das System wird im S-Mode konfiguriert. • Konfigurieren Sie das Gerät in der ETS.
○ ... ● ... ○ ... ● ... (aus)...(grün)...(aus)...(grün)... Langsames Blinken (ca. 1 Hz)	○ (aus)	Das Gerät ist komplett hochgefahren, aber noch nicht konfiguriert. Das System wird im S-Mode konfiguriert. • Konfigurieren Sie das Gerät in der ETS. Verbindung zu KNX ist unterbrochen. • Prüfen Sie, ob die Anschlüsse KNX und Spannung vertauscht sind. • Prüfen Sie die Busverbindung. • Prüfen Sie, ob die Spannungsversorgung korrekt angeschlossen ist.
○ . ● . ○ . ● . ○ . ● (aus).(grün).(aus).(grün).(aus).(grün) Schnelles Blinken	○ (aus)	Die Firmware kann nicht gestartet werden. • Kontaktieren Sie den Support.
○ ... ● ... ○ ... ● ... ● ... ○ ... ● ...○ ... (aus)...(grün)...(aus)...(grün)... (gelb)...(aus)...(gelb)...(aus)... Langsames Blinken (ca. 1 Hz) im Wechsel		Die neu geladene Firmware kann nicht gestartet werden. Das System versucht, die bisherige Firmware zu aktivieren (ungültige Firmware). • Kontaktieren Sie den Support.

Tabelle 8: Status des Geräts – Gerät startet

© 2021 ise Individuelle Software und Elektronik GmbH

8.2.2 LEDs im Betrieb

LED-Status nach abgeschlossenem Gerätestart:

APP	Beschreibung
● (grün)	Das Gerät funktioniert einwandfrei (Normalbetrieb). Der Portalzugriff ist generell erlaubt (Kommunikationsobjekt 1). Das Gerät verbindet sich mit dem SDA-Portalserver, jedoch ist derzeit der Fernzugriff nicht aktiv. Weiterleitungen sind möglich.
○ (aus)	Das Gerät startet gerade oder ist außer Betrieb. • Warten Sie, bis der Gerätestart abgeschlossen ist. • Falls das Gerät immer noch außer Betrieb ist, prüfen Sie die Anschlüsse und die Spannungsversorgung.
● … ○ Einmal langsames Blinken (ca. 1 Hz), dann 2 s Pause	Der Portalzugriff wurde über Kommunikationsobjekt 1 deaktiviert. Das Gerät verbindet sich nicht mit dem SDA-Portalserver. Ein Fernzugriff ist technisch unmöglich.
● … ○ … ● … ○ … ● … ○ (grün).(aus).(grün).(aus).(grün).(aus) Dreimal langsames Blinken (ca. 1 Hz), dann 2 s Pause	Der Fernzugriff ist für mindestens eine Zugriffsgruppe bzw. Quick Connect erlaubt und es gibt mindestens eine aktive Verbindung.

Tabelle 9: LED „APP“ im Betrieb

COM	Beschreibung
● (gelb)	Die KNX Verbindung ist hergestellt. Kein KNX Telegrammverkehr. Die LED gilt auch als dauerhaft an, falls kurze unregelmäßige Unterbrechungen auftreten.
○ . ● . ○ . ● . ○ . ● (aus).(gelb).(aus).(gelb).(aus).(gelb) Schnelles Blinken	KNX Verbindung ist hergestellt. KNX Telegrammverkehr.
Fehler	
○ (aus)	Verbindung zu KNX ist unterbrochen. • Prüfen Sie, ob die Anschlüsse KNX und Spannung vertauscht sind. • Prüfen Sie die Busverbindung. • Prüfen Sie, ob die Spannungsversorgung korrekt angeschlossen ist.

Tabelle 10: LED „COM“ im Betrieb

© 2021 ise Individuelle Software und Elektronik GmbH

8.3 Projektierung

Projektiert wird das Gerät in der Software ETS (Engineering Tool Software). Die ETS ist in unterschiedlichem Funktionsumfang über die KNX Association (www.knx.org) erhältlich.

Alle Beschreibungen in dieser Dokumentation zur Projektierung in der ETS beziehen sich auf die Variante „ETS Professional“ in Version 5.

Hilfe zur ETS erhalten Sie in der integrierten Online-Hilfe der ETS.

- Drücken Sie die Taste [F1].

Hinweis:
Der SMART CONNECT KNX Remote Access ist im Auslieferungszustand bzw. nach einem Werksreset folgendermaßen konfiguriert:

- Der Fernzugriff ist für die Zugriffsgruppen Bewohner und Installateur sowie für Quick Connect aktiviert.
- Die physikalische Adresse für das Gerät ist 15.15.255. Die drei weiteren physikalischen Schnittstellen (Tunneling Server) haben die 15.15.254.

Arbeitsschritte

1. Legen Sie den SMART CONNECT KNX Remote Access als Gerät in der ETS an, ► siehe Gerät in der ETS anlegen, S. 38.
2. Ordnen Sie dem Gerät in der ETS die physikalische Adresse sowie die bis zu drei physikalischen Adressen des Interfaces gemäß der KNX Topologie zu.
3. Wählen Sie die Option <<IP-Adresse automatisch beziehen>> oder wählen Sie <<Feste IP-Adresse verwenden>> und füllen die folgenden Felder aus: IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse, ► siehe IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse einstellen, S. 40.
4. Stellen Sie die allgemeinen Parameter ein, ► siehe Parameter konfigurieren, S. 51.
5. Verknüpfen Sie die Gruppenadressen mit den Kommunikationsobjekten.
6. Der SMART CONNECT KNX Remote Access ist nun bereit zur Inbetriebnahme mittels <<ETS Programmieren>> und zum Test der Funktionen.

Hinweis:

Wegen deutlich kürzerer Übertragungszeiten empfehlen wird den Download über die IP-Direktverbindung. Wählen Sie auf der ETS-Startseite den Reiter <<Bus>>→ <<Verbindungen>> →<<Optionen>> →<<Direkte IP-Verbindung verwenden, wenn verfügbar>>.

© 2021 ise Individuelle Software und Elektronik GmbH

8.3.1 Gerät in der ETS anlegen

Abhängig davon, ob der Produktdatenbankeintrag bereits im ETS-Katalog vorhanden ist oder das Gerät bereits in Ihrem bestehenden Projekt verwendet wird, sind unterschiedliche Arbeitsschritte erforderlich, um die aktuelle Version zu verwenden.

Arbeitsschritte	
Gerät bereits in ETS-Katalog vorhanden?	
Ja	Nein
Produktdatenbank aktualisieren. Beim Aktualisieren wird der alte Produktdatenbankeintrag durch den neuen Produktdatenbankeintrag ersetzt.	Produktdatenbankeintrag importieren. Um einen neuen Produktdatenbankeintrag zu importieren, gibt es zahlreiche Möglichkeiten. Nachfolgend gehen wir davon aus, dass Sie sich den Produktdatenbankeintrag selbst heruntergeladen haben. ► siehe Neuen Produktdatenbankeintrag importieren, S. 38.
Gerät in bestehendem Projekt soll aktualisiert werden?	
Ja	Nein
Damit die bestehenden Verknüpfungen mit Gruppenadressen erhalten bleiben, müssen Sie das Gerät auf die korrekte Weise aktualisieren. ► siehe Produkt in bestehendem Projekt aktualisieren, S. 39.	Fügen Sie wie gewohnt das Gerät Ihrer Topologie hinzu.

Tabelle 11: Arbeitsschritte - Gerät in der ETS anlegen

Neuen Produktdatenbankeintrag importieren

Voraussetzung: Sie haben den Produktdatenbankeintrag (Produktdatei) von unserer Webseite unter www.ise.de heruntergeladen.

1. Starten Sie die ETS und wählen Sie auf der Startseite den Reiter <<Kataloge>>.
2. Wählen Sie in der Werkzeugleiste die Schaltfläche <<Importieren>>.
3. Wählen Sie im Fenster <<Produktdatei öffnen>> die Produktdatei und bestätigen die Auswahl mit der Schaltfläche <<Öffnen>>.
4. Folgen Sie den weiteren Anweisungen in der ETS. Rufen Sie bei Bedarf die Online-Hilfe mit der Taste [F1] auf.

© 2021 ise Individuelle Software und Elektronik GmbH

Produkt in bestehendem Projekt aktualisieren

Voraussetzung: Neuer Produktdatenbankeintrag des Geräts ist im Katalog vorhanden.

1. Öffnen Sie in der ETS das Projekt, in dem das Gerät aktualisiert werden soll.
2. Suchen Sie den neuen Produktdatenbankeintrag im Katalog und fügen Sie die neue Version des Geräts zu den Geräten Ihres Projekts hinzu.
3. Wählen Sie die alte Version des Geräts in Ihrer Topologie.
4. Wählen Sie im Bereich <<Eigenschaften>> den Reiter <<Informationen>> → <<Applikationsprogramm>>.
5. Wählen Sie die Schaltfläche <<Aktualisieren>> unterhalb des Punkts <<Applikationsprogramm-Version aktualisieren>> (siehe Abbildung 26, Pos. 2).

   Wenn Sie den Wert unter <<Applikationsporgramm ändern>> (siehe Abbildung 26, Pos. 1) ändern, gehen benutzerdefinierte Einstellungen wie z. B. die Verknüpfungen zu den Gruppenadressen verloren.

6. Wählen Sie das neu hinzugefügte Gerät und löschen es wieder aus Ihrer Topologie.

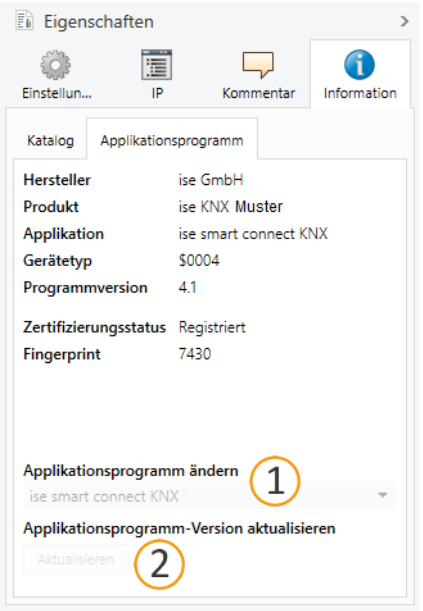


Abbildung 26: Applikationsprogramm aktualisieren

© 2021 ise Individuelle Software und Elektronik GmbH

8.3.2 IP-Einstellungen

Neben der physikalischen Adresse im KNX Netzwerk müssen dem SMART CONNECT KNX Remote Access eine IP-Adresse, die Subnetz-Maske und die Adresse des Standardgateways im IP-Datennetzwerk zugewiesen werden.

Die Einstellungen können Sie manuell in der ETS eingeben oder automatisiert beziehen (Bezug der Daten von einem DHCP-Server, z. B. im Router des Datennetzwerks integriert).

IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse einstellen

1. Wählen Sie in der ETS das Gerät in Ihrer Topologie aus.
2. Wählen Sie im Bereich <<Eigenschaften>> den Reiter <<IP>>.
3. Die zur Verfügung stehenden Auswahlmöglichkeiten finden Sie in Abbildung 27 und in der Tabelle 12 “Einstellungen zur manuellen IP-Adressen-Eingabe oder zum automatischen Bezug” auf S. 40.

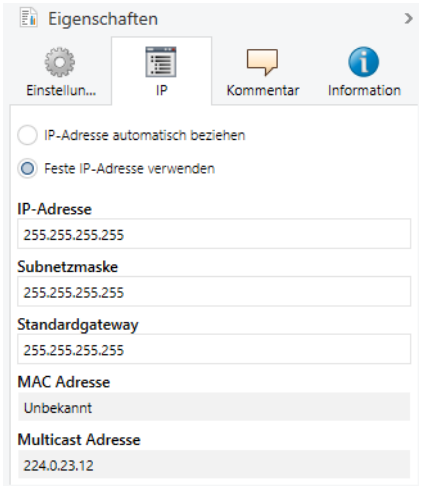


Abbildung 27: IP-Einstellungen

Einstellung	Beschreibung
IP-Adresse automatisch beziehen	Die Adressdaten werden automatisch von einem DHCP-Server im Datennetzwerk bezogen. Der DHCP-Server muss dem SMART CONNECT KNX Remote Access eine gültige IP-Adresse zuteilen. Ist kein DHCP-Server verfügbar, startet das Gerät nach einer Wartezeit mit einer AutoIP-Adresse im 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.
Feste IP-Adresse verwenden	Tragen Sie die Daten manuell ein. Den zulässigen IP-Adressbereich sowie die Subnetzmaske und das Standardgateway können Sie der Oberfläche der Routerkonfiguration entnehmen.

