HANDBUCH

V 1.3

ISONA – Secure Automation Tablet-OTP (SAT)

Inhaltsverzeichnis

1. Allgemeines

Die vorliegende Dokumentation beschreibt die Einsatzbereiche und die Handhabung des ISONA Secure Automation Tablet-OTP (SAT) sowie die erforderlichen Schritte zur Installation der VPN-Apps auf den Tablets (iPad und Android-Tablet). Die Bilder (Screenshots) in diesem Handbuch können von den aktuellen Screens abweichen, bedingt durch Weiterentwicklungen an den Apps bzw. an den Betriebssystemen IOS und Android.
Zusätzlich zu anderen Einsatzbereichen, ist das ISONA Secure Automation Tablet-OTP (SAT) eine ideale Ergänzung zum ISONA Automation Terminalserver. Auf dem Terminalserver installiert man dazu alle Windows-Programme, die man im Zusammenhang mit Steuerungen usw. benötigt und kann dann mit dem Tablet auf sämtliche Anlagen und Applikationen zugreifen.

Für die sichere Zwei-Faktor-Authentisierung des Benutzers am ISONA Secure Automation Gateway (zentrales VPN-Gateway) via Tablet gibt es zwei Artikelvarianten des Secure Automation Tablet-OTP (SAT):

1) Artikelnummer A-SAT: bei dieser Variante kann man über den mitgelieferten OTP-Token (**O**ne**T**ime**P**assword) auf Knopfdruck ein Einmalkennwort generieren, womit sich der Benutzer dann anmeldet.
2) Artikelnummer A-SAT-2: bei dieser Variante kann man, je nach Anforderung im Projekt, das Einmalkennwort über verschiedene Wege erzeugen bzw. sich zusenden lassen:
   a) über eine entsprechende App auf dem Smartphone oder Tablet, z.B. Google Authenticator App. Diese App muss vor der ersten Anwendung mittels eines QR-Codes initialisiert werden. Danach erzeugt die App auf Knopfdruck ein Einmalkennwort direkt auf dem Gerät (funktioniert auch ohne aktive Mobilfunkverbindung).
   b) das Einmalkennwort wird über SMS oder E-Mail an den Benutzer übermittelt.

2. Installation des VPN-Clients auf Tablets/Smartphones

Für den Zugriff auf Anlagenvisualisierungen, PCs usw. muss auf dem Tablet vor dem ersten Gebrauch ein VPN-Profil angelegt werden. Dies erfolgt über einen Link in einem ISONA Automation WebCenter (Webportal).
Die Vorgehensweise bei der VPN-Client Installation auf einem Tablet variiert je nach Betriebssystem (IOS, Android) und ist nachfolgend detailliert beschrieben.
In der CD-Box des Secure Automation Tablet-OTP (SAT) finden Sie üblicherweise ein Einlegeblatt mit Ihren persönlichen Zugangsdaten und die Internetadresse des für Sie relevanten Webportals. Falls Ihnen diese Daten nicht vorliegen, wenden Sie sich an den Administrator.

2.1 Installation des VPN-Clients auf einem iPad/iPhone

Es gibt zwei verschiedene VPN-Clientvarianten auf den iPads/iPhones, die in den beiden folgenden Kapiteln beschrieben sind.

2.1.1 Installation des Standard VPN-Clients beim iPad/iPhone

Rufen Sie die auf dem Einlageblatt vermerkte Internetadresse mit einem Browser auf Ihrem iPad auf und melden sich mit Ihren Zugangsdaten am Webportal an. Falls Ihnen keine Zugangsdaten vorliegen, wenden Sie sich an ihren Administrator.
Wenn Sie sich erfolgreich am Webportal angemeldet haben, wählen Sie den Menüpunkt „Konto“:

Abb.: Ansicht der Webseite „Konto“ am Beispiel des ISONA Demoportals (Abb. ähnlich)

Hier klickt man auf den Link „VPN-Profil auf iPhone / iPad installieren“ und es öffnet sich das folgende „Profil installieren“-Fenster:

Abb.: „Profil installieren“ Fenster (Abb. ähnlich)

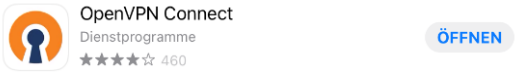
Klicken Sie hier auf den Button „Installieren“, um das iPad/iPhone für VPN zu konfigurieren. Event. erscheinen noch Warnmeldungen, die Sie immer mit „weiter“ quittieren müssen. Wenn bei dem Gerät eine Codesperre eingerichtet ist, dann muss in einem weiteren Fenster der Code eingegeben werden, bevor das VPN-Profil installiert werden kann. Ein letztes Fenster zeigt die erfolgreiche VPN-Installation an, dort auf den Button „Fertig“ klicken.

