

Honeywell Security Plug in

Enables the integration of the certified alarm systems MB Secure PRO and MB Secure by Honeywell Security.

Features:

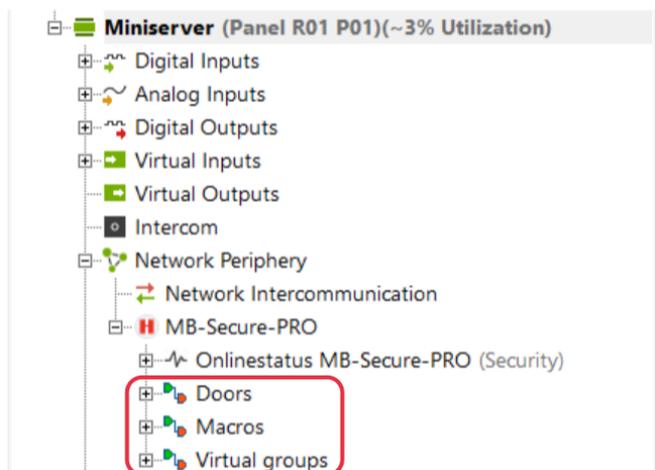
- Internal and external arming and disarming of the alarm system
- Virtual group events and controls
- Door events and controls
- Macro events and controls
- Output of all system states

Depending on the certification level of the alarm system, bidirectional communication in the programming can be restricted to unidirectional communication on the MB Secure side.

Information:

- For MB Secure PRO, the Smart Building License (License Option 059829) by Honeywell Security is required.
- For MB Secure, the Third-Party Integration Level 3 (License Option 059822) is required.
- This plugin is only supported by second-generation Miniservers.

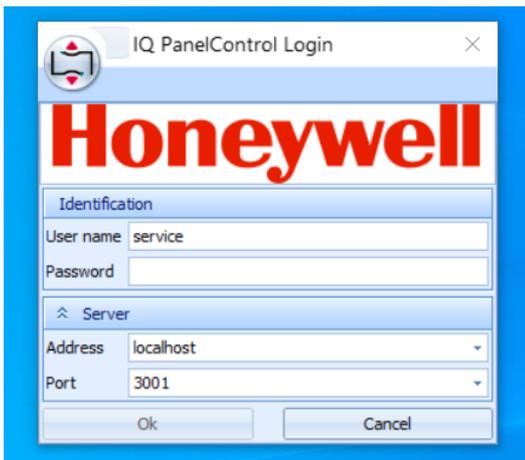
If access to the system is not available, please contact the Honeywell System Partner responsible for the project.



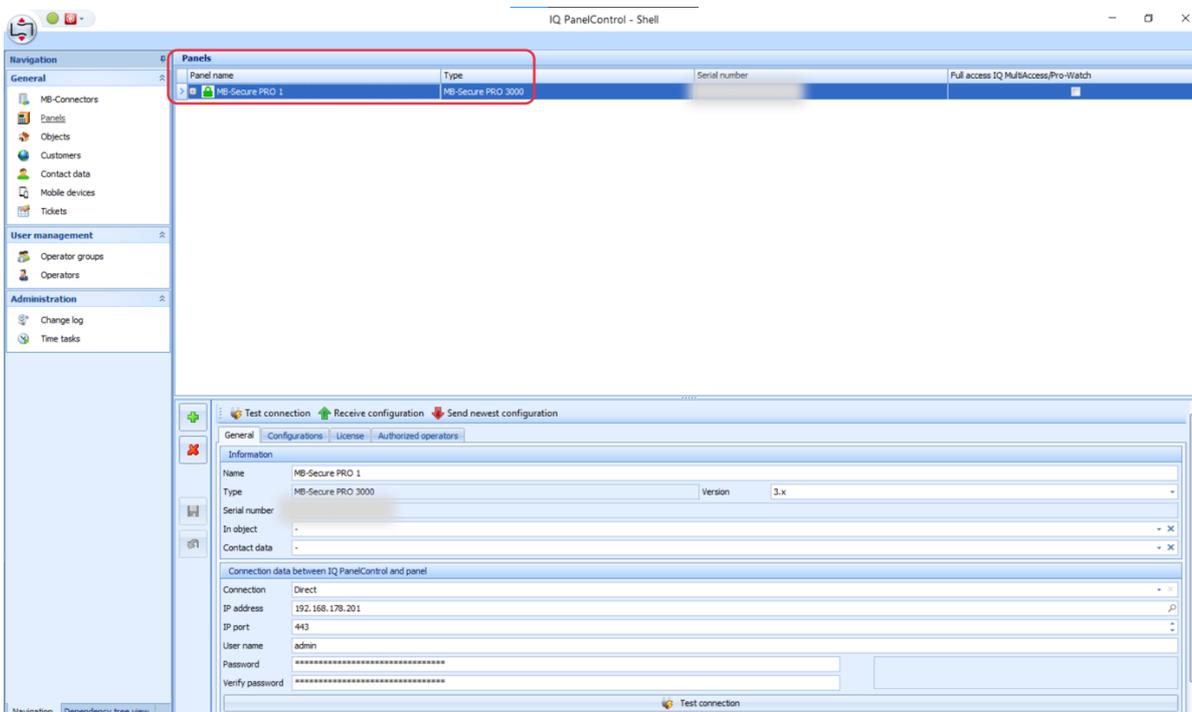
Initial Configuration:

Open the Honeywell software IQ PanelControl and log in with an authorized user. Ensure that the software requires at least version V16.05. The system **MB Secure PRO** must be running at least version **V03.06** and have an activated Smart Building License.

Perform an update if necessary.