Tabelle 12: Einstellungen zur manuellen IP-Adressen-Eingabe oder zum automatischen Bezug

© 2021 ise Individuelle Software und Elektronik GmbH

Schwerwiegende Fehlkonfiguration

Wenn Sie die Einstellung <<Feste IP-Adresse verwenden>> gewählt haben und dann aber vergessen die entsprechenden Felder zu befüllen, werden Default-Werte gesetzt. Dies hat zur Folge, dass das Gerät nicht einwandfrei startet.
Setzen Sie das Gerät auf Werkseinstellungen zurück. ► Auf Werkseinstellungen zurücksetzen, S. 43.
Falls danach noch Probleme bestehen sollten, kontaktieren Sie den Support.

8.3.3 Physikalische Adresse programmieren

Die physikalische Adresse, die Sie in der ETS vergeben haben, muss dem Gerät zugeordnet werden. Wir sprechen dabei von „programmieren“. Dazu müssen Sie das Gerät in den Programmiermodus versetzen.

Physikalische Adresse zuordnen

Voraussetzungen: Gerät und Busspannung sind eingeschaltet. Programmier-LED ist aus.

1. Drücken Sie kurz die Programmiertaste (siehe Abbildung 28, Pos. 1). Alternativ können Sie die Programmiertaste auch über die Gerätewebseite betätigen. Die Programmier-LED (siehe Abbildung 28, Pos.2) leuchtet rot.

2. Ordnen Sie dem Gerät in der ETS die physikalische Adresse gemäß der KNX Topologie zu und führen Sie die Programmierung in der ETS durch.

3. Tragen Sie auf dem Gerät in das Feld <<Phy. Addr.>> die zugeordnete physikalische Adresse mit einem abriebfesten Marker ein.

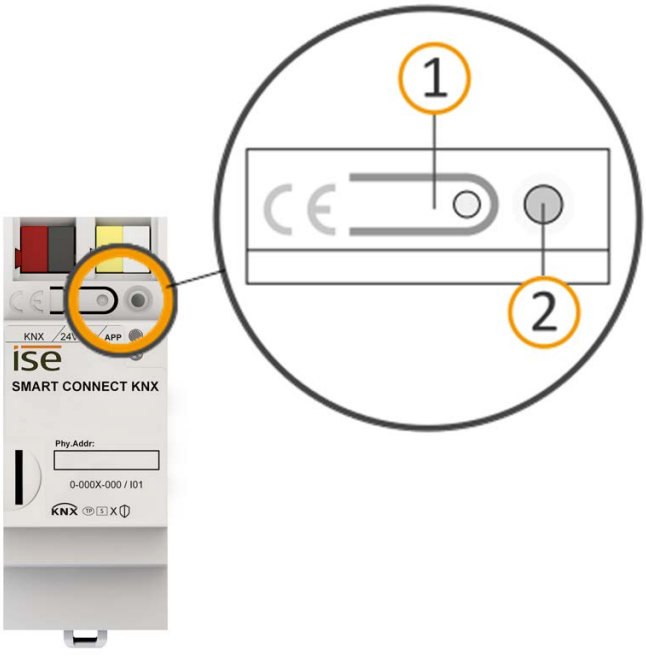


Abbildung 28: Programmierung

© 2021 ise Individuelle Software und Elektronik GmbH

Erfolgreiche Zuordnung der physikalischen Adresse erkennen:

- Gerät: Die Programmier-LED am Gerät ist aus.
- ETS: Auf dem Reiter <<Historie>> wird die abgeschlossene Übertragung mit grüner Markierung angezeigt. Programmieren-Flag <<Adr>> ist gesetzt und <<Cfg>> ist nicht gesetzt. Weitere Informationen zu diesen und weiteren Flags erhalten Sie in der ETS-Dokumentation.

Nachdem die IP-Adresse zugeordnet ist, können Sie das Gerät auch bequem über die Gerätewebseite in den Programmiermodus versetzen, anstatt direkt am Gerät die Programmiertaste zu drücken.

Tunneling Server

Der SMART CONNECT KNX Remote Access verfügt über drei Tunneling Server (KNX/IP-Interfaces). Diese Schnittstellen können für den Download sowie im Gruppen- und Busmonitor-Modus genutzt werden. Jedem Tunneling Server muss im Reiter <<Eigenschaften>> in der ETS eine physikalische Adresse zugeordnet werden. Sollten Sie nicht alle drei Schnittstellen benötigen, können Sie über <<Parken>> Adressen freigeben.

© 2021 ise Individuelle Software und Elektronik GmbH

8.3.4 Netzwerkeinstellungen über die Gerätewebseite vornehmen

Voraussetzung: Die Gerätewebseite ist geöffnet.

1. Wählen Sie in der Menüleiste <<System>> → <<Netzwerkeinstellungen>>. Die Seite Netzwerkeinstellungen wird angezeigt.

2. Tragen Sie z. B. in das Eingabefeld <<DNS-Server (optional)>> die IP-Adresse Ihres DNS-Servers ein.

3. Klicken Sie auf <<Speichern>> unterhalb des Eingabefeldes. Das System übernimmt die Konfiguration.

> Wenn Sie aus der ETS das Gerät programmieren oder <<Gerät zurücksetzen>> für das Gerät wählen, wird der DNS-Server auf das Standardgateway zurückgesetzt. Sie müssen dann den DNS-Server erneut auf der Gerätewebseite konfigurieren.

8.3.5 Auf Werkseinstellungen zurücksetzen

Wenn Sie das Gerät auf Werkseinstellungen zurücksetzen, verhält sich das Gerät wie im Auslieferungszustand. Das Gerät ist dann unprojektiert:

- Das Gerät verbleibt aber in den bestehenden Projekten.
- Die Registrierung des Geräts im SDA-Portal bleibt erhalten.
- Das Gerät behält die Version des Applikationsprogramms in der ETS.
- Die komplette Parametrierung wird verworfen.
- Die IP-Einstellungen werden zurückgesetzt.
- Das Passwort der Gerätewebseite wird auf das Initialpasswort zurückgesetzt.
- Als physikalische KNX Adresse hat das Gerät wieder: 15.15.255.

> Die grüne APP-LED wird nach dem Werksreset durchgängig grün leuchten.
> ► Siehe Tabelle 8 “Status des Geräts – Gerät startet” auf S. 35.

Um das Gerät auf Werkseinstellungen zurückzusetzen, haben Sie folgende Möglichkeiten:

- Manuell: Sie drücken die Programmiertaste am Gerät in einer bestimmten Abfolge.
- Automatisiert: Sie wählen die Funktion <<Werksreset>> auf der Gerätewebseite.

© 2021 ise Individuelle Software und Elektronik GmbH

Warnung

Gefahr durch elektrischen Schlag
Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung.
Elektrischer Schlag kann zum Tod führen.
Beachten Sie die Installationsvorschriften:

- Führen Sie die Busleitung mit intaktem Mantel bis nahe an die Busanschlussklemme.
- Schieben Sie die Busleitung mit Druck bis zum Anschlag in die Busanschlussklemme.
- Installieren Sie Busleitungsadern ohne Mantel (SELV) sicher getrennt von allen Nicht-Schutzkleinspannungsleitungen (PELV/FELV).
- Halten Sie den vorgeschriebenen Abstand ein.
- Stecken Sie die mitgelieferte Abdeckkappe auf.
- Weitere Informationen siehe auch VDE-Bestimmungen zu SELV (DIN VDE 0100-410/ „Sichere Trennung“, KNX Installationsvorschriften).

Gerät manuell auf Werkseinstellungen zurücksetzen

Voraussetzung: Das Gerät ist spannungslos geschaltet.

1. Drücken Sie die Programmiertaste (siehe Abbildung 28, Pos. 1) und halten Sie diese weiter gedrückt, während Sie die Spannungsanschlussklemme aufstecken.
2. Halten Sie die Programmiertaste weiterhin gedrückt, bis die folgenden LEDs alle gleichzeitig langsam blinken:

   - Programmier-LED (siehe Abbildung 24, Pos. 1)
   - APP-LED (siehe Abbildung 24, Pos. 2)
   - COM-LED (siehe Abbildung 24, Pos. 3)

   Übliche Dauer: ca. 30 Sekunden.
3. Lassen Sie die Programmiertaste kurz los.
4. Drücken Sie erneut die Programmiertaste und halten Sie diese solange gedrückt, bis die folgenden LEDs alle gleichzeitig schnell blinken:

   - Programmier-LED (siehe Abbildung 24, Pos. 1)
   - APP-LED (siehe Abbildung 24, Pos. 2)
   - COM-LED (siehe Abbildung 24, Pos. 3)
5. Lassen Sie die Programmiertaste los.

Die Werkseinstellungen werden zurückgesetzt. Sie müssen das Gerät nicht neu starten.

© 2021 ise Individuelle Software und Elektronik GmbH

Gerät über die Gerätewebseite auf Werkseinstellungen zurücksetzen

1. Rufen Sie die Gerätewebseite auf ► siehe Gerätewebseite: Startseite aufrufen, S. 29.
2. Wählen Sie in der Menüleiste <<System>> → <<Werksreset>>.
3. Bestätigen Sie die Sicherheitsabfrage.

Sobald die Werkseinstellungen vollständig zurückgesetzt wurden, wird die Startseite angezeigt.

Das Gerät muss nicht neu gestartet werden.

8.4 Firmware aktualisieren

Funktionserweiterungen für den SMART CONNECT KNX Remote Access erhalten Sie über eine neue Version der Firmware. Die jeweils aktuelle Firmware und das passende Produkthandbuch stehen Ihnen auf unserer Webseite unter www.ise.de zur Verfügung.

Damit Sie die neuen Funktionen nutzen können, müssen die Versionen der eingesetzten Firmware und des Produktdatenbankeintrags kompatibel sein.

8.4.1 Firmware über die Gerätewebseite aktualisieren

Sie können ausschließlich eine Firmwareversion aufspielen, die neuer ist als die aktuelle Version auf dem Gerät. Vorangegangene Versionen können nicht aufgespielt werden.

Es existieren zwei Varianten zur Aktualisierung:

- Online: Firmware automatisiert online aufspielen.
- Offline: Firmware offline aufspielen. Für Geräte ohne Internetanbindung in der Einbauumgebung.

Keine Kompatibilitätsprüfung

Das System prüft nicht, ob die aktuelle Konfiguration mit der neuen Firmware kompatibel ist. Sie müssen selbst prüfen, ob die Firmware mit dem Produktdatenbankeintrag kompatibel ist, ► siehe Kompatibilität zwischen Produktdatenbankeintrag und Firmwareversion, S. 47.

Firmware automatisiert online aufspielen

1. Laden Sie die aktuelle Firmwareversion von der Webseite www.ise.de herunter.
2. Rufen Sie die Gerätewebseite auf.
3. Wählen Sie in der Menüleiste <<System>> → <<Firmware aktualisieren>>.
   Das System ermittelt die aktuell installierte Firmwareversion. Falls eine neue Firmwareversion für das Gerät verfügbar ist, wird Ihnen diese angezeigt.
4. Klicken Sie auf die Schaltfläche <<Firmware aktualisieren>>.

© 2021 ise Individuelle Software und Elektronik GmbH

Firmware offline aufspielen

Voraussetzung: Sie haben die aktuelle Firmwareversion von der Webseite www.ise.de heruntergeladen.

1. Rufen Sie die Gerätewebseite auf.
2. Wählen Sie in der Menüleiste <<System>> → <<Firmware aktualisieren>>.
3. Wählen Sie die Schaltfläche <<Datei auswählen>>.
4. Wählen Sie im Explorer die gewünschte Firmware-Datei und bestätigen Sie Ihre Auswahl mit der Schaltfläche <<Öffnen>>.
5. Klicken Sie auf die Schaltfläche <<Firmware aktualisieren>>.

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

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

Das Update kann über die Schaltfläche <<Firmware aktualisieren>> gestartet werden. Im Fall einer möglichen Inkompatibilität muss das Update zur Sicherheit nochmals bestätigt werden.

