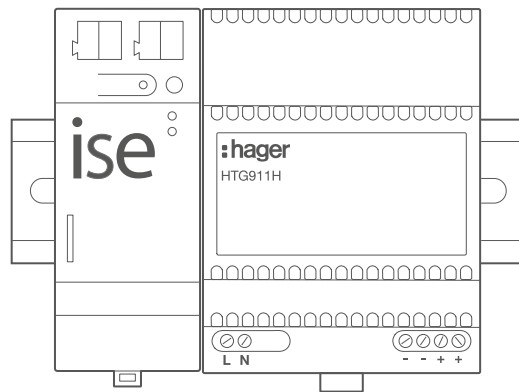


Fernzugriff

Hager intercom Türkommunikationssystem



Fernzugriffsmodul für Hager intercom
RTD230X

1	Einleitung.....	3
2	Sicherheitshinweise.....	4
3	Inbetriebnahme.....	5
3.1	Vorbereitungen.....	5
3.2	Fernzugriffsmodul in der ISE Cloud registrieren.....	6
3.2.1	ISE-Konto registrieren.....	6
3.2.2	Gerät in my.ISE hinzufügen.....	7
3.2.3	VPN-Zertifikat erstellen.....	8
3.3	Fernzugriff einrichten.....	10
3.3.1	VPN-Software installieren und VPN-Zugang einrichten.....	10
3.3.2	Einstellungen in Hager intercom manager.....	12

1 Einleitung

Zielgruppe

Dieses Dokument richtet sich an Installateure und Administratoren wie z. B. Facility-Manager des Türkommunikationssystems Hager intercom.

Die Installation des Fernzugriffsmoduls ist nur durch zertifizierte Elektrofachkräfte nach den relevanten Normen und Bestimmungen auszuführen. ► Siehe produktbeiliegende Montageanleitung.

Der Fernzugriff auf das Türkommunikationssystem Hager intercom kann auch durch den Anlagenadministrator eingerichtet werden.

Inhalt des Dokuments

Diese Dokumentation behandelt die Einrichtung des Fernzugriffs auf das Türkommunikationssystem Hager intercom.

Produkteigenschaften

- Bearbeitung der Benutzerverwaltung per Fernzugriff mit einem Rechner, auf dem das anlagenaktuelle Konfigurationstool intercom manager läuft.
- für die datensichere und verschlüsselte Datenübertragung wird ein VPN-Zugang auf das Gerät eingerichtet.
- die gesicherte Datenübertragung erfolgt über die Cloud von ISE **<https://my.ise.de>**
- Firmware-Updates der intercom Geräte per Fernzugriff



Updates per Fernzugriff nehmen mehr Zeit in Anspruch. Für die intercom motion wird empfohlen das Update vor Ort durchzuführen.

2 Sicherheitshinweise



Allgemeine Sicherheitshinweise



Warnung

Vor Inbetriebnahme ist die Installation des Fernzugriffsmoduls vor Ort beim Kunden durch eine Elektrofachkraft nach den geltenden Vorschriften auszuführen. Montageanleitung des Geräts beachten!

Die ausführende Elektrofachkraft muss über hinreichende Kenntnisse der Netzwerktechnik verfügen.

Beachten Sie zusätzlich auch die Sicherheitshinweise aus unserem Dokument „Inbetriebnahme & Benutzerverwaltung“ mit dem intercom manager.

Bei Nichtbeachtung können Fehlfunktionen, Schäden an der Anlage, Brand oder andere Gefahren entstehen.

Netzwerksicherheit



Achtung

Für den Fernzugriff wird ein VPN-Client benötigt (Empfehlung: OpenVPN). Laden Sie die entsprechende Software aus einer sicheren Quelle herunter:

<https://openvpn.net/community-downloads>

Bei der Einrichtung des VPN-Zugangs muss ein sicheres Passwort vergeben werden.



Achtung

Zur Inbetriebnahme und Anpassung der Konfiguration darf immer nur ein Rechner mit dem System verbunden sein!

Bei mehreren gleichzeitig verbundenen Rechnern können Synchronisierungsfehler auftreten und Servicekonflikte entstehen, verursacht durch abweichende Instanzen der laufenden Hager intercom Services.