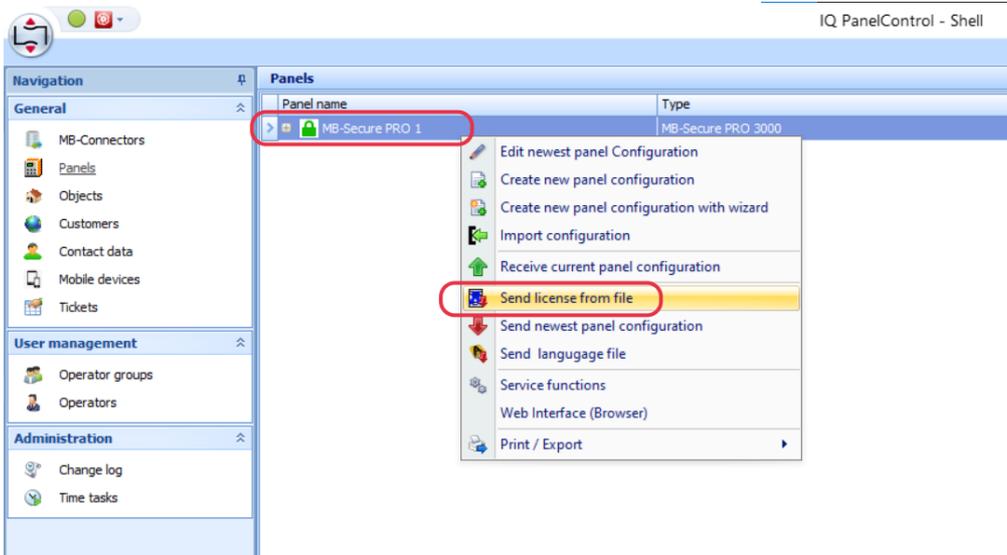


Your available panels will be displayed in the overview.



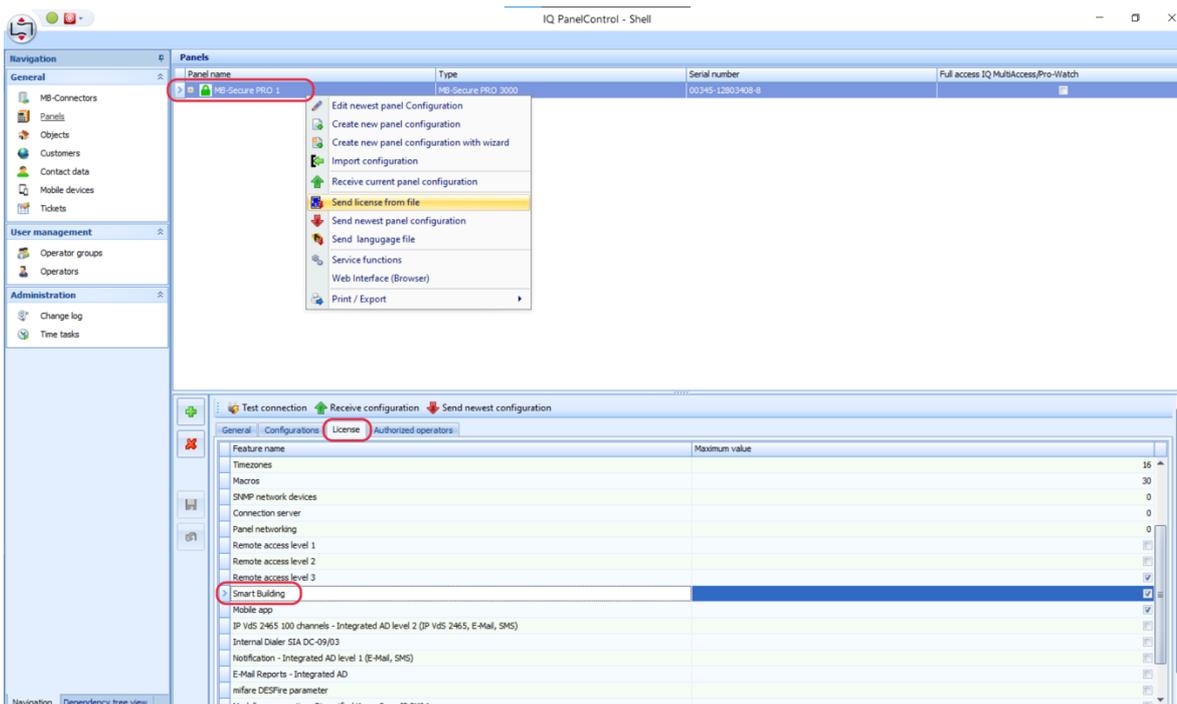
Send your Smart Building License to the MB Secure PRO by selecting it and using a right-click to choose the option "Send license from file."

To obtain this license, please contact the **Honeywell System Partner** responsible for the project.



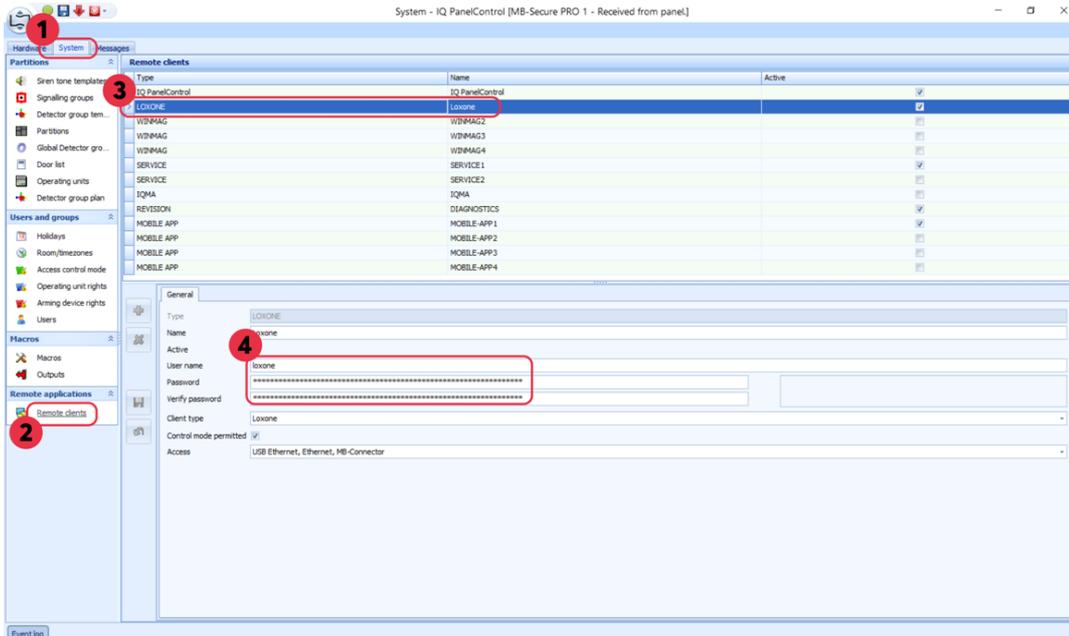
Under the "License" tab, the active licenses are displayed.