© 2021 ise Individuelle Software und Elektronik GmbH

8.4.2 Kompatibilität zwischen Produktdatenbankeintrag und Firmwareversion

Damit Sie den vollen Umfang der neuen Funktionen des Geräts nutzen können, muss die Version der eingesetzten Firmware mit der Version des Applikationsprogramms des Geräts im Projekt kompatibel sein. Das Applikationsprogramm ist Teil des Produktdatenbankeintrags.

Die Applikationsprogramm-Version finden Sie in der ETS im Bereich <<Eigenschaften>> des Geräts auf dem Reiter <<Information>> → <<Applikationsprogramm>> unter <<Programmversion>>.

Kompatibilität auf einen Blick

Wenn die Hauptversion des Applikationsprogramms und die der Firmware identisch sind, dann sind die Versionen voll kompatibel.

Die Versionsnummern sind nach folgendem Schema aufgebaut: <Hauptversionsnr.>.<Unterversionsnr.>

Beispiel: Volle Kompatibilität bei gleichen Hauptversionsnummern

- Firmwareversion: 2.3
- Applikationsprogramm-Version: 2.0

Damit Sie alle neuen Funktionen nutzen können, kann die Aktualisierung des Applikationsprogramms notwendig sein, ► siehe Produkt in bestehendem Projekt aktualisieren, S. 39.

© 2021 ise Individuelle Software und Elektronik GmbH

Inkompatibilität auf einen Blick

Wenn die neue Firmware eine höhere Hauptversionsnummer hat als das Applikationsprogramm, dann sind die Versionen inkompatibel.

Beispiel: Inkompatibilität bei höherer Hauptversionsnummer der Firmware

- Firmwareversion: 2.3
- Applikationsprogramm-Version: 1.3

Kompatibilität herstellen

Im Fall einer Inkompatibilität müssen Sie das Applikationsprogramm entladen.

- Das Gerät verbleibt in den bestehenden Projekten.
- Das Gerät behält die Version des Applikationsprogramms in der ETS.
- Die komplette Parametrierung wird verworfen.
- Benutzerdaten in der ETS bleiben erhalten.

Voraussetzung: Neuer Produktdatenbankeintrag des Geräts ist im Katalog vorhanden.

1. Öffnen Sie in der ETS das Projekt, in dem das Gerät aktualisiert werden soll.
2. Suchen Sie den neuen Produktdatenbankeintrag im Katalog und fügen Sie die neue Version des Geräts Ihrem Projekt hinzu.
3. Wählen Sie die alte Version des Geräts in der Topologie Ihres Projekts.
4. Wählen Sie im Fenster <<Topologie>> in der Menüleiste die Schaltfläche <<Entladen>> → <<Applikationsprogramm>>.

   Nach dem Entladen verhält sich das Gerät wie im Auslieferungszustand. Das Gerät ist dann unprojektiert. Beginnen Sie dann die Projektierung wie gewohnt. ▶ siehe Projektierung, S. 37.

5. Wählen Sie im Bereich <<Eigenschaften>> den Reiter <<Informationen>> → <<Applikationsprogramm>>.
6. Klicken Sie auf die Schaltfläche <<Aktualisieren>> unterhalb des Texts <<Applikationsprogramm-Version aktualisieren>>.
7. Wählen Sie das neu hinzugefügte Gerät und löschen Sie es wieder aus Ihrer Topologie.

© 2021 ise Individuelle Software und Elektronik GmbH

8.5 Konfiguration der Firewall

Der SMART CONNECT KNX Remote Access kommuniziert mit dem SDA-Portal ausschließlich über eine HTTPS-Verbindung. Alle Daten werden über diese Verbindung in beide Richtungen ausgetauscht, so dass in der Regel keine zusätzliche Konfiguration der Firewall notwendig ist.
Möchten Sie den Netzwerkzugriff auf bestimmte Domains und Ports bzw. IP-Adressen beschränken, empfehlen wir Ausnahmen zu konfigurieren. Auf https://securedeviceaccess.net finden Sie eine Übersicht mit den SDA-relevanten Domains, Ports und IP-Adressen.

8.6 VPN einrichten

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

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

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

Voraussetzung für die VPN-Einrichtung

- Unter https://securedeviceaccess.net wurde ein Benutzerkonto angelegt.
- Der SMART CONNECT KNX Remote Access ist mit dem Internet verbunden.
- Der SMART CONNECT KNX Remote Access ist im SDA-Portal registriert.
- Quick Connect wurde unter <<Gerätedaten>> im SDA-Portal deaktiviert.
- Eine veröffentlichte Version (released) des OpenVPN-Clients wurde heruntergeladen und auf dem PC oder Smartphone installiert.

VPN-Einrichtung

1. Melden Sie sich im SDA-Portal an.
2. Klicken Sie in der Funktionsübersicht auf <<VPN-Zugang>>.
3. Wählen Sie den Zugangstyp und den Umfang des Datenverkehrs.
4. Warten Sie, bis die Konfigurationsdatei erstellt wurde, und laden Sie die Datei herunter.
5. Öffnen Sie den OpenVPN-Client und importieren Sie die Konfigurationsdatei.
6. Aktivieren Sie im OpenVPN-Client die VPN-Verbindung.

Möchten Sie den VPN-Zugang für mehrere Benutzer anlegen, benötigt jeder dieser Benutzer ein eigenes

© 2021 ise Individuelle Software und Elektronik GmbH

Benutzerkonto im SDA-Portal. Die Schritte 4 bis 6 sind für jeden Benutzer zu wiederholen.

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

VPN-Einstellungen im SDA-Portal

Unter <<VPN-Zugang>> können Administratoren die folgenden Einstellungen vornehmen:

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

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

© 2021 ise Individuelle Software und Elektronik GmbH

9 Parameter konfigurieren

Nachfolgend sind die Reiter der Ansicht <<Parameter>> beschrieben. Weitere Details entnehmen Sie den entsprechenden Abschnitten.

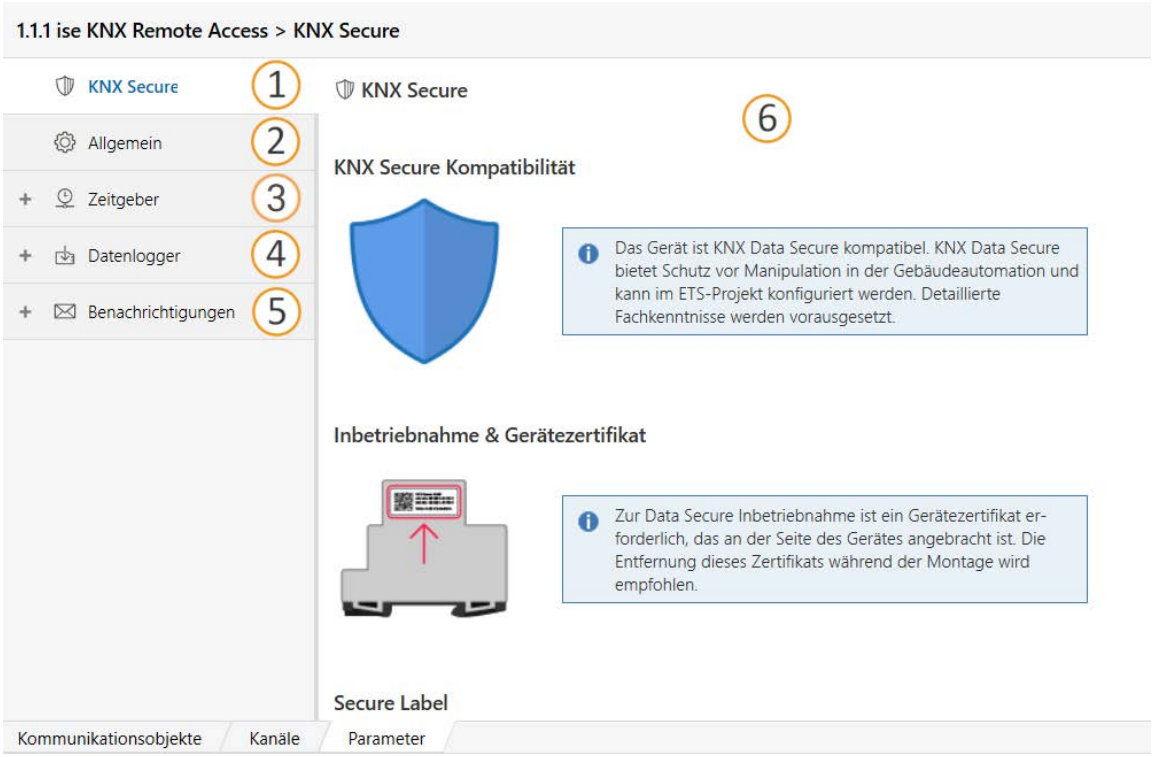


Abbildung 29: Parameter in der ETS

Pos.	Beschreibung
1	Informationen zu KNX Secure
2	Einstellungen allgemeiner Funktionen
3	Einstellungen der Zeitgeber-Funktion
4	Einstellungen der Datenlogger-Funktion
5	Einstellungen zu SDA-Benachrichtigungen
6	Information bzw. Konfiguration der Parameter des gewählten Reiters

© 2021 ise Individuelle Software und Elektronik GmbH

9.1 Parameter – Allgemein

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

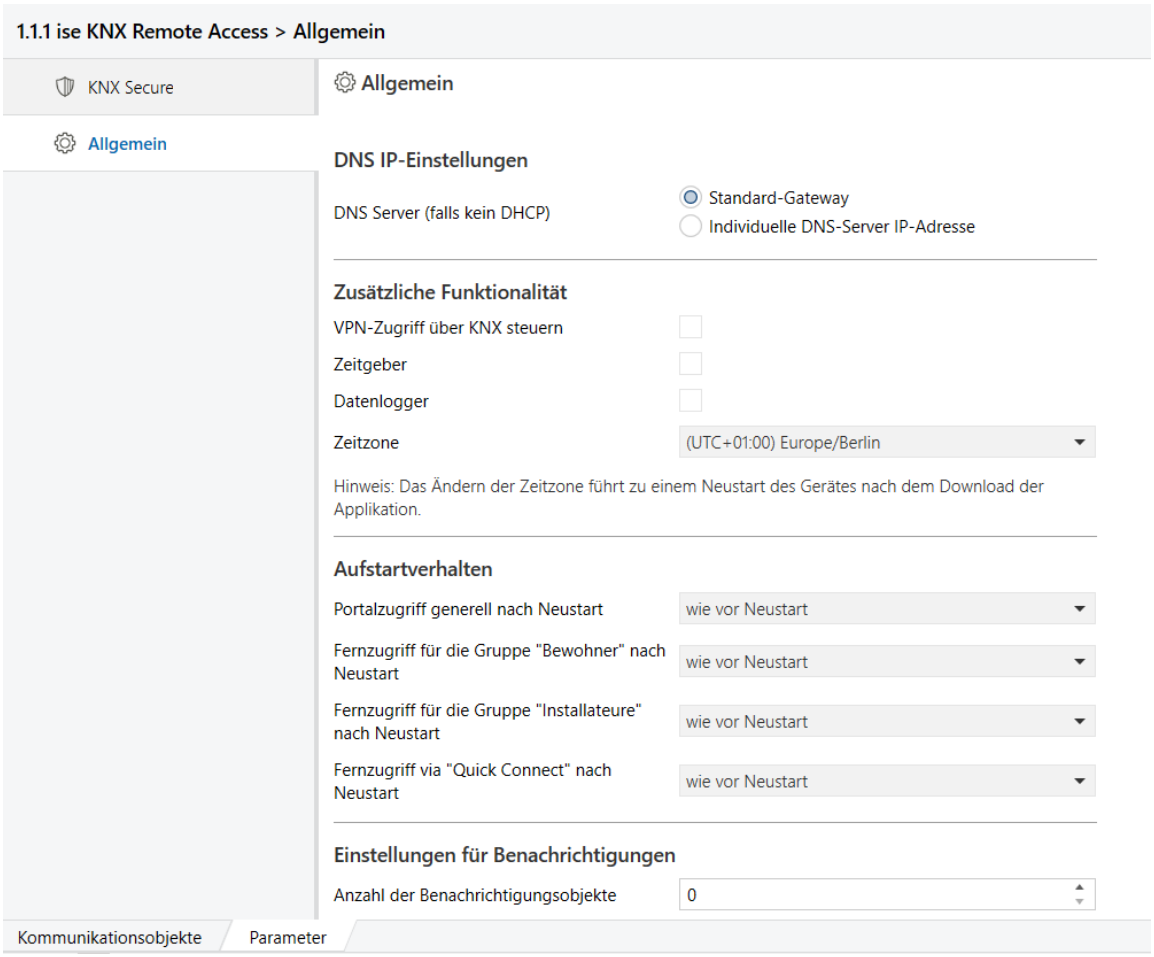


Abbildung 30: Parameter - Allgemein

9.1.1 DNS-Server (falls kein DHCP)

Eintrag / Auswahl	Beschreibung
Standard Gateway	Die IP-Adresse des Standardgateways wird verwendet.
Individuelle DNS-Server IP-Adresse	Das Feld <<Individuelle DNS-Server IP-Adresse>> wird hinzugefügt.
0.0.0.0	Tragen Sie die individuelle IP-Adresse ein. Bei Verwendung von 0.0.0.0 wird das Default Gateway verwendet.