Achtung

Änderungen einer bestehenden Anlage per Fernzugriff ohne Übergabe-Export führen zu Systemabweichungen und gfs. Fehlfunktionen.

Für die Überarbeitung einer Kundenanlage per Fernzugriff wird zwingend ein aktueller Übergabe-Export aus dem intercom manager benötigt. Der aktuelle Übergabe-Export vom Kundenrechner muss in den intercom manager des Fernzugriffsrechners importiert werden. Nach Abschluss der Arbeiten muss ein neuer Übergabe-Export erstellt werden und in den intercom manager des Kundenrechners importiert werden.

3 Inbetriebnahme



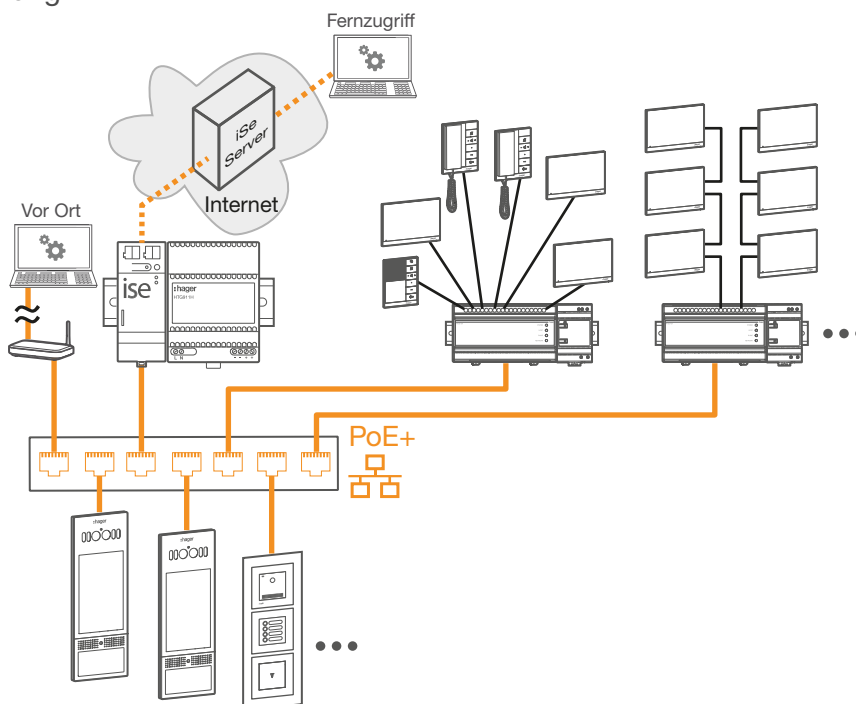
Die Inbetriebnahme erfolgt anders als in der produktbeiliegenden Anleitung beschrieben ohne die ETS Software. Die Inbetriebnahme oder Verwendung der KNX Schnittstelle ist für Hager intercom nicht notwendig.

3.1 Vorbereitungen

- ☑ Die Türkommunikationsanlage Hager intercom ist vor Ort gemäß der Projektplanung installiert.
- Notieren Sie sich die **Registrierungs-ID** und die **MAC-Adresse** des Fernzugriffsmoduls. Die Informationen finden Sie seitlich auf dem Gerät.



- Installieren Sie das Gerät nach Angabe des Herstellers, ► siehe produktbeiliegende Montageanleitung.



Der Rechner vor Ort muss bei Fernzugriff vom Netzwerk getrennt sein. Er kann erst mit einem Übergabe-Export des Fernzugriffs-Rechners wieder im Betrieb genommen werden.

Für das ISE Gerät wird für den Betrieb an der gelb (+) / weißen (-) Steckklemme eine zusätzliche Spannungsversorgung 24 V= Hager HTG911H oder TGA200 benötigt.