For the **MB Secure PRO**, the **Smart Building License** is required, and for the **MB Secure**, the **"Remote Access Level 3" License** is needed. Ensure that the respective license matching the system you are using is displayed here, corresponding to the system you are using is displayed here.



By double-clicking on the system in the panel, another window with the system's configuration opens.

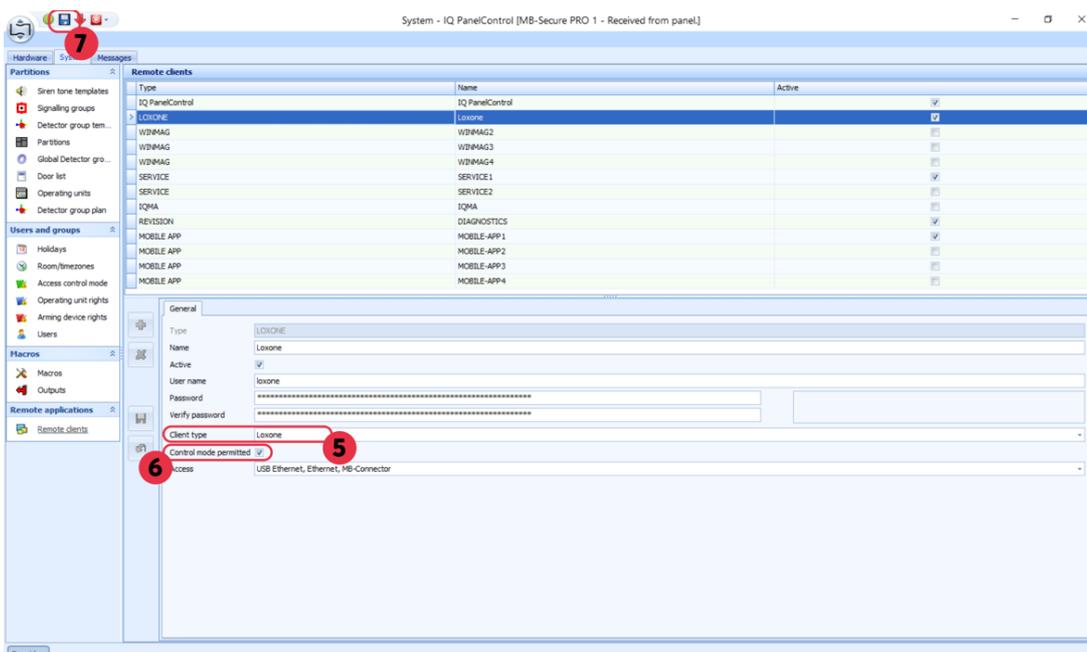
Under **System (1)** → **Remote Clients (2)**, check whether **Loxone (3)** is displayed (license-dependent). Then assign a **username and password (4)**, which the Loxone Miniserver can use to query and – depending on control access – also operate the system.



Configure this user with the **Remote Client Type "Loxone" (5)**.

The selection **"Control mode permitted" (6)** determines whether the system can be controlled by the Miniserver. Note that this may affect the **VdS certification level**.

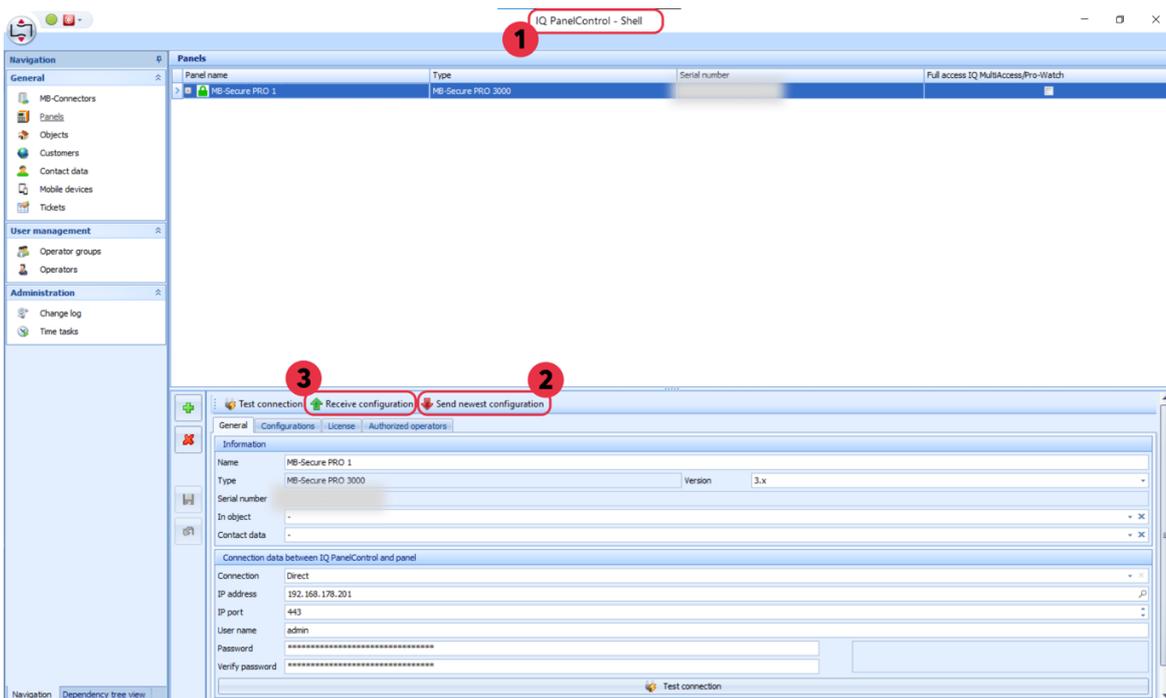
Finally, save the file (7).



Switch back to the program window **IQ PanelControl "Shell"** (1) and send the configuration to the system using the red arrow **"Send newest configuration"** (2).