Wenn man überprüfen möchte, ob und welche Profile installiert wurden, wählt man in der App „Einstellungen“ den Menüpunkt „Allgemein“ und dort den Untermenüpunkt „Profile“ aus. Hier erhält man eine Liste aller auf dem Gerät installierten VPN-Profile und Zertifikate mit Detailinfos zu diesen Objekten.

Wichtig: Bitte melden Sie sich nach der erfolgreichen Tablet-Konfiguration am Webportal über den Button „Abmelden“ ab!

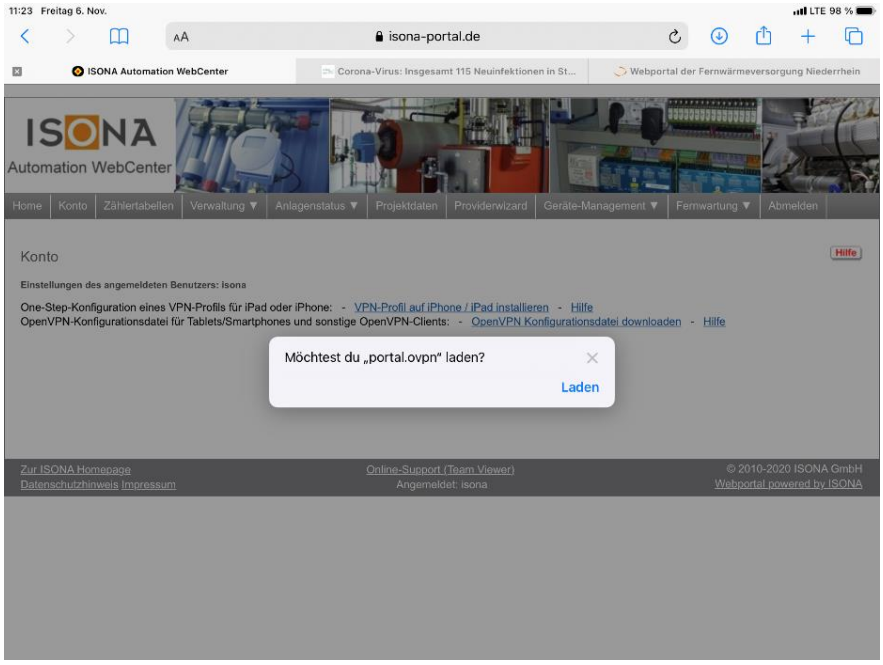
2.1.2 Installation des OpenVPN-Clients beim iPad/iPhone

Zuerst muss auf dem Gerät über den App-Store die Original OpenVPN-App installiert werden:

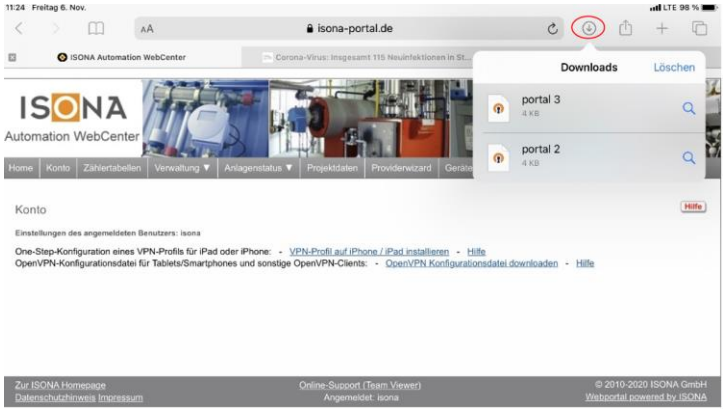


Danach öffnet man im Browser das ISONA Automation WebCenter (Webportal), loggt sich ein und klickt auf den Menüpunkt „Konto“ (Abb. ähnlich):

Hier klickt man auf den Link (in obigem Bild rot markiert), worauf folgende Abfrage erscheint:



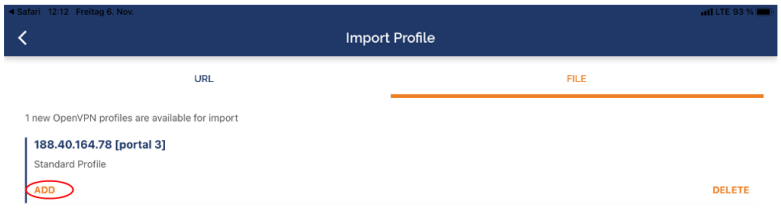
Jetzt klickt man auf „Laden“ und danach auf das Download-Symbol des Browsers:



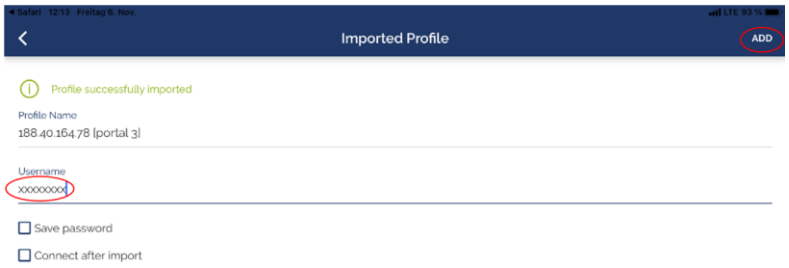
Hier klickt man auf den gewünschten Eintrag (OpenVPN Datei) und in dem folgenden Fenster auf den rot markierten Link:

Jetzt auf das OpenVPN-Symbol klicken, um die Datei in die OpenVPN-App zu verschieben und die App aufzurufen:

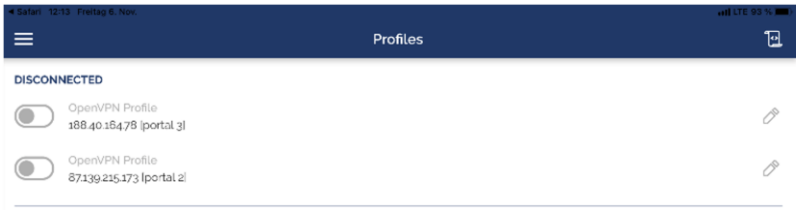
In dem sich öffnenden OpenVPN App-Fenster auf „ADD“ klicken:



Danach muss die Meldung Profile successfully imported erscheinen. In das Feld „Username“ trägt man einen beliebigen Benutzernamen ein und klickt dann auf „ADD“, um das Profil der OpenVPN-App hinzuzufügen:



Jetzt ist die Konfiguration des OpenVPN Clients abgeschlossen und das in der OpenVPN App angelegte Profil (event. auch mehrere Profile) wird angezeigt:



2.2 Installation des OpenVPN-Clients auf Android-Tablets/-Smartphones

Öffnen Sie die auf dem Einlageblatt der DVD-Box vermerkte Internetadresse auf einem Windows PC o.ä. und melden sich mit Ihren Zugangsdaten an. Dieser Anmeldevorgang mit dem OTP-Token ist auf der Anmelde-Webseite ausführlich in der Hilfe beschrieben.
Wenn Sie sich erfolgreich am Webportal angemeldet haben, klicken Sie auf den Menüpunkt „Konto“:

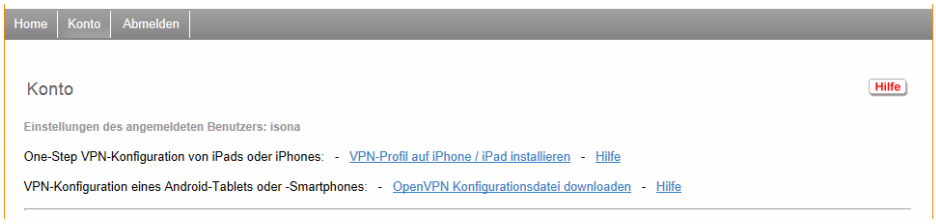


Abb.: Ansicht der Webseite „Konto“ am Beispiel des ISONA Demoportals (Abb. ähnlich)

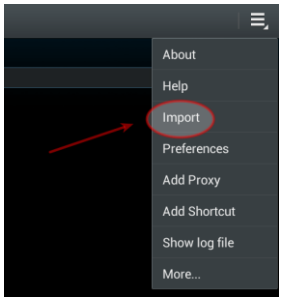
Hier klickt man auf den Link „OpenVPN Konfigurationsdatei downloaden“ und speichert diese .ovpn-Datei (Dateiname: portal.ovpn) z.B. auf einem USB-Stick ab, um sie dann auf das Tablet zu übertragen. Oder man

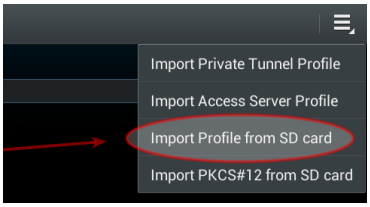
sendet die .ovpn-Datei an eine E-Mailadresse, die man dann auf dem Tablet aufruft und die angehängte Datei lokal abspeichert.