3.2 Fernzugriffsmodul in der ISE Cloud registrieren

3.2.1 ISE-Konto registrieren

- Öffnen Sie folgende Website: <https://my.ise.de>

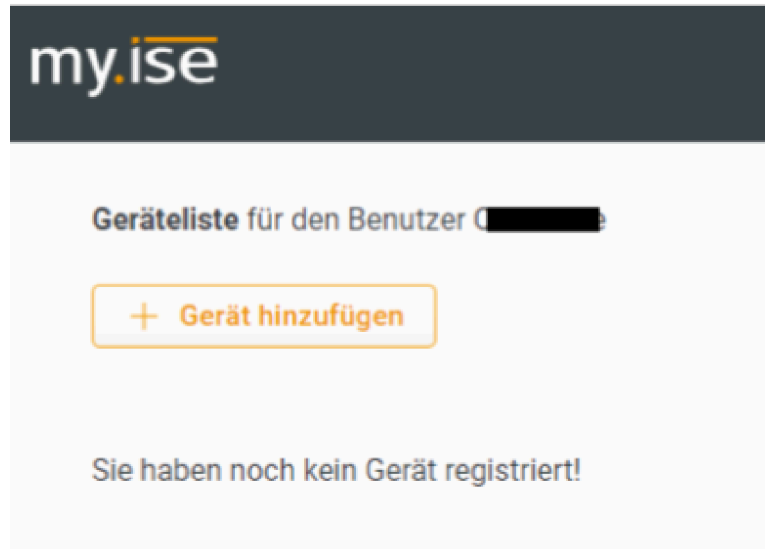
- Geben Sie Ihre Registrierungsdaten ein. Pflichtfelder sind:
 - **Name**
 - **E-Mail**
 - **Passwort**

- Lesen und akzeptieren Sie die Datenschutzerklärung.
- Klicken Sie auf **Registrieren**.

Sie erhalten eine Bestätigungsmail. Anschließend können Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort anmelden.

3.2.2 Gerät in my.ISE hinzufügen

- Klicken Sie auf + **Gerät hinzufügen**..

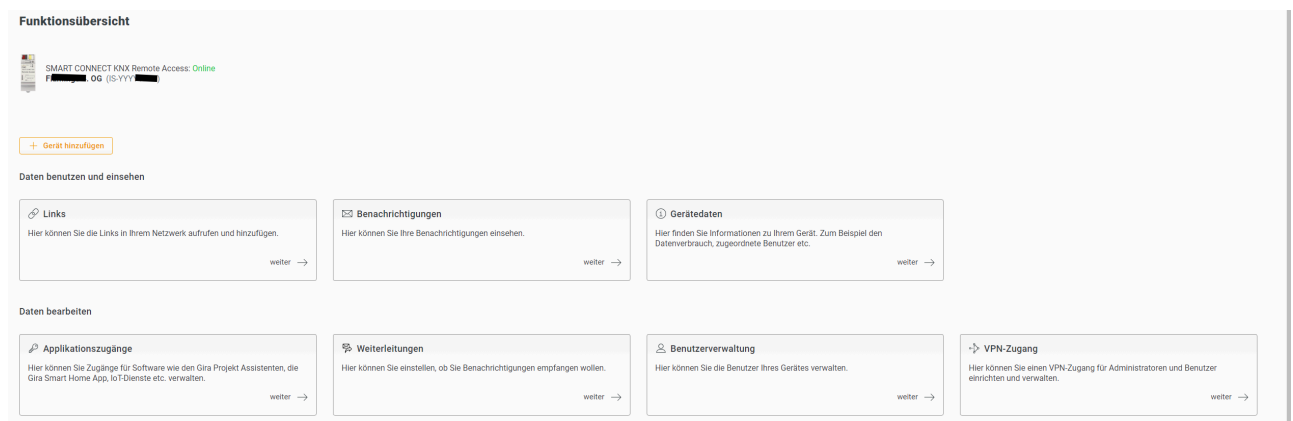


- Geben Sie die Registrierungs-ID von Ihrem Gerät ein.