Tabelle 13: Einstellungen zu Parameter <<DNS-Server (falls kein DHCP)>>

© 2021 ise Individuelle Software und Elektronik GmbH

9.1.2 VPN-Zugriff über KNX steuern

Eintrag / Auswahl	Beschreibung
Nein	Die Kommunikationsobjekte zu VPN-Zugriff bleiben ausgeblendet.
Ja	Die Kommunikationsobjekte zu VPN-Zugriff werden eingeblendet.

Tabelle 14: Einstellungen zu Parameter <<VPN-Zugriff über KNX steuern>>

9.1.3 Zeitgeber

Eintrag / Auswahl	Beschreibung
Nein	Der Reiter <<Zeitgeber>> und die entsprechenden Kommunikationsobjekte bleiben ausgeblendet.
Ja	Der Reiter <<Zeitgeber>> und die entsprechenden Kommunikationsobjekte werden eingeblendet. Das Gerät arbeitet als Zeitgeber und sendet in konfigurierbaren Intervallen die aktuelle Zeit und das Datum auf den KNX Bus.

Tabelle 15: Einstellungen zu Parameter <<Zeitgeber>>

9.1.4 Datenlogger

Eintrag / Auswahl	Beschreibung
Nein	Der Reiter <<Datenlogger>> und die entsprechenden Kommunikationsobjekte bleiben ausgeblendet.
Ja	Der Reiter <<Datenlogger>> und die entsprechenden Kommunikationsobjekte werden eingeblendet. Das Gerät arbeitet als Datenlogger und speichert die Daten im festgelegten Speichertyp.

Tabelle 16: Einstellungen zu Parameter <<Datenlogger>>

© 2021 ise Individuelle Software und Elektronik GmbH

9.1.5 Zeitzone

Eintrag / Auswahl	Beschreibung
(UTC+01:00) Europe/Berlin	Auswahl der Zeitzone. Es existieren mehrere Zeitzonen mit identischen UTC-Abweichungen. In einigen dieser Zeitzonen erfolgt die Sommer-/Winterzeitumstellung zu einem anderen Zeitpunkt.
Weitere UTC-Zeitzonen	

Tabelle 17: Einstellungen zu Parameter <<Zeitzone>>

Hinweis:

Wird diese Einstellung geändert, erfolgt nach der Programmierung der Applikation ein sofortiger Neustart des SMART CONNECT KNX Remote Access.
Die Option, NTP über die Gerätewebseite zu deaktivieren, wurde ab Firmwareversion 5.0 entfernt. Wenn Sie NTP deaktiviert haben, wird dieses automatisch mit dem Standard-NTP-Server pool.ntp.org aktiviert.

9.1.6 Portalzugriff generell nach Neustart

Eintrag / Auswahl	Beschreibung
wie vor Neustart	Der generelle Portalzugriff wird nach einem Neustart auf den letzten bekannten Wert vor dem Neustart eingestellt. Ist z. B. der generelle Portalzugriff vor Neustart aktiviert, wird der Portalzugriff nach Neustart auch aktiviert.
aktiviert	Erlaubt dem Gerät nach jedem Neustart eine Verbindung zum SDA-Portalserver aufzubauen.
deaktiviert	Verbietet dem Gerät nach jedem Neustart eine Verbindung zum SDA-Portalserver aufzubauen.

Tabelle 18: Einstellungen zu Parameter <<Portalzugriff generell nach Neustart>>

© 2021 ise Individuelle Software und Elektronik GmbH

9.1.7 Fernzugriff nach Neustart

Der Fernzugriff wird in die Zugriffsgruppen Bewohner und Installateure sowie Quick Connect unterteilt.

Eintrag / Auswahl	Beschreibung
wie vor Neustart	Der Fernzugriff der jeweiligen Gruppe bzw. Quick Connect wird nach jedem Neustart auf den letzten bekannten Wert vor dem Neustart eingestellt. Ist z. B. der Fernzugriff vor Neustart aktiviert, wird der Fernzugriff 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 nach jedem Neustart.

Tabelle 19: Einstellungen zu Parameter <<Fernzugriff (...) nach Neustart>>

9.1.8 Anzahl der Benachrichtigungsobjekte

Eintrag / Auswahl	Beschreibung
0|1…|49|50	Hier wird die Anzahl der SDA-Benachrichtigungsobjekte festgelegt (max. 50). Entsprechend der Auswahl werden die Gruppenobjekte „101 ff“ sichtbar.
Trennzeichen für Fließkommazahlen.	Sie können zwischen Komma und Punkt als Trennzeichen wählen.

Tabelle 20: Einstellungen zu Parameter <<Anzahl der Benachrichtigungsobjekte>>

© 2021 ise Individuelle Software und Elektronik GmbH

9.2 Parameter – Zeitgeber

Als Zeitgeber kann der SMART CONNECT KNX Remote Accesss die aktuelle Uhrzeit in konfigurierbaren Intervallen auf den KNX Bus senden. Die gesendete Zeit wird aus der Systemzeit bezogen. Diese wird mit einem über die Gerätewebseite konfigurierbaren NTP-Server synchronisiert. Über die Parameter „Uhrzeit senden“ (Kommunikationsobjekt 50) und „Datum senden“ (Kommunikationsobjekt 51) wird das Intervall für das Senden des Kommunikationsobjekts 52 „Datum und Uhrzeit“ festgelegt. Sofern sich die Parameterwerte unterscheiden, wird das kürzere Intervall verwendet.

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

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

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

Durch den Parameter <<Zeitgeber>> wird das Kommunikationsobjekt 53 zur Verfügung gestellt, mit dem das Senden der Zeit/des Datums ausgelöst werden kann (Trigger).

Bei der Auslieferung ist die Zeitgeberfunktion deaktiviert.

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

Tabelle 21: Parameter auf Reiter <<Zeitgeber>>

© 2021 ise Individuelle Software und Elektronik GmbH

9.3 Parameter – Datenlogger

Die Datenloggerfunktionalität wird über den Parameter <<Datenlogger>> in der Parameteransicht <<Allgemein>> freigeschaltet. Ist er auf <<Ja>> eingestellt, ist die Datenloggerfunktionalität grundsätzlich aktiviert. Wird eine microSD-Karte in das Gerät gesteckt oder befindet sich bereits eine microSD-Karte im Gerät, so startet das Loggen automatisch, sofern es nicht über das Kommunikationsobjekt 57 „Aktiviere Datenlogger“ deaktiviert ist.

Der Datenlogger-Zustand wird über das Kommunikationsobjekt 58 „Datenlogger Status“ gesendet. Der Datenlogger-Zustand kann aber auch direkt abgefragt werden. Solange der Datenlogger aktiv ist, hat das Kommunikationsobjekt den Wert 1. Das Kommunikationsobjekt „Datenlogger Status“ übernimmt den Wert 0 und sendet diesen, wenn

- die microSD-Karte entfernt wird,
- kein Speicherplatz auf der microSD-Karte vorhanden ist oder
- der Datenlogger über das Kommunikationsobjekt 57 „Aktiviere Datenlogger“ deaktiviert wurde.

Über den Parameter <<Datenloggingformat>> in derselben Parameteransicht kann konfiguriert werden, ob ein ETS3 (.trx) oder ETS4/ETS5 (.xml)-konformes Dateiformat verwendet werden soll. Der Datenlogger kann über das Kommunikationsobjekt „Aktiviere Datenlogger“ aktiviert und deaktiviert werden. Die Benennung und Ablage der Logdateien auf der microSD-Karte erfolgt nach folgendem Schema:

Jahr
-----Monat
----------Tag
----------2010_01_06_TP1.xml

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

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

Der SMART CONNECT KNX Remote Access unterstützt SDHC-Karten bis maximal 32 GB. Die Karten müssen mit FAT32 formatiert werden.

Achtung

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

© 2021 ise Individuelle Software und Elektronik GmbH

Zur Überwachung des Speicherstatus stehen die Kommunikationsobjekte 59 und 60 zur Verfügung.

Hinweis:

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

Parameter	Eintrag / Auswahl	Bemerkungen
<<Format>>	**ETS4/ETS5**	Die Daten werden in einem ETS4-konformen Format auf die microSD-Karte geloggt (.xml), welches auch mit der ETS5 lesbar ist.
	ETS3	Die Daten werden in einem ETS3-konformen Format geloggt (.trx).
<<Speichertyp>>	Ringspeicher	Dieser Parameter legt fest, wie der microSD-Karten-speicher verwendet werden soll.
	Festspeicher	
Nur sichtbar, wenn der <<Speichertyp>> auf <<Festspeicher>> eingestellt ist. Dieser Parameter legt fest, welchem Typ das Statusobjekt des Kartenfüllstands entsprechen soll.		
<<Speicherstatus-typ>>	Binär	Es wird ein 1-Bit-Objekt verwendet. Der Wert <<1>> bedeutet, dass die microSD-Karte voll ist. Eine <<0>> bedeutet, dass auf der microSD-Karte noch Platz zum Loggen ist.
	Wert (0-255)	Es wird ein 1-Byte-Objekt verwendet. Der Wertebe-reich liegt zwischen 0 - 255. Dabei entspricht der Wert <<255>> einem Kartenfüllstand von 100 %.

Tabelle 22: Parameter auf Reiter <<Datenlogger>>

© 2021 ise Individuelle Software und Elektronik GmbH

Zugriff auf das Datenlogger-Archiv

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

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

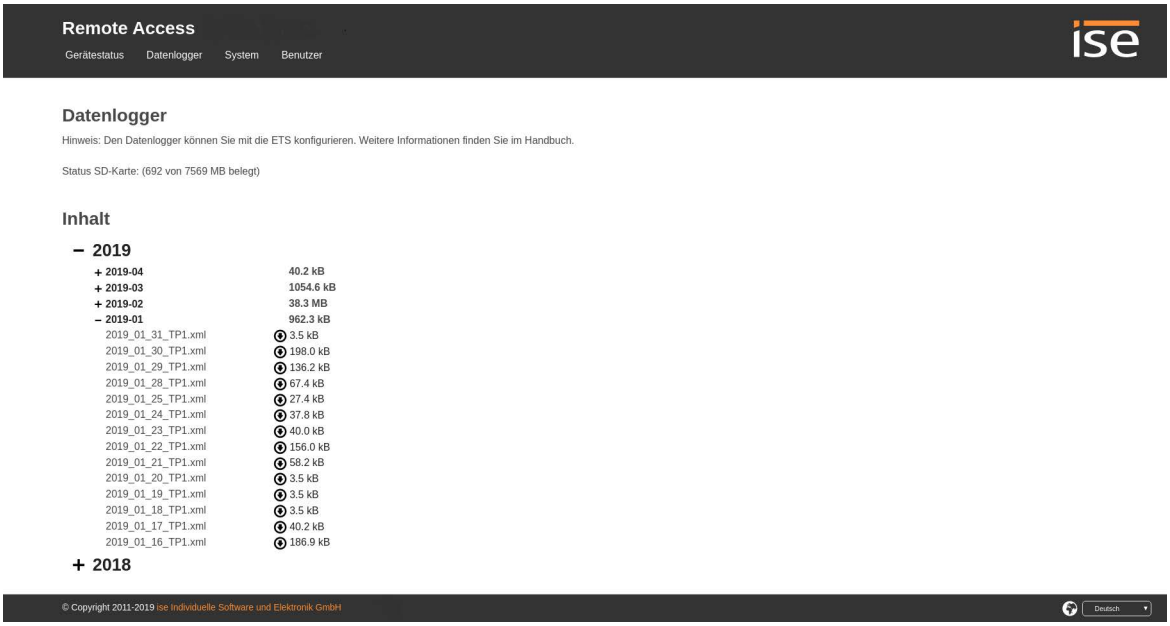


Abbildung 31: Datenlogger-Archiv

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

Hinweis:

Sollten sich Secure-Telegramme im Gruppenmonitor der ETS5 nicht entschlüsseln lassen, starten Sie die ETS5 neu und wiederholen Sie die Entschlüsselung.