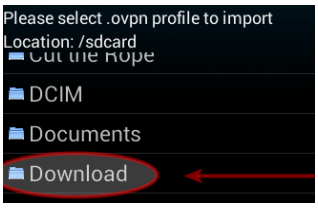
Auf dem Android-Tablet muss die App „OpenVPN Connect“ (von OpenVPN Technologies, siehe Google Play Store) installiert sein. Diese App starten, um das VPN zu konfigurieren:

Dann ruft man in der App die Einstellungen auf:

In diesem Menü wählt man „Import“:







Dann wählt man den Speicherort aus, wo man die .ovpn-Datei (Dateiname: portal.ovpn) abgespeichert hat und importiert diese. Der VPN-Client ist damit fertig konfiguriert.

Wichtig: Bitte melden Sie sich nach der erfolgreichen Tablet-Konfiguration am Webportal über den Button „Abmelden“ ab!

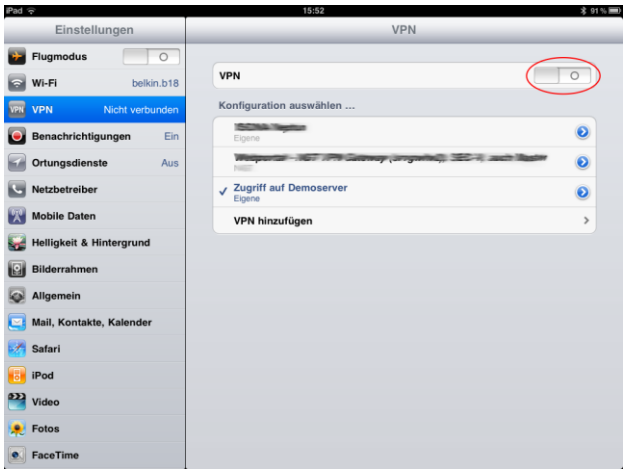
3. Start eines VPN-Profils beim iPad/iPhone

Für den Zugriff auf eine Anlagenvisualisierung o.ä. muss zuerst der VPN-Tunnel auf dem iPad/iPhone gestartet werden. Dabei zuerst sicherstellen, dass das Gerät Zugang zum Internet hat. Wenn der VPN-Tunnel aufgebaut ist, kann die jeweils benötigte App aufgerufen werden, die dann diesen VPN-Tunnel benutzt um auf die Anlagenvisualisierung o.ä. zuzugreifen.
Es gibt beim iPad/iPhone zwei Möglichkeiten, um einen VPN-Tunnel aufzubauen:

a) mit dem in den Geräten integrierten VPN-Client, der über das IPsec-Protokoll einen VPN-Tunnel zum ISONA Secure Automation Gateway (VPN-Gateway) aufbaut.
b) über eine zu installierende OpenVPN-App, die über OpenSSL einen VPN-Tunnel zum ISONA Secure Automation Gateway (VPN-Gateway) aufbaut.

3.1 Standard VPN-Tunnel (IPsec) auf dem iPad/iPhone starten

Zuerst ruft man die „Einstellungen“ auf und wählt den Menüpunkt „VPN“. Sind mehrere VPN-Profile auf dem Gerät eingerichtet, wählt man das gewünschte Profil aus (Häkchen setzen) und startet dann das VPN über den Button (im Bild rot markiert):



Jetzt erscheint ein Eingabefeld für das Kennwort und je nach Einstellung im SAG zusätzlich noch ein Eingabefeld für das Einmalkennwort (per OTP-Token oder Einmalkennwort per SMS/Mail/App), siehe hierzu auch die vom Administrator erhaltenen Zugangsdaten:

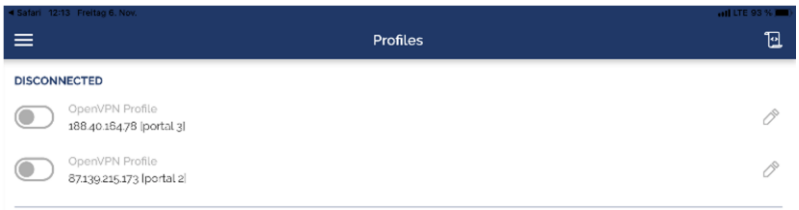
Wenn die Benutzer-Authentisierung erfolgreich war, wird der VPN-Tunnel aufgebaut, was man an dem VPN-Zeichen (im Bild rot markiert) in der Statuszeile am oberen Rand des Gerätes jederzeit erkennen kann:

Wichtig: Während der VPN-Tunnel aufgebaut ist, kann aus Sicherheitsgründen keine andere App auf das Internet zugreifen!

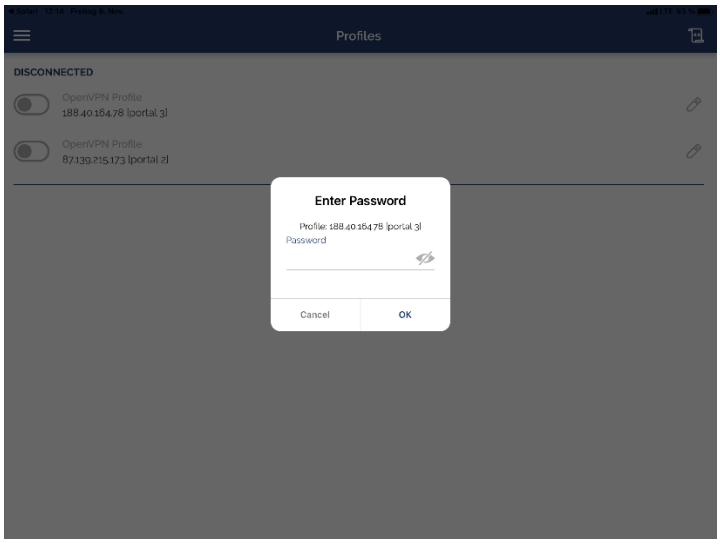
Jetzt kann man die gewünschte App starten, um auf die Anlagenvisualisierung o.ä. zuzugreifen. Dazu gibt man in der App die sog. externe IP-Adresse der Steuerung o.ä. ein, die man vom Administrator erhalten hat.

3.1 OpenVPN-Tunnel auf dem iPad/iPhone starten

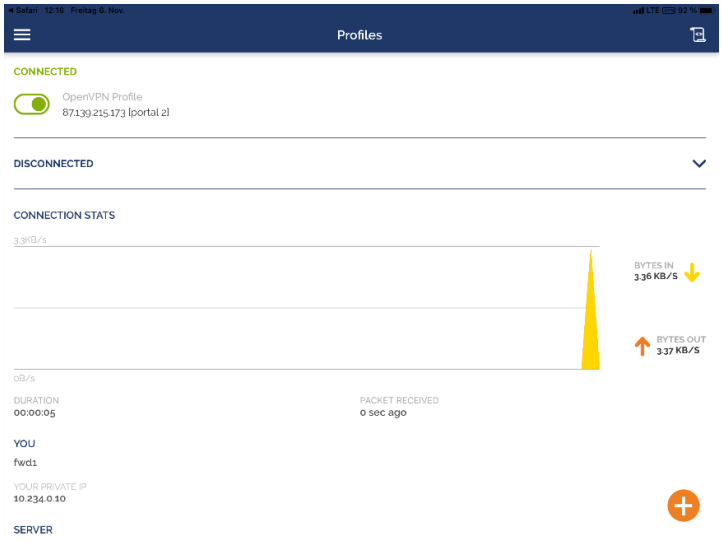
Dazu die OpenVPN App aufrufen und, falls mehrere VPN-Profile eingerichtet sein sollten, das gewünschte Profil über den Button starten:



Jetzt gibt man zuerst das statische Kennwort, direkt gefolgt vom Einmalkennwort (OTP), ein:



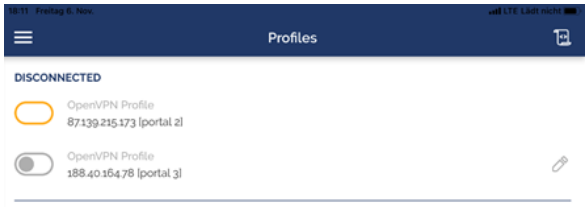
Wenn der OpenVPN-Tunnel erfolgreich aufgebaut wurde, wird dies in der OpenVPN App mit Connected angezeigt. Dort sieht man auch einen Statistikbereich mit der Dauer der VPN-Verbindung, dem Datentransfervolumen usw.:



Zusätzlich sieht man oben in der Kopfzeile des Gerätes das VPN-Symbol (im Bild rot markiert):

Jetzt kann man die gewünschte Zugriffs-App aufrufen (z.B. eine RDP-App).