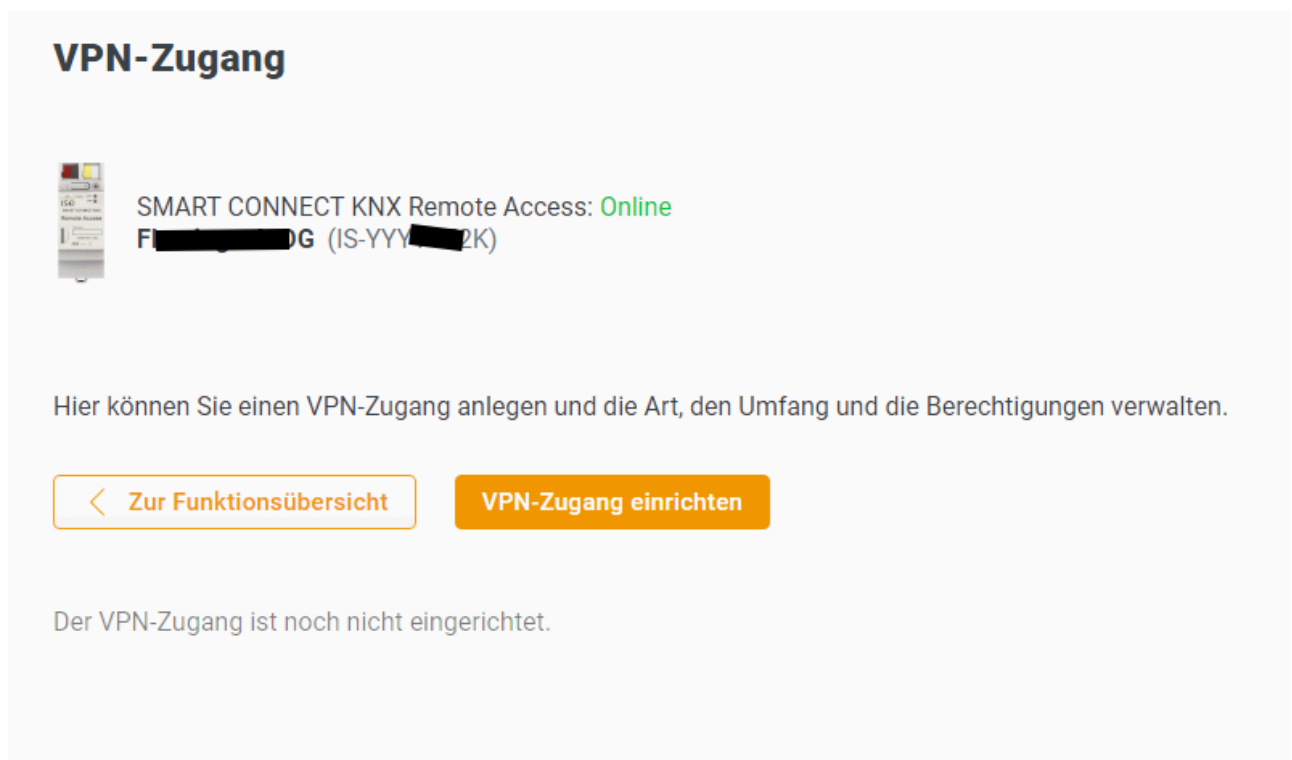
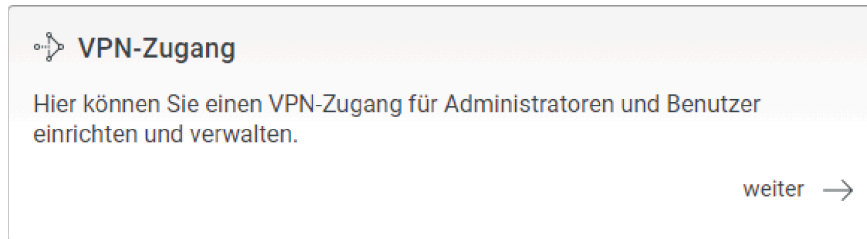
Das Gerät muss während dieses Schrittes mit dem Internet verbunden sein.

- Überprüfen Sie den Online-Status in der Funktionsübersicht.



3.2.3 VPN-Zertifikat erstellen

- Klicken Sie in der Funktionsübersicht auf **VPN-Zugang** und anschließend auf **VPN-Zugang einrichten**.



- Wählen Sie die Option „**Direkte Teilnahme im Netzwerk des SMART CONNECT KNX Remote Access**“ aus, um sicherzustellen, dass der Hager intercom manager die Geräte beim Scannen findet.