© 2021 ise Individuelle Software und Elektronik GmbH

9.4 Parameter – Benachrichtigungen

KNX Kommunikationsobjekte sowie Systemereignisse wie das An-/Abmelden eines SMART CONNECT KNX Remote Access am SDA-Portal können genutzt werden, um Nachrichten (sog. SDA-Benachrichtigungen) im SDA-Portalserver zu generieren. Diese können neben statischen Texten auch Werte vom KNX Bus oder auch einen Anhang wie z. B. ein Kamerabild beinhalten. Diese Benachrichtigungen können per E-Mail, Telefon oder SMS weitergeleitet werden.

Hinweis:

Anhänge von Benachrichtigungen sind auf eine Datenmenge von 250 kB begrenzt. Wird diese Datenmenge überschritten, erfolgt keine Übertragung. Eine Fehlermeldung wird im SDA-Portal ausgegeben.

Eine SDA-Benachrichtigung besteht aus folgenden Eigenschaften:

- Erzeugungsdatum
- Kategorie
- Betreff
- Inhaltstext
- Dringlichkeit (Niedrig, Hoch, Alarm, System)
- Optional einen Anhang, z. B. Bild einer IP-Kamera

SDA-Benachrichtigungen über KNX

Im Datenbankeintrag stehen 50 KNX Kommunikationsobjekte zur Verfügung, um Werte vom KNX Bus zu empfangen und Benachrichtigungen daraus zu erzeugen.

Folgende Datentypen werden unterstützt:

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

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

© 2021 ise Individuelle Software und Elektronik GmbH

Die beiden Texteigenschaften „Betreff“ und „Text“ können aus statischen Texten bestehen, in denen per Platzhalter der vom KNX empfangene Wert eingesetzt werden kann.

Außerdem kann optional eine Webadresse angegeben werden, um von einem Webserver (z. B. IP-Kamera) einen Anhang zu laden und diesen an eine Nachricht anzuhängen.

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

Die Parameter-Seite <<Benachrichtigungen>> ist nur sichtbar, wenn die Anzahl der Benachrichtigungsobjekte auf der Parameter-Seite <<Allgemein>> größer 0 ist.

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

Benachrichtigungen unterdrücken

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

© 2021 ise Individuelle Software und Elektronik GmbH

Parameter	Eintrag / Auswahl	Bemerkungen
<<Datentyp>>	**Bool (1 Bit, DPT 1.001)** Prozent (1 Byte, DPT 5.001) Zähler (1 Byte, DPT 5.010) Fließkomma (2 Bytes, DPT 9.*) Text (14 Bytes, DPT 16.001)	Der gewünschte Datentyp der jeweiligen SDA-Benachrichtigung kann ausgewählt werden.
<<Benachrichtigung nur bei Wertänderung>>	**Checkbox deaktiviert** Checkbox aktiviert	Benachrichtigung immer senden. Benachrichtigung nur senden, wenn sich der Wert im Gruppentelegramm geändert hat.
<<Schwellwert>>	0-1000 Angabe als Ganzzahl	Benachrichtigungen werden unterdrückt, bis der Schwellwert überschritten wird. Der Schwellwert ist die Abweichung vom letzten Wert (als absolute Zahl), der eine Benachrichtigung erzeugt hat. 0: Kein Schwellwert. Sie erhalten bei jeder Änderung eine Benachrichtigung.
<<Schwellwert Basis>>	**1: Kein Faktor** Wert gemäß Auswahlliste	Faktor mit dem der Schwellwert bei Bedarf multipliziert wird.
<<Filter>>	Text	Der Filter kann aus einem festen Wert oder bis zu zwei Bedingungen bestehen. Beim DPT 1.001 (Bool) ist das Filtern über eine Auswahlliste möglich.
<<Priorität>>	**Niedrig** Hoch Alarm	
<<Kategorie>>	Text	Kann zum Filtern der SDA-Benachrichtigungen und deren Weiterleitungen im SDA-Portal genutzt werden.
<<Betreff>>		Wird beim Versand von E-Mails, SMS oder Pushmitteilungen als Betreff genutzt.
<<Text>>		Wird beim Versand von E-Mails, SMS oder Pushmitteilungen als Text genutzt.
<<Anhang hinzufügen>>	**Checkbox deaktiviert** Checkbox aktiviert	
<<URL des Anhangs>>	Text	Nur http-Anfragen werden unterstützt. Beachten Sie die maximal zulässige Dateigröße von 250 kB.

Tabelle 23: Parameter auf Reiter <<Benachrichtigungen>>

© 2021 ise Individuelle Software und Elektronik GmbH

10 Kommunikationsobjekte

Der SMART CONNECT KNX Remote Access stellt die folgenden Kommunikationsobjekte zur Anbindung von Gruppenadressen zur Verfügung.

Wichtiger Hinweis für alle Kommunikationsobjekte, die eine laufende Verbindung signalisieren:

Bei der Nutzung des HTTP-Zugriffs, also ohne SDA-Client, wird die Verbindung zum Gerät nicht sofort nach dem Laden der Seiten bzw. Schließen des Browsers beendet. HTTP-Verbindungen können bis zu fünf Minuten zum Schließen benötigen. Die entsprechenden Kommunikationsobjekte signalisieren das Schließen erst, wenn dieser Vorgang abgeschlossen ist. Bei der Nutzung des SDA-Clients erfolgt der Verbindungsabbau synchron.

Einschränkungen und Freigaben von Zugriffsrechten über Kommunikationsobjekte

Wenn der SMART CONNECT KNX Remote Access in einem ETS-Projekt eingefügt wird, können über dessen Kommunikationsobjekte KNX Zugriffsmöglichkeiten verboten bzw. erlaubt werden. Die über den KNX in der entfernten Installation festgelegten Einschränkungen von Zugriffsrechten wiegen immer stärker als Festlegungen im SDA-Portal. So kann über Gruppentelegramme der SDA-Fernzugriff unabhängig von Einstellungen im SDA-Portal komplett deaktiviert werden. Ebenso kann auch sämtliche Kommunikation mit dem SDA-Portal über Gruppentelegramme deaktiviert werden.

10.1 Fernzugriff

1 |	
Name	Portalzugriff zulassen
Funktion	Erlaubt oder verbietet dem Gerät eine Verbindung zum SDA-Portalserver aufzubauen. Ist der Verbindungsaufbau verboten, ist das Gerät nicht von außen zu erreichen.
Mögliche Werte	0: Verbieten 1: Erlauben
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 24: Portalzugriff zulassen

© 2021 ise Individuelle Software und Elektronik GmbH

2 |	
Name	Portalzugriff zulassen – Status
Funktion	Zeigt an, ob das Gerät eine Verbindung zum SDA-Portalserver aufbauen darf.
Mögliche Werte	0: Verboten 1: Erlaubt
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü---

Tabelle 25: Portalzugriff zulassen – Status

3 | 5 | 7	
Kommunikationsobjekte	3: Bewohner 5: Installateure 7: Quick Connect
Name	Fernzugriff zulassen
Funktion	Erlaubt oder verbietet den Fernzugriff für Mitglieder der jeweiligen Gruppe bzw. über „Quick Connect“.
Mögliche Werte	0: Verbieten 1: Erlauben
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 26: Fernzugriff zulassen

© 2021 ise Individuelle Software und Elektronik GmbH

4 | 6 | 8	
Kommunikationsobjekte	4: Bewohner 6: Installateure 8: Quick Connect
Name	Fernzugriff zulassen – Status
Funktion	Zeigt an, ob Fernzugriff für Mitglieder der jeweiligen Gruppe bzw. über „Quick Connect“ erlaubt ist.
Mögliche Werte	0: Verboten 1: Erlaubt
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 27: Fernzugriff zulassen – Status

9 |	
Name	VPN-Zugriff zulassen
Funktion	Aktiviert oder deaktiviert den VPN-Zugriff aller Benutzer, für die VPN im SDA-Portal freigegeben wurde.
Mögliche Werte	0: Deaktivieren 1: Aktivieren
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Schreiben
Flags (KLSÜAI)	K--S---

Tabelle 28: VPN-Zugriff zulassen

© 2021 ise Individuelle Software und Elektronik GmbH

10 |	
Name	VPN-Zugriff zulassen — Status
Funktion	Zeigt an, ob VPN-Zugriff zugelassen ist.
Mögliche Werte	0: Verboten 1: Erlaubt
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.003/Freigeben
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 29: VPN-Zugriff zulassen – Status

20 |	
Name	Portalverbindung — Status
Funktion	Zeigt an, ob eine Portalverbindung aufgebaut ist. Genauere Informationen stellt Kommunikationsobjekt 31 zur Verfügung.
Mögliche Werte	0: Getrennt 1: Verbunden
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.011/Status
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 30: Portalverbindung – Status

© 2021 ise Individuelle Software und Elektronik GmbH

21 |	
Name	Fernzugriffsverbindung — Status
Funktion	Zeigt an, ob mindestens eine Fernzugriffsverbindung, unabhängig von der Art der Verbindung, derzeit aktiv ist.
Mögliche Werte	0: Nicht aktiv 1: Aktiv
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.011/Status
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 31: Fernzugriffsverbindung – Status

22 | 23 | 24	
Kommunikationsobjekte	22: Bewohner 23: Installateure 24: Quick Connect
Name	Fernzugriffsverbindung „Gruppe“ — Status
Funktion	Zeigt an, ob eine Fernzugriffsverbindung für Mitglieder der jeweiligen Gruppe bzw. über „Quick Connect“ aktiv ist.
Mögliche Werte	0: Nicht aktiv 1: Aktiv
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.011/Status
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 32: Fernzugriffsverbindung „Gruppe“ – Status

© 2021 ise Individuelle Software und Elektronik GmbH

25 |	
Name	VPN-Zugriff — Status
Funktion	Zeigt an, ob derzeit eine aktive VPN-Verbindung besteht.
Mögliche Werte	0: Nicht aktiv 1: Aktiv
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.011/Status
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 33: VPN-Zugriff – Status

10.2 Verbindungsfehler

30 |	
Name	Fehleranzeige
Funktion	Zeigt einen Verbindungsfehler an, der durch Kommunikationsobjekt 32 beschrieben wird. Weitere Details auf der Gerätewebseite des SMART CONNECT KNX Remote Access.
Mögliche Werte	0: Kein Alarm 1: Alarm
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.005/Alarm
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 34: Fehleranzeige

© 2021 ise Individuelle Software und Elektronik GmbH

31 |	
Name	Info Portalverbindung
Funktion	Diagnoseinformationen zur Portalverbindung.
Details	Liefert genauere Informationen zum Portalverbindungsstatus, der durch Kommunikationsobjekt 20 angezeigt wird.
Datenbreite	14 Byte
Datenpunkttyp / Datentyp	16.001/Zeichen (ISO 8859-1)
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 35: Info Portalverbindung

32 |	
Name	Info Verbindungsfehler
Funktion	Zusätzliche Diagnoseinformation im Falle eines Fehlers der Portalverbindung.
Details	Liefert genauere Informationen zum Verbindungsfehler, der durch Kommunikationsobjekt 30 angezeigt wird.
Datenbreite	14 Byte
Datenpunkttyp / Datentyp	16.001/Zeichen (ISO 8859-1)
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 36: Info Verbindungsfehler

© 2021 ise Individuelle Software und Elektronik GmbH

10.3 Zeitgeber

50 |	
Name	Uhrzeit
Funktion	Sendet zyklisch und auf Anfrage die aktuelle Uhrzeit.
Details	Das Intervall ist parametrierbar. Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie die derzeitige Systemzeit, die von der korrekten Zeit abweichen kann.
Datenbreite	3 Byte
Datenpunkttyp / Datentyp	10.001/Tageszeit
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 37: Uhrzeit

51 |	
Name	Datum
Funktion	Sendet zyklisch und auf Anfrage das aktuelle Datum.
Details	Das Intervall ist parametrierbar. Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie das derzeitige Systemdatum, das vom korrekten Datum abweichen kann.
Datenbreite	3 Byte
Datenpunkttyp / Datentyp	11.001/Datum
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 38: Datum