Zum Beenden des OpenVPN-Tunnels in die OpenVPN App wechseln und das entspr. Profil beenden:

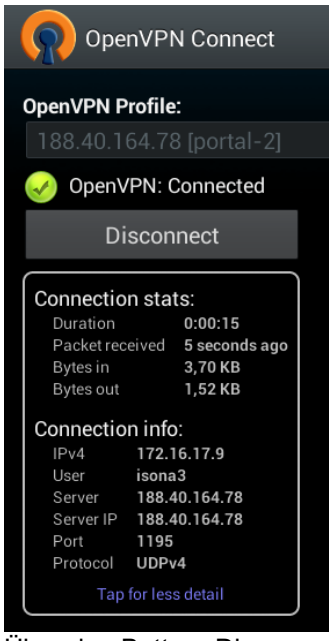


Je nach Konfiguration erfolgt noch eine Abfrage, ob man die App wirklich beenden möchte.

4. Start eines OpenVPN-Profils bei Android-Tablets

Zuerst die App „OpenVPN Connect“ starten:

Wenn der VPN-Tunnel erfolgreich aufgebaut wurde, wird die Meldung „OpenVPN connected“ sowie der Verbindungsstatus angezeigt:



Über den Button „Disconnect“ muss der VPN-Tunnel dann nach Abschluss der Arbeiten beendet werden.

5. Informationen zu Apps

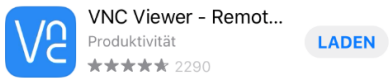
Nachfolgend finden Sie Informationen zu diversen Apps, die sich im Zusammenhang mit dem ISONA Secure Automation Tablet-OTP (SAT) als nützlich erwiesen haben.

Wichtiger Hinweis: Es handelt sich hier um Empfehlungen, für die ISONA aber keinerlei Garantie übernimmt. Die entsprechenden Apps sind über den Apple App Store (für iPad und iPhone) bzw. Google Play Store (für Android-Tablets und -Smartphones) zu beziehen.
Eventuell stehen bezüglicher dieser Liste neuere Apps oder auch andere Apps für den jeweiligen Einsatzbereich in den entsprechenden Stores zur Verfügung, wir empfehlen dies von Zeit zu Zeit zu überprüfen.

Name der App: **Microsoft-Remotedesktop:**

Funktion: Diese kostenlose App von Microsoft (ab iOS 8.0) ermöglicht einen RDP-Zugriff auf WIN PCs/WIN-Server sowie auf einen ISONA Automation Terminalserver.

Name der App: **VNC-Viewer:**



Funktion: Mit dieser kostenlosen App kann man sich auf entferne PCs und Systeme verbinden, auf denen ein VNC-Server installiert sind. Diese wird oft zum Fernzugriff im Automationsbereich verwendet.

Apps für den Bereich Automation/Steuerungen (Auszug):

Name der App: **SBC Micro Browser (Lite- oder Vollversion)**
Funktion: Diese App dient als herstellerspezifischer Browser, mit dem man sich die Webfrontends der diversen Saia Automationsgeräte (PCD, VisiPlus usw.) anzeigen lassen kann.

Name der App: **Saia PCD Energy Manager**
Funktion: Diese App dient als herstellerspezifischer Browser, mit dem man sich die Webfrontends der diversen Saia Energiemanagementgeräte wie z.B. dem Energy Manager anzeigen lassen kann.

Name der App: **Pro-face Remote HMI**
Funktion: Diese App dient als herstellerspezifischer App, mit der man auf Proface-Steuerungen der Firma Schneider Electric zugreifen kann.

6. Kontakt

ISONA GmbH
Sant-Ambrogio-Ring 13a
D-55276 Oppenheim

E-Mail support@isona.de
Internet www.isona.de