Schritt 1 von 2

VPN-Zugang einrichten

Welchen Zugangstyp soll der VPN-Zugang nutzen?

☐ Eigenes Netzwerk erstellen (empfohlen)
Dieser Zugangstyp erzeugt ein eigenes Netzwerk zwischen Client und SMART CONNECT KNX Remote Access und bietet zusätzliche Sicherheit. Das Datenaufkommen ist geringer als bei einer direkten Teilnahme des Clients im Netzwerk des SMART CONNECT KNX Remote Access.

☒ **Direkte Teilnahme im Netzwerk des SMART CONNECT KNX Remote Access**
Der Client erhält eine eigene IP-Adresse im Netzwerk des SMART CONNECT KNX Remote Access. Das erforderliche Datenaufkommen ist höher als beim Einsatz eines eigenen Netzwerks zwischen dem Client und dem SMART CONNECT KNX Remote Access. Diese Einstellung ist jedoch für bestimmte Anwendungszwecke nötig.

Weiter →

Abbrechen

Schritt 2 von 2

VPN-Zugang einrichten

Soll der gesamte Datenverkehr über die VPN-Verbindung laufen?

☐ DEAKTIVIERT (EMPFOHLEN)
Nur der Datenaustausch mit dem Ziernetzwerk erfolgt über die VPN-Verbindung. Der Internetverkehr läuft dann wie gewohnt direkt über den lokalen Router bzw. das mobile Netz.

← Zurück

Fertigstellen

Abbrechen

- Klicken Sie auf **Fertigstellen** und warten Sie bis das Fenster zum Download der VPN-Konfigurationsdatei erscheint, um die Datei herunterzuladen.

VPN-Konfigurationsdatei wird generiert.

Dieser Vorgang kann ein paar Minuten dauern.

Anschließend können Sie die Datei herunterladen und in Ihren OpenVPN-Client importieren.

AGB

Die VPN-Konfigurationsdatei steht bereit.

Der Vorgang ist abgeschlossen.

Sie können die Datei nun herunterladen, um sie in Ihren OpenVPN-Client zu importieren. Dies können Sie auf dieser Seite auch später jederzeit tun.

VPN-Konfigurationsdatei herunterladen

Schließen

AGB

3.3 Fernzugriff einrichten

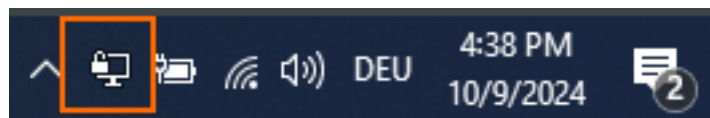
3.3.1 VPN-Software installieren und VPN-Zugang einrichten

- ☑ Es wird eine VPN-Software benötigt, die VPN Layer2 unterstützt. Empfehlung: OpenVPN Community Edition Software

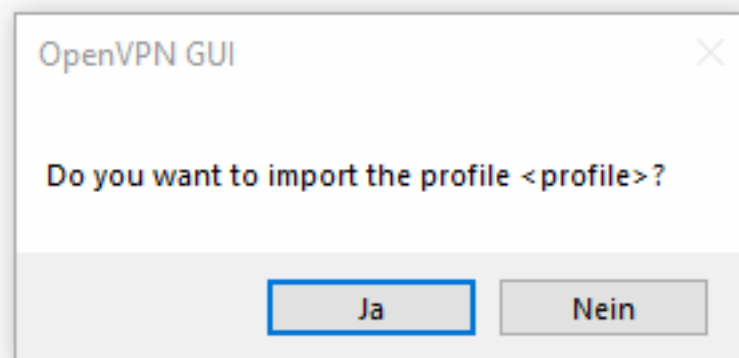
Beispielhaft wird hier die Installation der OpenVPN Community Edition Software mit Windows 11 beschrieben.

- Laden Sie OpenVPN Community Edition herunter: openvpn.net/community-downloads
- Installieren Sie die OpenVPN-Software.