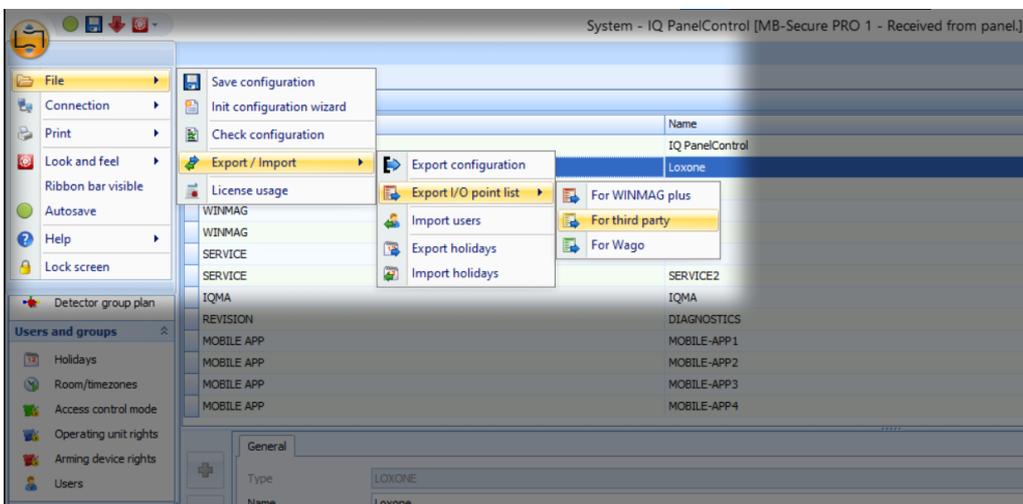
Important: The configuration must then be loaded back from the system using the green arrow **"Receive configuration"** (3) to store the current timestamp, which is relevant for authentication.

For every change or extension, these steps must be repeated. Otherwise, the Miniserver will display an error message.



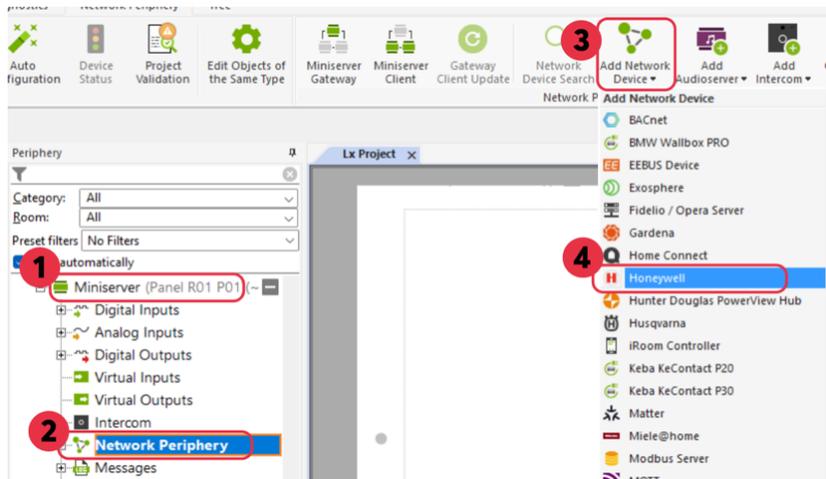
Only then can the current configuration be reopened, and the inputs and (optionally) outputs exported as an **OPIF file**.

Next, export the configuration of the **I/O list** from the file. This will provide you with the **"OPIF file,"** which must then be imported into the **Loxone Config**.

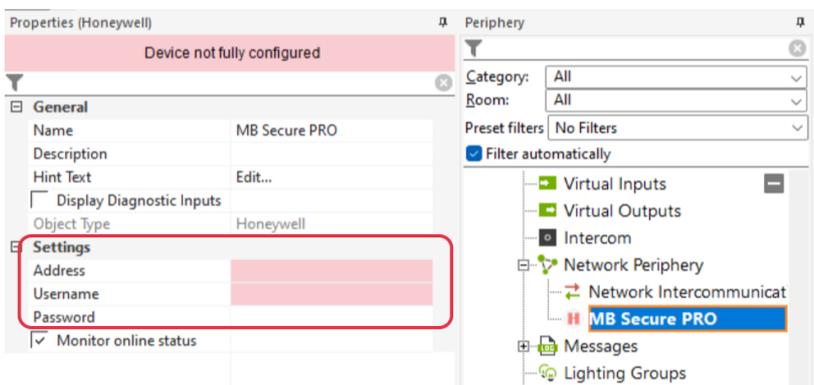


Loxone Config Settings:

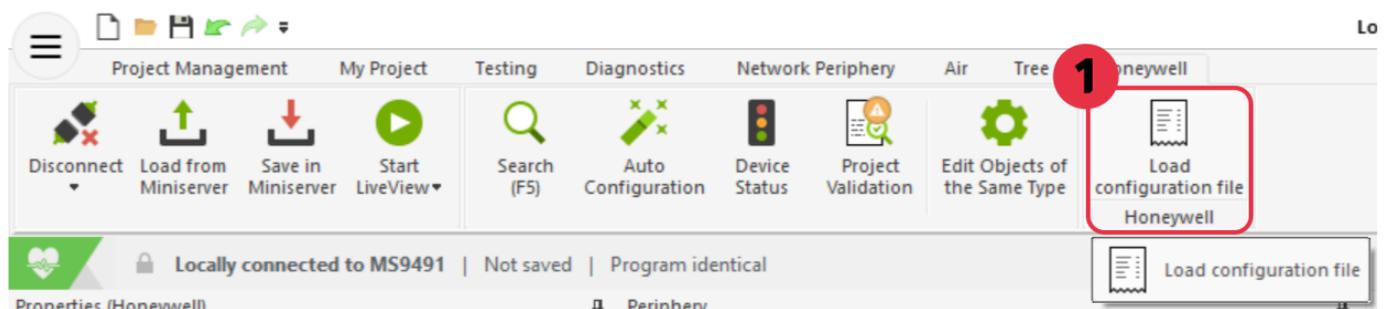
In your configuration on the Miniserver, add the **Honeywell Security Plugin** from the network devices.



Enter the **IP address** of the alarm system as well as the **username** and **password** that you previously created in the Honeywell Security software.