© 2021 ise Individuelle Software und Elektronik GmbH

52 |	
Name	Datum und Uhrzeit
Funktion	Sendet zyklisch und auf Anfrage aktuelles Datum und Uhrzeit.
Details	Das Intervall wird aus dem geringeren Intervall der Kommunikationsobjekte 50 und 51 bestimmt. Wenn Sie dieses Objekt direkt auslesen, wenn noch keine gültige NTP-Zeit abgefragt werden konnte, erhalten Sie die derzeitige Systemzeit und -datum, welche von der korrekten Zeit und Datum abweichen können.
Datenbreite	8 Byte
Datenpunkttyp / Datentyp	19.001/Datum/Zeit
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 39: Datum und Uhrzeit

53 |	
Name	Auslöser Datum/Uhrzeit senden
Funktion	Löst das Senden von Datum und Uhrzeit aus.
Details	1 Bit Objekt zum Auslösen des Sendens der/des aktuellen Zeit/Datums, wenn dem Objekt ein beliebiger Wert zugewiesen wird. Wenn noch keine NTP-Abfrage erfolgreich war, werden keine Werte gesendet.
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.017/Auslöser
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 40: Auslöser Datum/Uhrzeit senden

© 2021 ise Individuelle Software und Elektronik GmbH

54 |	
Name	NTP-Abfrage — Status
Funktion	Zeigt an, ob eine gültige Uhrzeit vom NTP-Server abgefragt werden konnte.
Mögliche Werte	0: NTP-Abfrage war nicht erfolgreich 1: NTP-Abfrage war erfolgreich
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.002/Boolesch
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 41: NTP-Abfrage – Status

10.4 Datenlogger

55 |	
Name	SD-Kartenfehler
Funktion	Zeigt an, ob derzeit ein Fehler mit der SD-Karte vorhanden ist.
Mögliche Werte	0: Kein Fehler 1: Fehler
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.002/Boolesch
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 42: SD-Kartenfehler

© 2021 ise Individuelle Software und Elektronik GmbH

56 |	
Name	SD-Fehlercode
Funktion	Zeigt den derzeitigen Fehlercode an.
Mögliche Werte	0: microSD-Karte OK 1: microSD-Karte voll 2: microSD-Karte nicht gesteckt 4: microSD-Karte hat Fehler (z. B. falsch formatiert)
Datenbreite	1 Byte
Datenpunkttyp / Datentyp	20.*/1-Byte
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 43: SD-Fehlercode

57 |	
Name	Aktiviere Datenlogger
Funktion	Aktiviert oder deaktiviert das Logging und zeigt auf Abfrage den Status an.
Mögliche Werte	0: Deaktivieren 1: Aktivieren
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.001/Schalten
Richtung	Schreiben
Flags (KLSÜAI)	KLS---

Tabelle 44: Aktiviere Datenlogger

© 2021 ise Individuelle Software und Elektronik GmbH

58 |	
Name	Datenlogger — Status
Funktion	Zeigt an, ob der Datenlogger derzeit Daten aufzeichnet.
Mögliche Werte	0: Nicht aktiv 1: Aktiv
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.002/Boolesch
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 45: Datenlogger – Status

59 |	
Name	SD-Karte — Speicherzustand
Funktion	Zeigt an, ob der Speicher der SD-Karte erschöpft ist.
Mögliche Werte	0: Nicht voll 1: Voll
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.002/Boolesch
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 46: SD-Karte Speicherzustand

60 |	
Name	SD-Karte — Speicherfüllstand
Funktion	Zeigt an, wie viel % des SD-Kartenspeichers belegt sind.
Mögliche Werte	0 bis 255 entspricht 0 bis 100 %
Datenbreite	1 Byte
Datenpunkttyp / Datentyp	5.001/Prozent (0…100 %)
Richtung	Lesen
Flags (KLSÜAI)	KL-Ü--

Tabelle 47: SD-Karte – Speicherfüllstand

© 2021 ise Individuelle Software und Elektronik GmbH

10.5 Benachrichtigungen

Die nachfolgenden Kommunikationsobjekte stellen fünf mögliche Datenpunkttypen zur Verfügung. Die Festlegung des Datenpunkttyps erfolgt durch die Auswahl der entsprechenden Parameter.

101…150	
Name	Benachrichtigung Auslöser Nr. 1/…/50
Funktion	Sendet eine Benachrichtigung an das SDA-Portal. Der boolesche Wert kann in der Benachrichtigung mitgesendet werden.
Mögliche Werte	0: Deaktivieren 1: Aktivieren
Datenbreite	1 Bit
Datenpunkttyp / Datentyp	1.001/Ein/Aus
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 48: Benachrichtigung Auslöser – Boolesch

101…150	
Name	Benachrichtigung Auslöser Nr. 1/…/50
Funktion	Sendet eine Benachrichtigung an das SDA-Portal. Der Prozentwert kann in der Benachrichtigung mitgesendet werden.
Mögliche Werte	0 bis 255 entspricht 0 bis 100 %
Datenbreite	1 Byte
Datenpunkttyp / Datentyp	5.001/Prozent (0…100%)
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 49: Benachrichtigung Auslöser – Prozent

© 2021 ise Individuelle Software und Elektronik GmbH

101…150	
Name	Benachrichtigung Auslöser Nr. 1/…/50
Funktion	Sendet eine Benachrichtigung an das SDA-Portal. Der Zählwert kann in der Benachrichtigung mitgesendet werden.
Mögliche Werte	0 bis 255
Datenbreite	1 Byte
Datenpunkttyp / Datentyp	5.010/Zählimpulse (0…255)
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 50: Benachrichtigung Auslöser – Zähler

101…150	
Name	Benachrichtigung Auslöser Nr. 1/…/50
Funktion	Sendet eine Benachrichtigung an das SDA-Portal. Der Fließkommawert kann in der Benachrichtigung mitgesendet werden.
Mögliche Werte	Liste von 2 Bytes getrennt durch Leerzeichen oder Komma
Datenbreite	2 Bytes
Datenpunkttyp / Datentyp	9.*/Fließkommawert
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 51: Benachrichtigung Auslöser – Fließkommawert

101…150	
Name	Benachrichtigung Auslöser Nr. 1/…/50
Funktion	Sendet eine Benachrichtigung an das SDA-Portal. Der Text kann in der Benachrichtigung mitgesendet werden.
Mögliche Werte	Frei wählbarer Text
Datenbreite	14 Bytes
Datenpunkttyp / Datentyp	16.001/Zeichen (ISO 8859-1)
Richtung	Schreiben
Flags (KLSÜAI)	K-S---

Tabelle 52: Benachrichtigung Auslöser – Text

© 2021 ise Individuelle Software und Elektronik GmbH

11 Fehlersuche

Fehlercodes werden auf der Gerätewebseite unter <<Gerätestatus>> ausgegeben.

Hat die Fehleranzeige den Wert <<False>>, sind keine Fehler aufgetreten.

Die Gerätewebseite wird nicht immer automatisch aktualisiert.
Nutzen Sie die Funktion Ihres Browsers zum Aktualisieren.

Weitere Informationen liefern Ihnen die LEDs des Geräts:

► Siehe LEDs beim Gerätestart, Seite 35.

► Siehe LEDs im Betrieb, Seite 36.

Lösungen zu angezeigten Fehlercodes und zu möglichen Konfigurationsfehlern finden Sie in der nachfolgenden Tabelle. Führen die nachfolgenden Lösungsansätze nicht zum Erfolg, überprüfen Sie die Konfiguration und den Status der Zugriffsgruppen im SDA-Portal und auf der Gerätewebseite.

Problem	Fehlerbehebung
Die COM-LED leuchtet nicht.	Prüfen Sie die KNX Verkabelung und die LED-Statusanzeigen gemäß Abschnitt “LEDs im Betrieb” auf Seite 36.
Die APP-LED leuchtet dauerhaft.	Prüfen Sie die generelle Freigabe des Portalzugriffs über die KNX Kommunikationsobjekte 1 und 2.
Die APP-LED blinkt gleichmäßig und langsam mit 1 Hz.	Prüfen Sie die Geräteparametrierung in der ETS gemäß Kapitel “Gerät in der ETS anlegen” auf Seite 38.
Das Gerät ist in der Windows-Netzwerkumgebung nicht sichtbar.	Prüfen Sie die Netzwerkverkabelung und die Parametrierung der Geräte-IP in der ETS gemäß Abschnitt “IP-Adresse, IP-Subnetzmaske und Standardgateway-Adresse einstellen” auf Seite 40.
Das Gerät wird im SDA-Portal als offline angezeigt.	Prüfen Sie die Verbindung zum Internet. Falls Sie kein DHCP benutzen, überprüfen Sie den angegebenen DNS-Server. Beachten Sie die Gerätewebseite für weitere Fehlerinformationen. Ergab die Überprüfung keine Störungen, starten Sie das Gerät über die Gerätewebseite neu.

Tabelle 53: Fehlerbehebung

© 2021 ise Individuelle Software und Elektronik GmbH

11.1 Logdateien generieren

Mit Hilfe von Logdateien bekommt der Support Informationen, um Ihre Problemstellung zu analysieren. Diese Logdateien generieren Sie über die Gerätewebseite und laden diese als ZIP-Datei herunter.

Den Umfang der in den Logdateien enthaltenen Informationen konfigurieren Sie durch den Logging-Modus.

Logging-Modus umstellen

Voraussetzung: Die Gerätewebseite ist geöffnet.

1. Wählen Sie auf der Seite <<Gerätestatus>> im Bereich <<Systemkonfiguration>> die entsprechende Schaltfläche beim <<Logging-Modus>>.

<<Einfach>>	Basisinformationen werden gesammelt.
<<Erweitert>>	Umfängliche Informationen werden gesammelt.

> Der Logging-Modus <<Erweitert>> beeinflusst die Performance negativ. Schalten Sie diesen Modus nur ein, wenn der Support die erweiterten Logdateien anfordert. Schalten Sie den Modus wieder aus, sobald Sie die Logdateien generiert haben.

2. Bestätigen Sie die Sicherheitsabfrage.

Logdateien generieren

Voraussetzung: Die Gerätewebseite ist geöffnet. Ggf. bittet Sie unser Support darum, den Logging-Modus zu konfigurieren.

1. Wählen Sie in der Menüleiste <<System>> → <<Logdatei herunterladen>>.

Die Logdateien werden erstellt und als ZIP-Datei heruntergeladen.

© 2021 ise Individuelle Software und Elektronik GmbH

11.2 Support kontaktieren

Wenn Sie ein Problem mit Ihrem SMART CONNECT KNX Remote Access haben und Support benötigen, kontaktieren Sie uns:

- E-Mail an support@ise.de
- Rufen Sie uns an unter Tel.: +49 441 680 06 12
- Faxen Sie uns: +49 441 680 06 15

Folgende Daten benötigen wir, damit wir Ihnen helfen können:

- Zur Identifikation des Geräts: Name des Produkts oder Bestellnummer
- Registration ID
- MAC-Adresse (optional)
- Version des Produktdatenbankeintrags
- Version der Firmware
- ETS-Version
- Aussagekräftige Fehlerbeschreibung inklusive Fehlercode (falls vorhanden)

Gerne auch:

- Logdateien
- Screenshot von <<Gerätestatus>> auf der Gerätewebseite

© 2021 ise Individuelle Software und Elektronik GmbH

11.3 FAQ – Häufig gestellte Fragen

Wie finde ich die IP-Adresse meines SMART CONNECT KNX Remote Access?

Sie finden die IP-Adresse auf der Gerätewebseite, siehe “Gerätewebseite: Startseite aufrufen” auf Seite 29.

Wie viel Internet-Datenverkehr (Traffic) entsteht, wenn ich den SMART CONNECT KNX Remote Access mit dem SDA-Portal verbunden habe?

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

Welchen Kommunikationskanal benutzt der SMART CONNECT KNX Remote Access zum SDA-Portal?

Der SMART CONNECT KNX Remote Access kommuniziert mit dem SDA-Portal ausschließlich über eine HTTPS Verbindung über den Standardport 443. Über diese eine Verbindung werden in beide Richtungen alle Daten ausgetauscht, sodass i. d. R. keine Konfiguration in der Firewall notwendig ist. Möchten Sie den Netzwerkzugriff auf bestimmte Domains und Ports bzw. IP-Adressen beschränken, empfehlen wir Ausnahmen zu konfigurieren. Auf https://securedeviceaccess.net finden Sie eine Übersicht, mit den SDA-relevanten Domains, Ports und IP-Adressen.