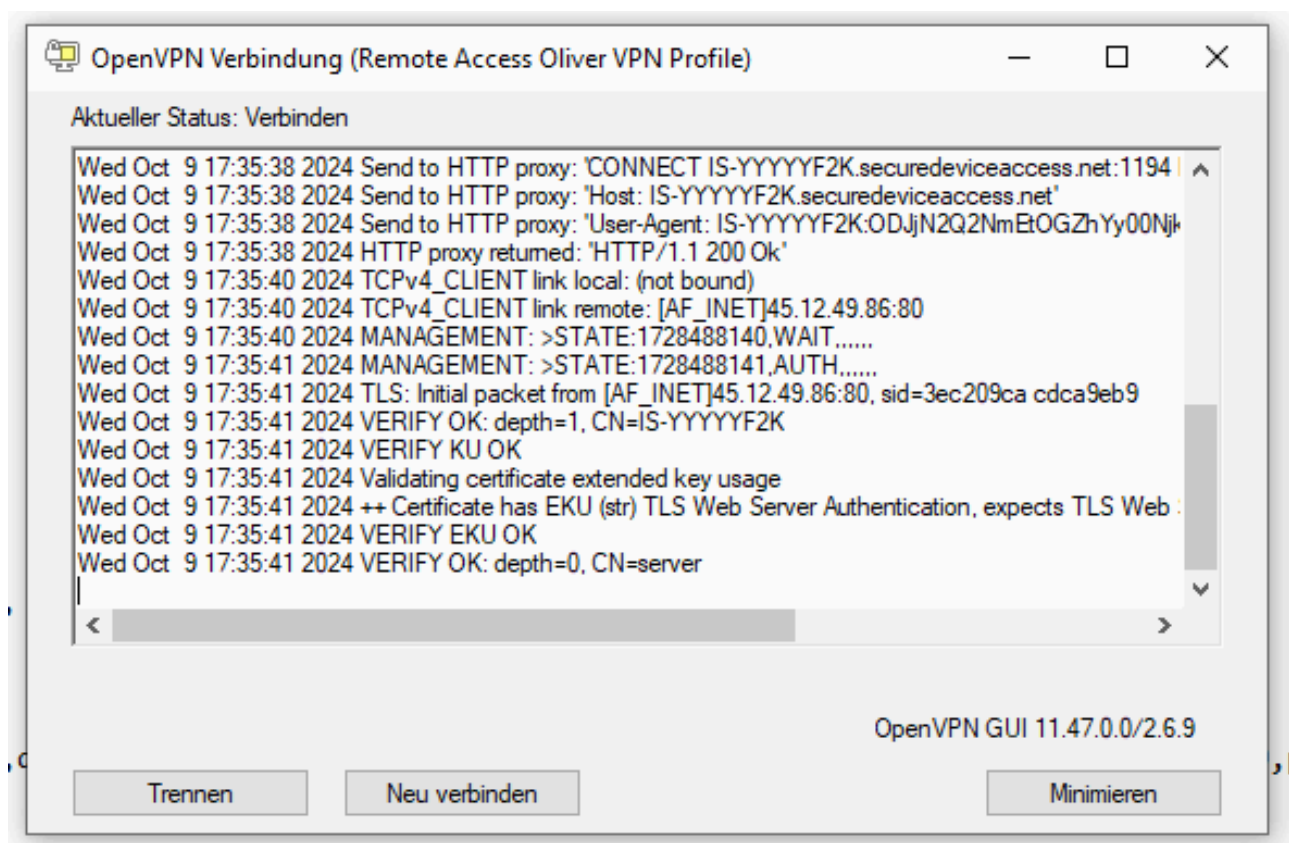
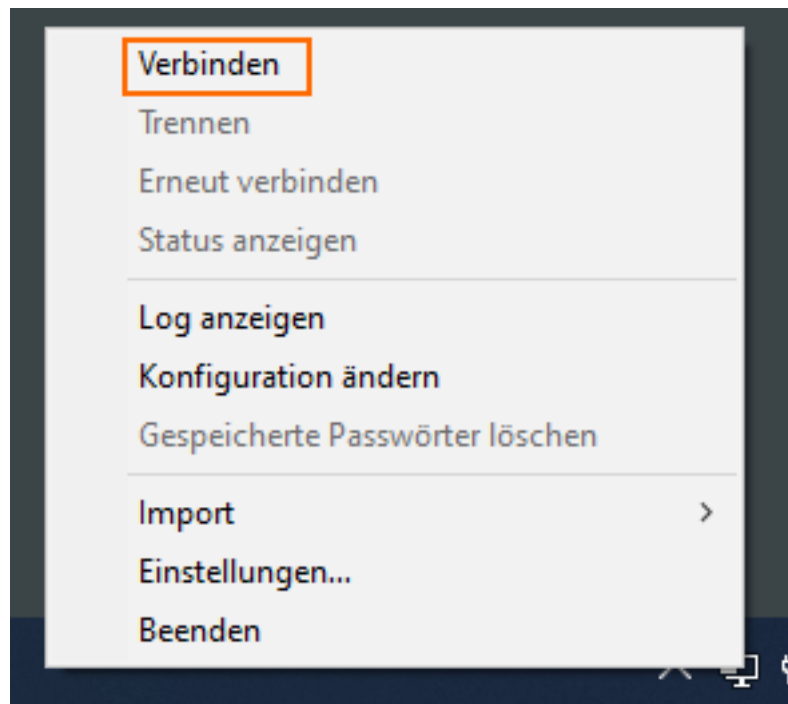
Bei erfolgreicher Installation erscheint ein neues Symbol in der Statusleiste.