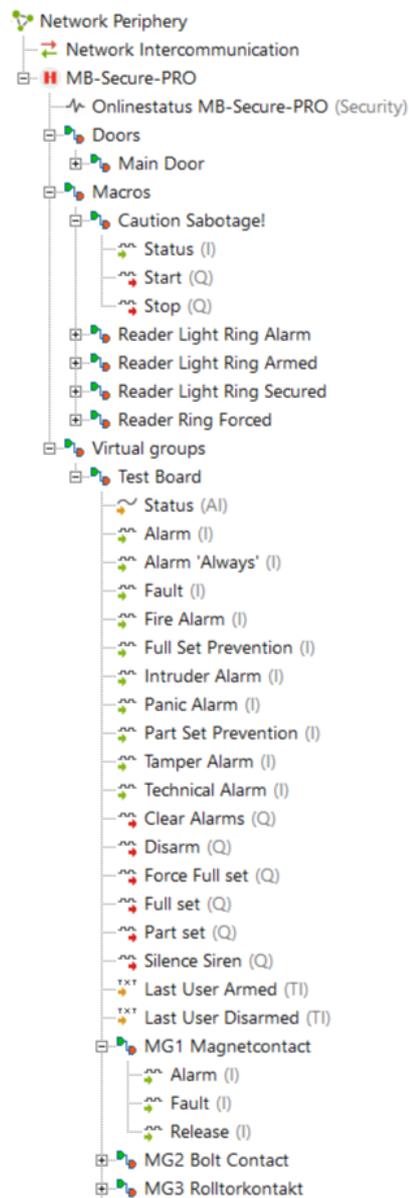


Import the **OPIF file** under "Load configuration file" into the Config.



The inputs will be automatically created.

Depending on the control access, all available outputs will also be added.



Honeywell Security Plug in

Ermöglicht die Einbindung der zertifizierten Alarmanlagen MB Secure PRO und MB Secure von Honeywell Security.

Features:

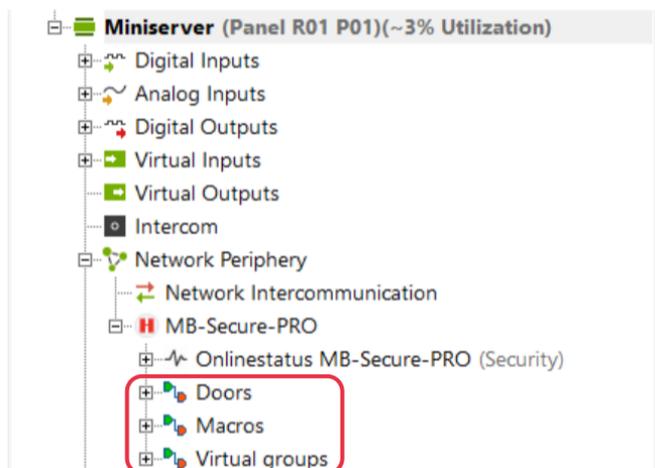
- Intern und Externe Scharf- und Unscharfstellen der Alarmanlage
- Virtuelle Gruppenereignisse und -ansteuerungen
- Türereignisse und -ansteuerungen
- Makroereignisse und -ansteuerungen
- Ausgabe aller Systemzustände

Je nach Zertifizierungsgrad der Alarmanlage kann die bidirektionale Kommunikation in der Programmierung auf eine unidirektionale Kommunikation auf Seiten der MB Secure eingeschränkt werden.

Informationen:

- Für die MB Secure PRO wird die **Smart Building Lizenz** (Lizenzoption 059829) von Honeywell Security benötigt.
- Für die MB Secure wird die **Fremdanbindung Stufe 3** (Lizenzoption 059822) benötigt.
- Dieses Plugin wird ausschließlich von Miniservern der **zweiten Generation** unterstützt.

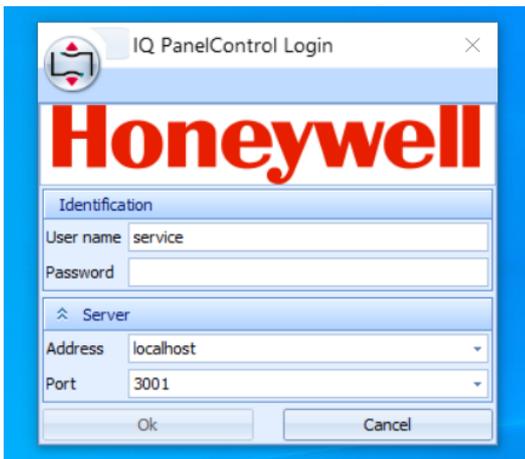
Sollte kein Zugriff auf die Anlage vorhanden sein, kontaktieren Sie den für das Projekt verantwortliche Honeywell System Partner.



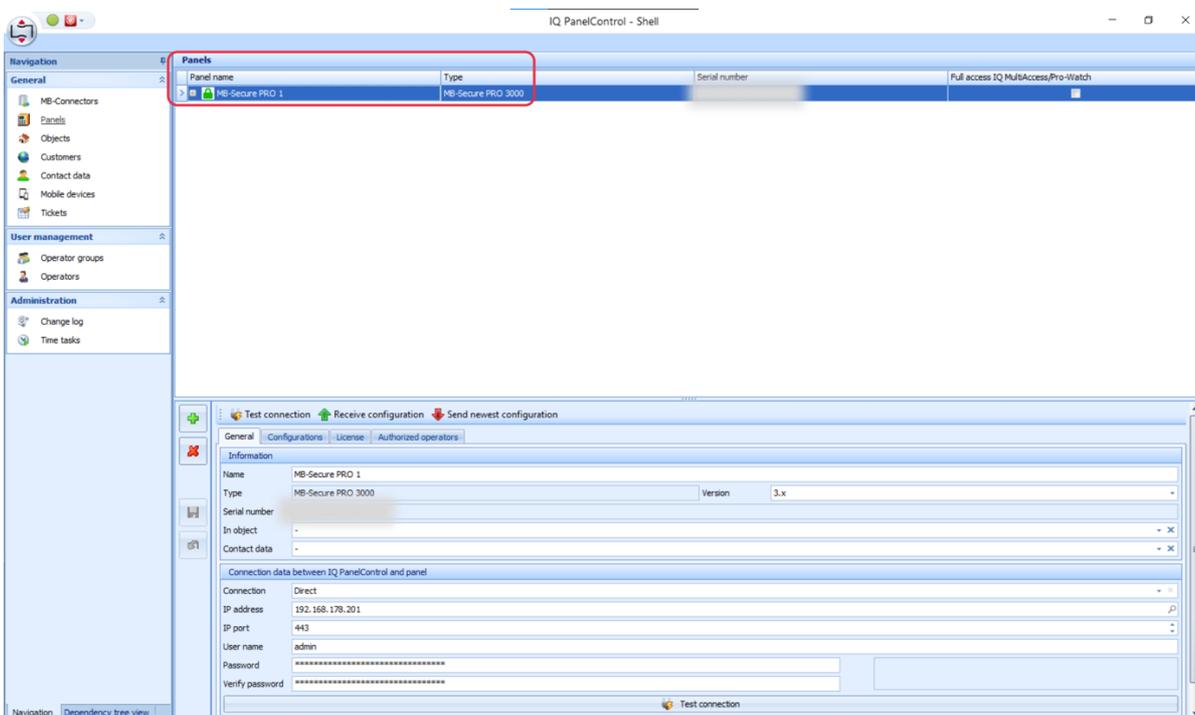
Erstkonfiguration:

Öffnen Sie die Honeywell Software **IQ PanelControl** und loggen Sie sich mit einem berechtigten Benutzer ein. Achten Sie darauf, dass die Software mindestens die Version **V16.05** benötigt. Die Anlage **MB Secure PRO** muss sich mindestens auf **V03.06** befinden und eine aktivierte Smart Building Lizenz besitzen.

Führen Sie gegebenenfalls ein Update durch.

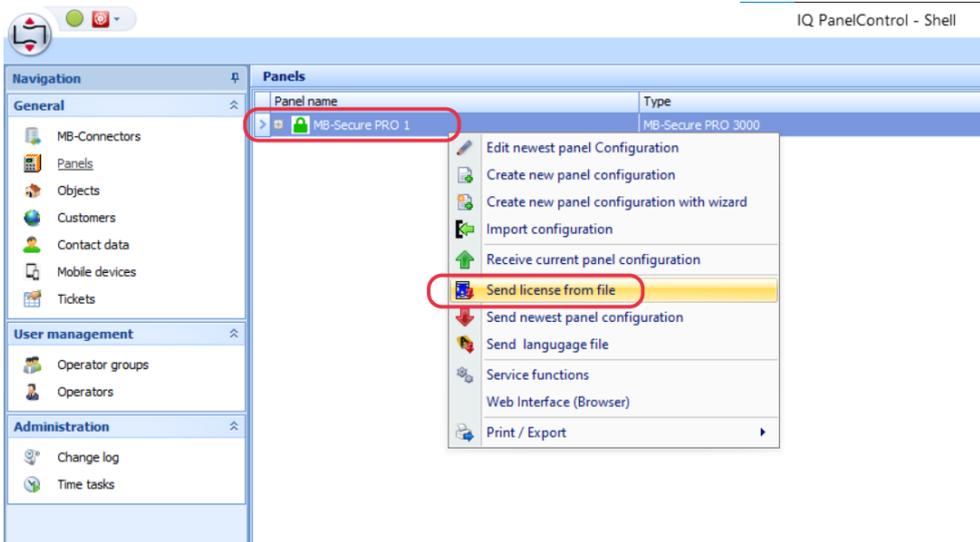


Ihre Verfügbaren Panels werden in der Übersicht angezeigt.



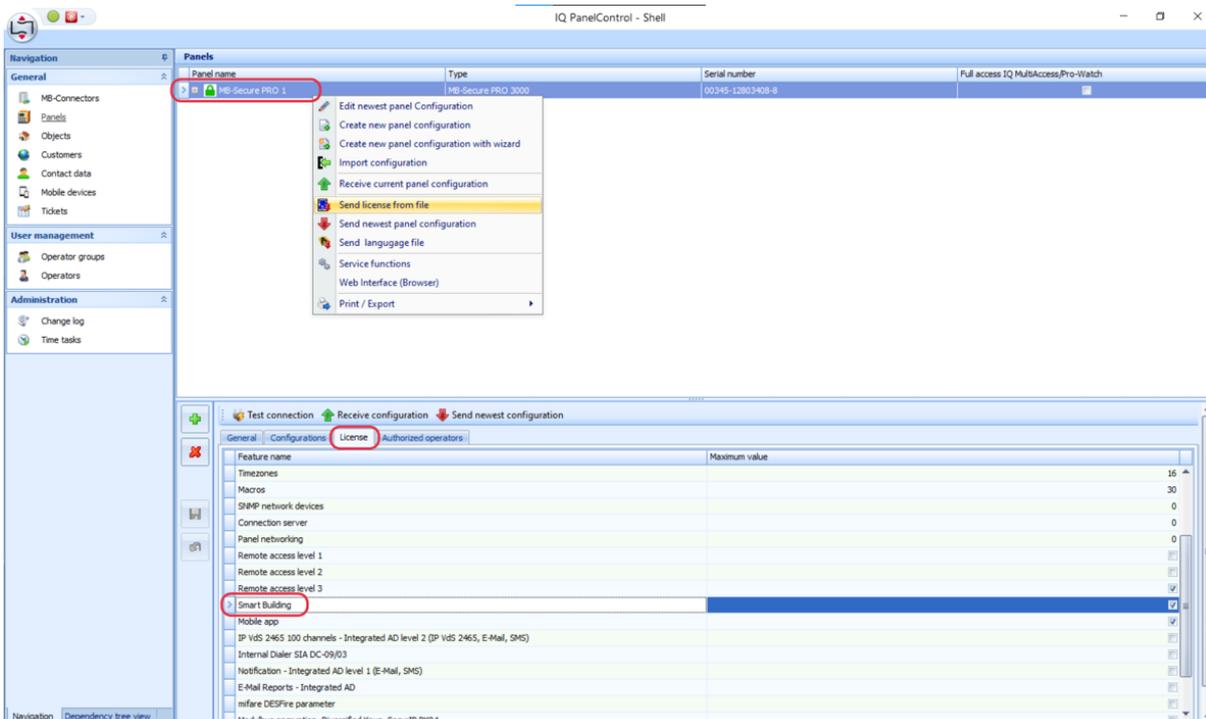
Senden Sie Ihre Smart Building Lizenz zur MB Secure PRO, indem Sie diese auswählen und mit einem Rechtsklick die Option "Lizenz aus Datei senden" auswählen.