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

Für die Absicherung der Zugriffe und der Verbindung werden von Secure Device Access Cookies benutzt. Es erfolgt kein Tracking. Ein Austausch mit Dritten erfolgt nur bei Verknüpfung von Benutzerkonten mit Drittanbietern.

Gibt es Software-Updates für meinen SMART CONNECT KNX Remote Access?

Informationen zu Software-Updates finden Sie unter “Firmware aktualisieren” auf Seite 45.

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?

Lesen Sie hierzu den Eingangshinweis unter “Kommunikationsobjekte” auf Seite 63.

Wie kann ich die drei physikalischen Adressen der KNX/IP-ETS-Schnittstellen (Tunnelling Server) im ETS-Projekt konfigurieren?

Lesen Sie hierzu den Abschnitt “Tunneling Server” auf Seite 42.

© 2021 ise Individuelle Software und Elektronik GmbH

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 SMART CONNECT KNX Remote Access auch über das Internet sicher erreichbar?

Ja, die Gerätewebseite kann über das Internet gesichert abgerufen werden.

Warum wird die Gerätewebseite meines SMART CONNECT KNX Remote Access nicht angezeigt?

Der verwendete Browser wird nicht unterstützt oder die Version des Browsers wird nicht unterstützt.

Wir unterstützen die marktüblichen, aktuellen Browser wie bspw. Google Chrome, Microsoft Edge und Mozilla Firefox mindestens in der aktuellen Version (Stand dieser Dokumentation). Wir empfehlen Ihnen aber aus Sicherheitsgründen Ihren Browser stets aktuell zu halten.

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. Nur wenn Sie die aktuellste Version der ETS benutzen, können wir die volle Leistungsfähigkeit des SMART CONNECT KNX Remote Access sicherstellen.

Ist der SDA-Portalserver wirklich nötig?

Es gibt heute noch 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 aufwendig konfiguriert werden muss.

Welche Daten speichert der Server?

Der Server speichert nur die für die Erbringung des Dienstes absolut notwendigen Daten. Dazu gehören, neben den von Ihnen bei der Anmeldung angegebenen und über die Benutzeroberfläche einsehbaren Daten, 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 die restriktive Datenschutz-Grundverordnung (DSGVO).

Warum schließt die Lizenz einen Dauerbetrieb (24x7) aus und enthält eine Datenvolumenbegrenzung?

Da alle Daten über den SDA-Portalserver 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 gerne. Lizenzmodelle mit erweitertem Umfang sind für die Zukunft nicht ausgeschlossen.

© 2021 ise Individuelle Software und Elektronik GmbH

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

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

Warum sehe ich nach dem Entladen der Applikation auf der Gerätewebseite noch die vorher konfigurierten IP- und physikalischen Adressen?

Die Gerätewebseite wird nach dem Entladen erst nach einem erneuten Laden der Seite aktualisiert.

© 2021 ise Individuelle Software und Elektronik GmbH

12 Demontage und Entsorgung

Wenn Sie das Gerät, beispielsweise aufgrund eines Defekts, demontieren möchten, gehen Sie in umgekehrter Reihenfolge wie bei der Montage vor.

Abdeckkappe entfernen

Warnung

Gefahr durch unsachgemäße Verwendung

Bei unsachgemäßer Verwendung können Schäden am Gerät, Brand oder andere Gefahren entstehen.

- Einbau und Demontage elektrischer Geräte nur durch Elektrofachkräfte.
- Beachten Sie die Anleitungen in diesem Produkthandbuch.

Warnung

Gefahr durch elektrischen Schlag

Elektrischer Schlag bei Berühren spannungsführender Teile in der Einbauumgebung. Elektrischer Schlag kann zum Tode führen.

- Gerät freischalten.
- Spannungsführende Teile in der Umgebung abdecken.

1. Drücken Sie die Abdeckkappe seitlich leicht ein (siehe Abbildung 32, Pos. 1).
2. Ziehen Sie die Abdeckkappe nach oben ab (siehe Abbildung 32, Pos. 2).

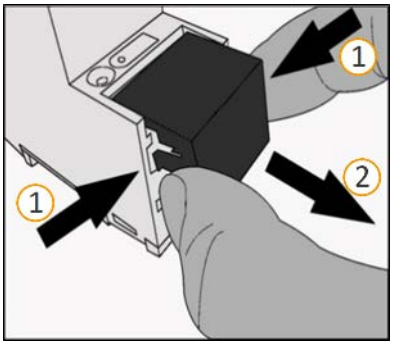


Abbildung 32: Abdeckkappe entfernen

© 2021 ise Individuelle Software und Elektronik GmbH

Gerät von Hutschiene lösen

Voraussetzung: Spannungsversorgung, Busleitung und Netzwerkanschluss sind abgeklemmt.

1. Führen Sie einen Schraubendreher (siehe Abbildung 33, Pos. 1) in den Lösehebel (siehe Abbildung 33, Pos. 2) und schieben Sie den Lösehebel nach unten (siehe Abbildung 33, Pos. 3).

2. Nehmen Sie das Gerät von der Hutschiene.

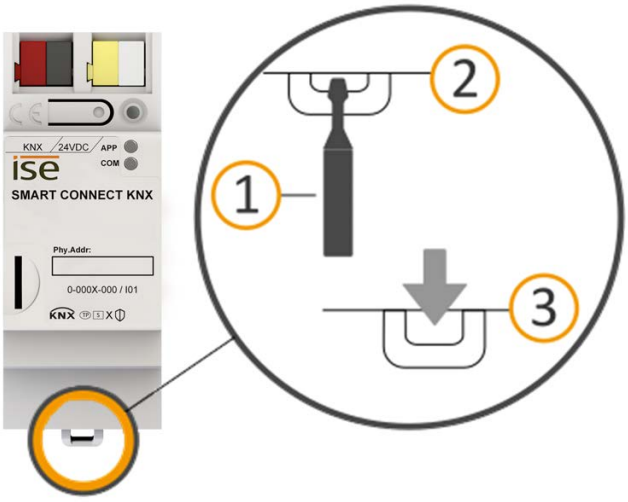


Abbildung 33: Gerät von Hutschiene lösen

Entsorgung

Tragen Sie bitte aktiv zum Erhalt unserer Umwelt bei, indem Sie alle Materialien umweltgerecht entsorgen.

Verpackung und Karton

Entsorgen Sie das Verpackungsmaterial in die Sammelbehälter für Pappe, Papier und Kunststoffe.

Gerät

Altgeräte dürfen nicht mit dem Hausmüll entsorgt werden!

Sie können Ihr Altgerät kostenlos an ausgewiesene Rücknahmestellen oder ggf. an Ihren Fachhändler abgeben. Einzelheiten über die Rücknahme erhalten Sie von Ihrer örtlichen Verwaltung.

© 2021 ise Individuelle Software und Elektronik GmbH

13 Glossar

Authentifizierungsschlüssel

Wird durch eine Software (z. B. eine Visualisierung) eine SDA-Verbindung geöffnet, muss sich die Software gegenüber dem SDA-Portal authentifizieren. Dazu wird von einem Benutzer im SDA-Portal ein Authentifizierungsschlüssel angelegt, welcher die Anmeldedaten des Benutzers (E-Mail und Passwort) ersetzt.

Benutzerrolle, Rolle

Ein Portalbenutzer hat bezogen auf einen für ihn freigegebenen SMART CONNECT KNX Remote Access eine der folgenden Rollen:

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

Der „Eigentümer“ (englisch „Owner“) eines SMART CONNECT KNX Remote Access ist die rechtlich verantwortliche Person. Die Rechte des Eigentümers sind identisch mit denen des Administrators. Jeder mit einem Portalkonto verknüpfte SMART CONNECT KNX Remote Access hat genau einen Eigentümer. Per „Schlüsselübergabe“ kann der Eigentümer geändert werden.

Datenvolumen, Traffic

Bezeichnet die über den SDA-Portalserver übertragene Nutzdatenmenge. In unterschiedlichen Anwendungen werden stark unterschiedlich viele Daten übertragen. KNX Kommunikation verursacht wenig, ein Livestream von einer Webcam verursacht hingegen viel Datenvolumen. Die übertragene Datenmenge belastet den SDA-Portalserver. Das Übertragungsvolumen ist pro Monat und SMART CONNECT KNX Remote Access auf maximal 2 GB beschränkt. Siehe “Maximal zulässiges Übertragungsvolumen” auf Seite 90.

DPT, DP-Typ, Datenpunkttyp

Der Datenpunkttyp ist die standardisierte Codierung der über Gruppentelegramme übertragenen Daten.

Entferntes Netzwerk

Als entferntes Netzwerk wird das Netzwerk bezeichnet, in dem sich der SMART CONNECT KNX Remote Access befindet.

ETS (Engineering Tool Software)

Projektiert wird das Gerät in der Software ETS. Die ETS ist in unterschiedlichem Funktionsumfang über die KNX Association (www.knx.org) erhältlich.

FDSK (Factory Default Setup Key, Fabrikschlüssel)

Der FDSK ist Bestandteil des KNX Secure-Zertifikats und dient einer sicheren Kommunikation von Geräten der Kategorie „KNX IP Secure Gerät“. Durch Kombination von FDSK und Seriennummer des Geräts kann dieses eindeutig identifiziert werden. Zusammen bilden sie das Gerätezertifikat.
Je nach Anwendungsfall wird das Zertifikat für die erste Authentifizierung in der ETS oder für die Verschlüsselung der Kommunikation benötigt.

Das KNX Secure-Zertifikat ist auf einem Aufkleber an der Geräteseite aufgedruckt. Ein zweiter Aufkleber wird dem Produkt beigelegt.

© 2021 ise Individuelle Software und Elektronik GmbH

Fernzugriff

Gesicherter Zugriff über den SDA-Portalserver und einen SMART CONNECT KNX Remote Access auf ein Gerät im Heimnetzwerk.

Fernzugriffs-ID

Die Fernzugriffs-ID ist eine verkürzte Variante der Registration ID und besteht aus deren ersten beiden Blöcken.

Firmware

Software, die auf der Gerätehardware eingebettet ist und zum Betrieb des Geräts dient. Funktionserweiterungen für das Gerät erhalten Sie über eine neue Firmwareversion.

Flags (KLSÜAI)

Jedes Kommunikationsobjekt hat so genannte Flags, mit denen das Kommunikationsobjekt Methoden erhält: K=Kommunikation, L=Lesen, S=Schreiben, Ü=Übertragen, A=Aktualisieren, I=Initialisieren.

Gerätewebseite

Applikation zur Überprüfung des Gerätestatus, Einspielung von Aktualisierungen und Anzeige von Geräteinformationen.

Gesicherte Verbindung

Bezeichnet eine verschlüsselte und beidseitig authentifizierte Kommunikationsverbindung zwischen zwei Kommunikationspartnern.

Heimnetzwerk

Computernetzwerk (Ethernet) in Ihrem Zuhause. Über das Heimnetzwerk sind Ihre Netzwerkgeräte mit dem SMART CONNECT KNX Remote Access verbunden.

httpaccess.net

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

Katalog

Kurzform für „KNX Online-Produktkatalog“. Der Katalog ist eine Produktdatenbank. Der Katalog enthält die von/bei der KNX zertifizierten bzw. registrierten Geräte. Die Daten zu einem Gerät sind als Produktdatenbankeintrag gespeichert.

Lokales Netzwerk

Als lokales Netzwerk wird das Netzwerk bezeichnet, in dem sich der PC befindet, mit dem über SDA auf ein Gerät im entfernten Netzwerk zugegriffen wird. Der Zugriff erfolgt entweder über das SDA-Portal oder den SDA-Client.

Netzwerkgerät

Ein im Heimnetzwerk eingebautes Gerät mit IP- oder TP-Anschluss, auf das über SDA zugegriffen wird.

© 2021 ise Individuelle Software und Elektronik GmbH

Portal Login

Zugriff auf Geräte hinter einem SMART CONNECT KNX Remote Access mit Portalanmeldung. Portal Login ist das Gegenstück zum Quick Connect.

SDA-Portalserver

Zentraler Server der SDA-Infrastruktur zur Zugriffsverwaltung des SMART CONNECT KNX Remote Access.
Wir betreiben den Server in Deutschland unter Einhaltung der strengen europäischen Datenschutzrichtlinien. Erreichbar unter https://securedeviceaccess.net.