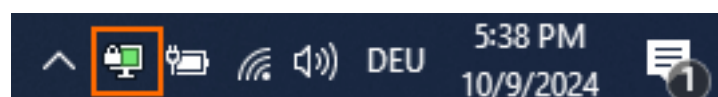
- Klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie im Kontextmenü **importieren**, um die VPN-Konfigurationsdatei zu importieren. Alternativ: Doppelklick auf die VPN-Konfigurationsdatei



- Um eine Verbindung zum VPN-Netzwerk herzustellen, klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie im Kontextmenü **Verbinden**.



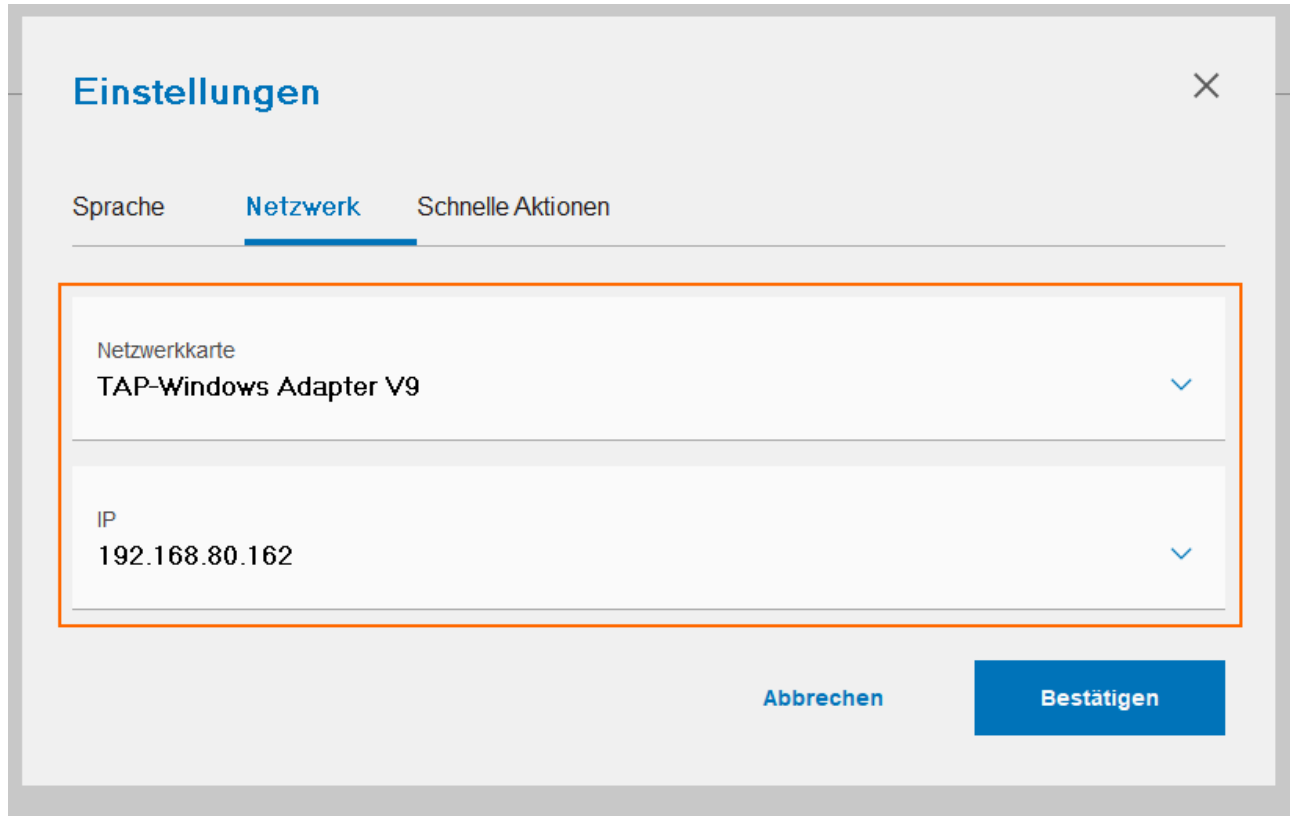
Bei erfolgreicher Verbindung wird das Protokollfenster geschlossen und das Symbol in der Statusleiste ist grün.