Um diese Lizenz zu beziehen, kontaktieren Sie den für das Projekt verantwortliche Honeywell System Partner.



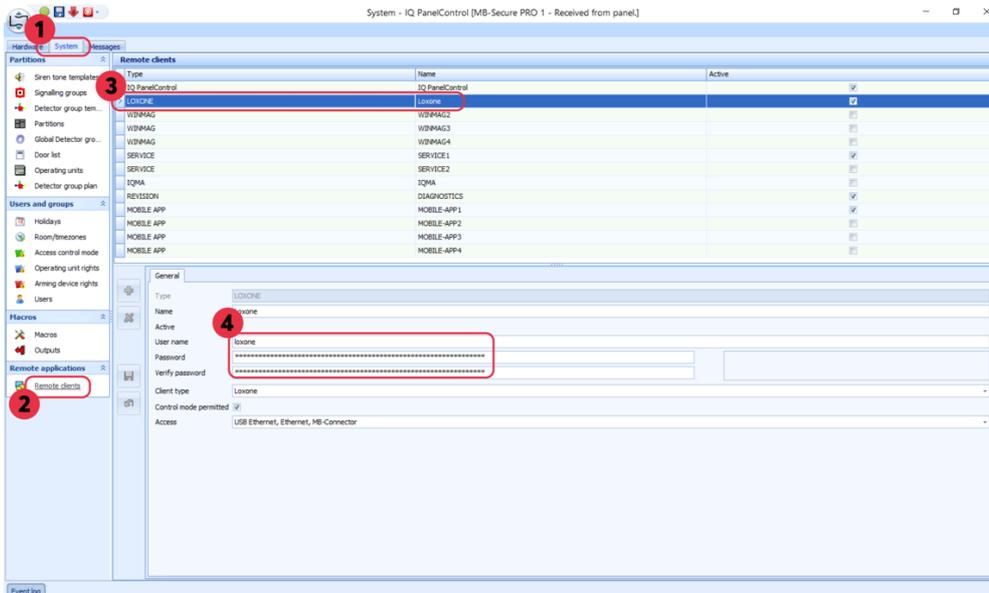
Unter dem Reiter „License“ werden die aktiven Lizenzen angezeigt.

Für die MB Secure PRO wird die Smart Building Lizenz benötigt, und für die MB Secure die „Remote Access Level 3“ Lizenz. Stellen Sie sicher, dass die jeweilige Lizenz, die zu der von Ihnen verwendeten Anlage passt, hier angezeigt wird.



Mit einem Doppelklick auf die Anlage im Panel, öffnet sich ein weiteres Fenster mit der Programmierung der Anlage.

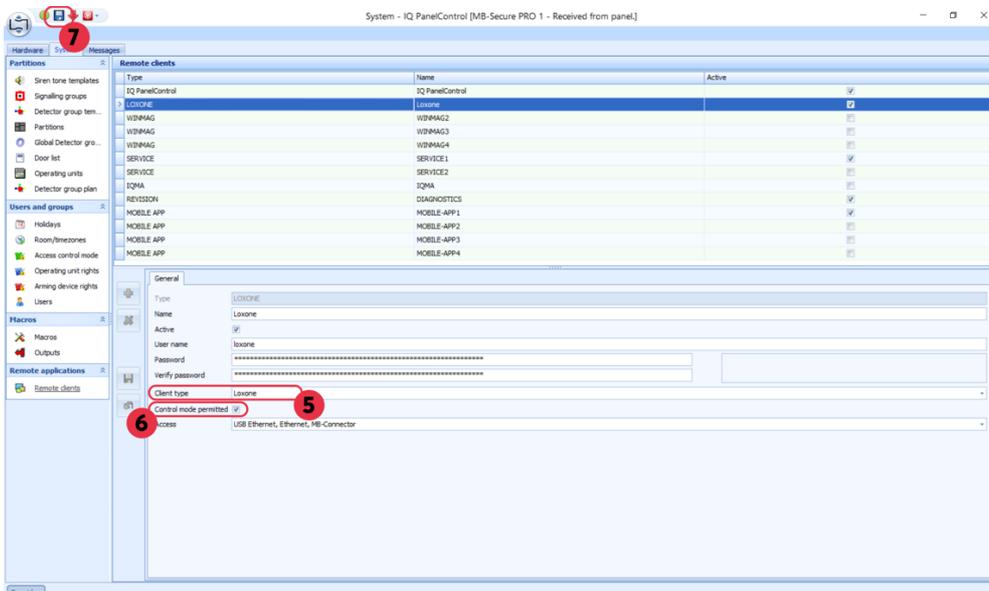
Unter **System** (1) → **Remote Clients** (2) überprüfen Sie, ob **Loxone** (3) angezeigt wird (lizenzabhängig). Vergeben Sie anschließend einen **Benutzernamen** und ein **Passwort** (4), mit denen der Loxone Miniserver die Anlage abfragen und – je nach Steuerzugriff – auch ansteuern kann.



Konfigurieren Sie diesen Benutzer mit dem Remote-Client-Typ „**Loxone**“ (5).

Die Auswahl „**Control mode permitted**“ (6) legt fest, ob die Anlage vom Miniserver angesteuert werden darf. Beachten Sie dabei, dass dies Auswirkungen auf den Vds Zertifizierungsgrad haben kann.