Produktdatenbankeintrag (auch Katalogeintrag)

Daten zu einem Gerät im „Online KNX Produkt Katalog“ der ETS. Der Produktdatenbankeintrag enthält alle Daten, um das Gerät in der ETS projektieren zu können. Der Produktdatenbankeintrag wird in Form einer Datei von den Herstellern der Geräte bereitgestellt. Die neueste Version von Produktdatenbankeinträgen der ise Individuelle Software und Elektronik GmbH können Sie kostenfrei auf unserer Webseite www.ise.de herunterladen.

Der Produktdatenbankeintrag wird häufig auch als „Katalogeintrag“ bezeichnet.

Quick Connect

Zugriff auf Geräte hinter einem SMART CONNECT KNX Remote Access ohne Portalanmeldung, durch Eingabe der Registration ID.

Registration ID

Jeder SMART CONNECT KNX Remote Access hat eine eindeutige Registration ID (früher Connector ID), welche auf einem Aufkleber an der Geräteseite aufgedruckt ist. Die Registration ID dient dem sicheren Zugriff ohne Portalanmeldung (Quick Connect) und der Verknüpfung eines SMART CONNECT KNX Remote Access mit einem Portalkonto. Ein zweiter Aufkleber wird dem Produkt beigelegt.

Schlüsselübergabe

Bezeichnet die Funktion des SDA-Portalservers, den Eigentümer eines SMART CONNECT KNX Remote Access zu ändern. Dieser Fall tritt regelmäßig auf, wenn eine neue Gebäudeinstallation vom Errichter an den Bauherren übergeben wird, deshalb der Name „Schlüsselübergabe“.

Secure Device Access, SDA

Bezeichnet das komplette System, welches den sicheren Zugriff über das Internet auf Ihr Zuhause bereitstellt.

SDA-Benachrichtigungen

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

SDA-Client

PC-Software, die anderen Anwendungen die Kommunikation über SDA erlaubt.

© 2021 ise Individuelle Software und Elektronik GmbH

SDA-Connector

KNX Gateway zur Verbindung des Heimnetzwerks mit dem Portalserver, um Fernzugriff zu ermöglichen. SMART CONNECT KNX Remote Access und SDA-Connector werden synonym verwendet.

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.

Updates

Informationen zu neuen Versionen der Firmware finden Sie in dieser Dokumentation unter dem Suchbegriff „Aktualisierung“.

Webseite

Informationen zur Applikation des Geräts finden Sie in dieser Dokumentation unter dem Suchbegriff „Gerätewebseite“.

Zugriffsgruppen

Über den SDA-Portalserver können für den SMART CONNECT KNX Remote Access Personen freigegeben werden. Über die Einteilung in Zugriffsgruppen kann z. B. über KNX Taster der Zugriff getrennt erlaubt oder verboten werden. Der Zugriff ist für beide Gruppen standardmäßig freigeschaltet.

Bewohner: Zugriffsgruppe für Hausbewohner.

Installateur: Zugriffsgruppe für externe Dienstleister.

© 2021 ise Individuelle Software und Elektronik GmbH

14 Lizenzvertrag SMART CONNECT KNX Remote Access

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

14.1 Definitionen

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

Lizenznehmer: Der rechtmäßige Empfänger der SMART CONNECT KNX Remote Access-Software.

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

SMART CONNECT KNX Remote Access: Als SMART CONNECT KNX Remote Access-Software wird die gesamte Software inklusive der Betriebsdaten bezeichnet, die für das Produkt SMART CONNECT KNX Remote Access zur Verfügung gestellt wird. Dies sind insbesondere die Firmware und die Produktdatenbank.

14.2 Vertragsgegenstand

Gegenstand dieses Vertrags ist die auf Datenträger oder durch Download bereitgestellte SMART CONNECT KNX Remote Access-Software, die SDA-Client-Software, die zur Verfügungstellung des SDA-Portals sowie die zugehörige Dokumentation in schriftlicher oder elektronischer Form.

14.3 Rechte zur Software-Nutzung

14.3.1 Firmware und SDA-Client

Der Lizenzgeber räumt dem Lizenznehmer das nicht ausschließliche, zeitlich unbegrenzte und nicht übertragbare Recht ein, die SMART CONNECT KNX Remote Access-Software gemäß den nachstehenden Bedingungen für die in der gültigen Fassung der Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) genannten Zwecke und Anwendungsbereiche zu nutzen.

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

14.3.2 Secure Device Access Portal

Der Lizenzgeber stellt dem Lizenznehmer für die Nutzung mit der Firmware und dem SDA-Client einen Secure Device Access Portalserver unter https://securedeviceaccess.net zur Verfügung. Hierzu nutzt er derzeit die Dienstleistung der ise Individuelle Software und Elektronik GmbH. Der Lizenzgeber kann aus wichtigem Grund den Betrieb des SDA-Portalservers mit einer Frist von 5 Jahren kündigen. Der Lizenzgeber muss in diesem Fall auf Anfrage des Lizenznehmers die SDA-Portalsoftware dem Lizenznehmer im Quellcode zugänglich machen, um ihm ein eigenes Hosting der Serversorftware und damit eine fortlaufende Nutzung von SDA zu ermöglichen.

© 2021 ise Individuelle Software und Elektronik GmbH

14.4 Beschränkung der Nutzungsrechte

14.4.1 Maximal zulässiges Übertragungsvolumen

Die Lizenz schließt die Nutzung des Fernzugriffs im Dauerbetrieb aus, z. B. für Visualisierung oder Standortvernetzung. Der Lizenzgeber betrachtet wiederholte ununterbrochene Nutzung von mehr als 12 Stunden am Stück als Dauernutzung.
Das Übertragungsvolumen ist pro Monat und SMART CONNECT KNX Remote Access auf maximal 2 GB beschränkt.
Der Lizenzgeber behält sich vor, die o. g. Nutzungsgrenzen durch technische Maßnahmen durchzusetzen.

14.4.2 Kopieren, Bearbeiten oder Übertragen

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

14.4.3 Reverse-Engineering oder Umwandlungstechniken

Der Lizenznehmer ist nicht berechtigt, Reverse-Engineering Techniken auf die SMART CONNECT KNX Remote Access-Software anzuwenden oder die SMART CONNECT KNX Remote Access-Software in eine andere Form umzuwandeln. Zu solchen Techniken gehört insbesondere das Disassemblieren (Umwandlung binär kodierter Maschinenbefehle eines ausführbaren Programms in eine für Menschen lesbarere Assemblersprache) oder Dekompilieren (Umwandlung binär kodierter Maschinenbefehle oder Assemblerbefehle in Quellcode in Form von Hochsprachenbefehlen).

14.4.4 Die Firmware und Hardware

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

14.4.5 Weitergabe an Dritte

Die SMART CONNECT KNX Remote Access-Software darf nicht an Dritte weitergegeben oder Dritten zugänglich gemacht werden.

14.4.6 Vermieten, Verleasen oder Unterlizenzen

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

14.4.7 Software-Erstellung

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

14.4.8 Die Mechanismen des Lizenzmanagements und des Kopierschutzes

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

© 2021 ise Individuelle Software und Elektronik GmbH

14.5 Eigentum und Geheimhaltung

14.5.1 Dokumentation

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

14.5.2 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.

14.6 Änderungen und Nachlieferungen

Die SMART CONNECT KNX Remote Access-Software und die Dokumentation (die in gedruckter Form oder aber auch als Onlinehilfe bzw. Onlinedokumentation zur Verfügung gestellt wird) unterliegen eventuell Änderungen durch den Lizenzgeber. Die aktuellsten Stände von Software und Dokumentation finden Sie auf www.ise.de.

14.7 Gewährleistung

Die SMART CONNECT KNX Remote Access-Software wird zusammen mit der Software von Dritten ausgeliefert. Für die Software Dritter wird keinerlei Gewährleistung übernommen. Für weitere Informationen ► siehe Open-Source-Software, S.93.

14.7.1 Software und Dokumentation

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

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

Die Erfüllung der Gewährleistung erfolgt durch Ersatzlieferung.

14.7.2 Gewährleistungsbeschränkung

Im Übrigen wird für die Fehlerfreiheit der SMART CONNECT KNX Remote Access-Software und ihrer Datenstrukturen keine Gewährleistung übernommen. Die Gewährleistung erstreckt sich auch nicht auf Mängel, die auf unsachgemäße Behandlung oder andere Ursachen außerhalb des Einflussbereichs des Lizenzgebers zurückzuführen sind. Weitere Gewährleistungsansprüche sind ausgeschlossen.

© 2021 ise Individuelle Software und Elektronik GmbH

14.8 Haftung

Der Lizenzgeber ist nicht haftbar für Schäden aus entgangenem Gewinn, Verlust von Daten oder anderem finanziellen Verlust, die im Rahmen der Benutzung der SMART CONNECT KNX Remote Access-Software entstehen, selbst wenn der Lizenzgeber von der Möglichkeit eines solchen Schadens Kenntnis hat.

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

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

14.9 Anwendbares Recht

Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.
Gerichtsstand ist Oldenburg (Oldb).

14.10 Beendigung

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

Mit Beendigung des Vertrags erlischt die Lizenz zur Nutzung der SMART CONNECT KNX Remote Access-Software. Das Produkt SMART CONNECT KNX Remote Access muss in diesem Fall außer Betrieb genommen werden. Eine weitere Nutzung des SMART CONNECT KNX Remote Access ohne Lizenz ist ausgeschlossen.

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

14.11 Nebenabreden und Vertragsänderungen

Nebenabreden und Vertragsänderungen bedürfen zu ihrer Gültigkeit der Schriftform.

14.12 Ausnahme

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

© 2021 ise Individuelle Software und Elektronik GmbH

15 Open-Source-Software

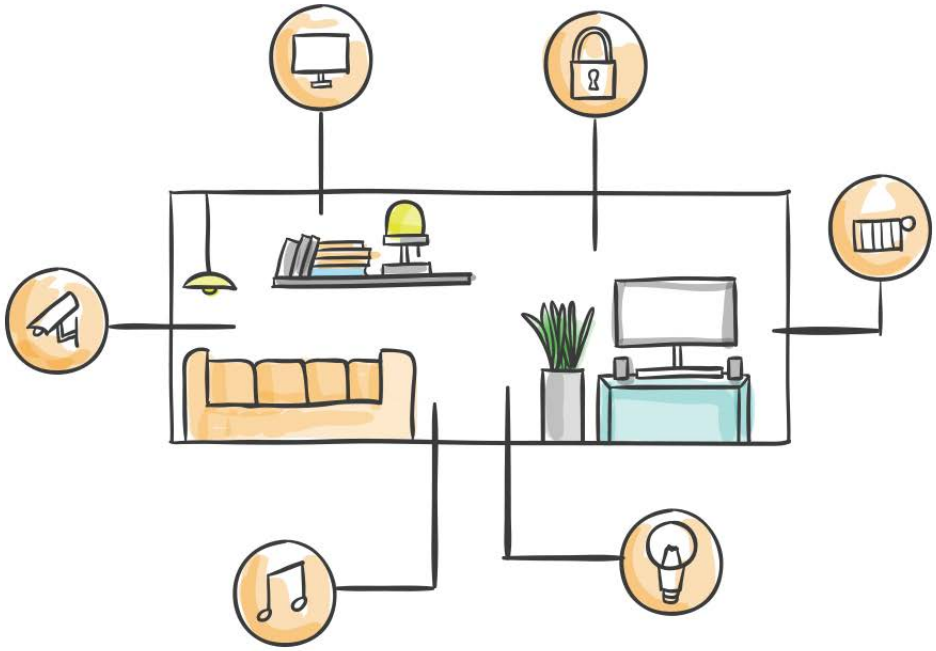
Dieses Produkt verwendet Software aus dritten Quellen, die im Rahmen von unterschiedlichen Open-Source-Lizenzen veröffentlicht sind.

Die einzelnen verwendeten Software-Pakete sowie deren Lizenzen werden auf der Gerätewebseite dieses Produkts unter <<System>> → <<Lizenzen>> aufgeführt und beschrieben.

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

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

© 2021 ise Individuelle Software und Elektronik GmbH



ise Individuelle Software und Elektronik GmbH
Osterstraße 15
26122 Oldenburg, Deutschland

Telefon: +49 441 680 06 11
Fax: +49 441 680 06 15
E-Mail: vertrieb@ise.de