- Falls die Verbindung fehlschlägt, setzen Sie das Gerät zurück und versuchen Sie es erneut.

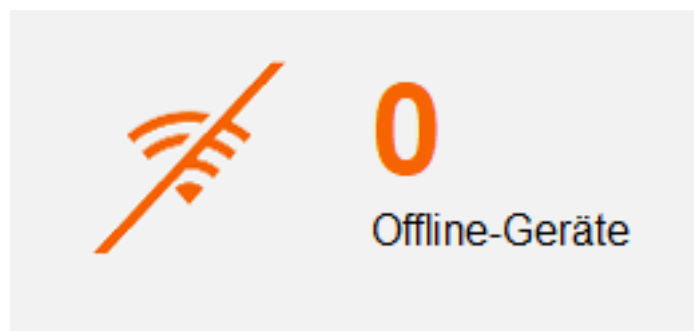
3.3.2 Einstellungen in Hager intercom manager

- Nachdem die VPN-Verbindung erfolgreich hergestellt wurde, starten Sie den Hager intercom manager. Wählen Sie in den allgemeinen Einstellungen ⚙ das **Netzwerk** der Hager intercom Installation aus, auf die Sie zugreifen möchten.









Der Hager intercom manager startet neu und Ihre Geräte werden anschließend mit dem Status online angezeigt.

Anzeige auf dem Dashboard:



Anzeige in der Geräteverwaltung:

<div> + Gerät hinzufügen Synchronisieren Importieren Exportieren + Gerät erstellen Installationseinstellungen </div>									
Alle Status		Alle Typen		Liste filtern		Zurücksetzen			
<input type="checkbox"/>	Typ	Knoten	Standort	Kommentar	Gerätename	IP	MAC	Status	Firmware
<input type="checkbox"/>		1.1	Gebäude 1	links	Front door left ODT	192.168.80.155	XXXXXXXXXXXX	✓ Online	915.75.1.544
<input type="checkbox"/>		1.1	Gebäude 1	mitte	Front door ODT	192.168.80.140	XXXXXXXXXXXX	✓ Online	915.75.1.544
<input type="checkbox"/>		1.1	Gebäude 1	rechts	Front door right ODT	192.168.80.156	XXXXXXXXXXXX	✓ Online	915.75.1.544
<input type="checkbox"/>		1.1	Gebäude 1		Building 1 Combi	192.168.80.148	XXXXXXXXXXXX	✓ Online	320.75.10.137
<input type="checkbox"/>		1.1	Gebäude 1		WebRelay X-401	192.168.80.184		Not applicable	
<input type="checkbox"/>		1.1	Gebäude 1		WebRelay WuT	192.168.80.185		Not applicable	



Hager Controls

BP10140

67703 Saverne Cedex

France

+33 (0) 3 88 02 87 00

info@hager.com

[hager.com](https://www.hager.com)