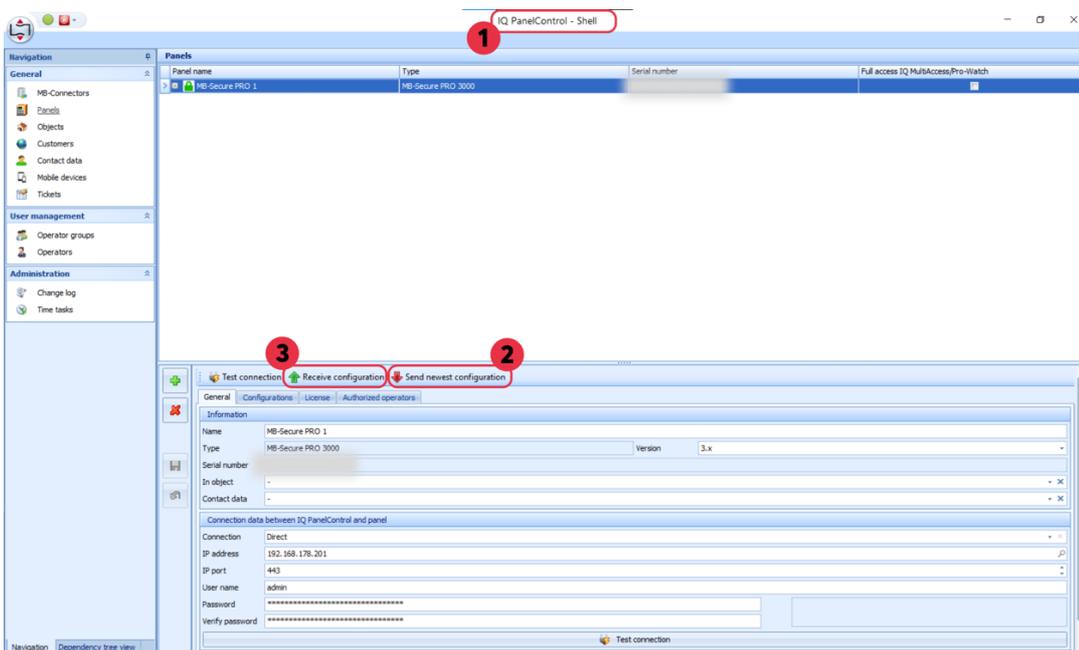
Speichern Sie anschließend die Datei (7) ab.



Wechseln Sie danach zurück in das Programmfenster IQ PanelControl „Shell“ (1) und senden Sie die Konfiguration über den roten Pfeil „Send newest configuration“ (2) an die Anlage.

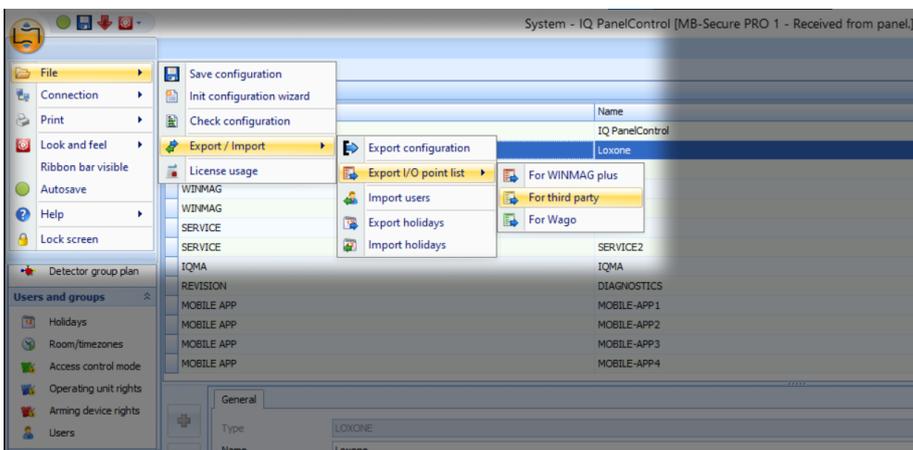
Wichtig: Danach muss die Konfiguration über den grünen Pfeil „Receive configuration“ (3) aus der Anlage geladen werden, um den aktuellen Zeitstempel zu hinterlegen, der für die Authentifizierung relevant ist.

Bei jeder Änderung oder Erweiterung müssen die folgenden Schritte erneut durchgeführt werden. Andernfalls gibt der Miniserver eine Fehlermeldung aus.



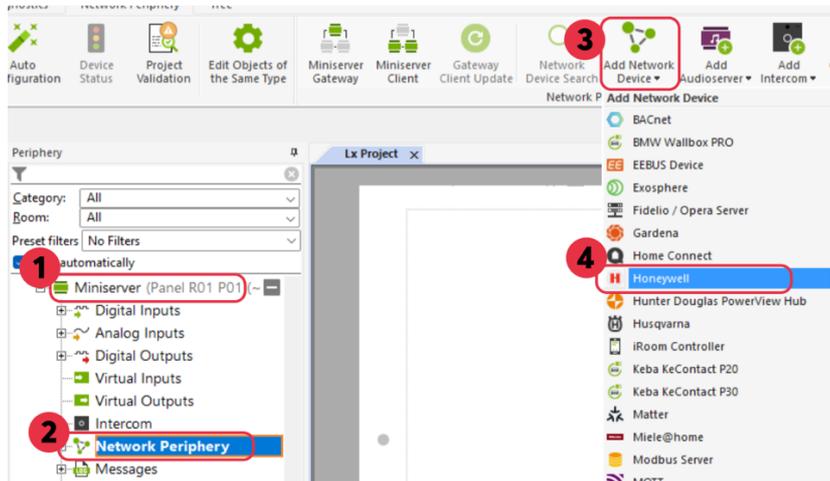
Erst dann kann die aktuelle Programmierung erneut geöffnet und die Ein- und (optional) Ausgänge als **OPIF-Datei** exportiert werden.

Exportieren Sie anschließend die Konfiguration der I/O-Liste aus der Datei. Dadurch erhalten Sie die „**OPIF-Datei**“, welche anschließend in die **Loxone Config** importiert werden muss.

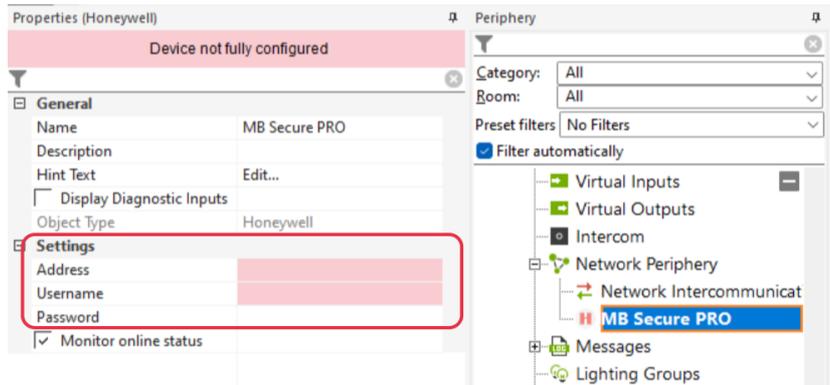


Loxone Config Settings:

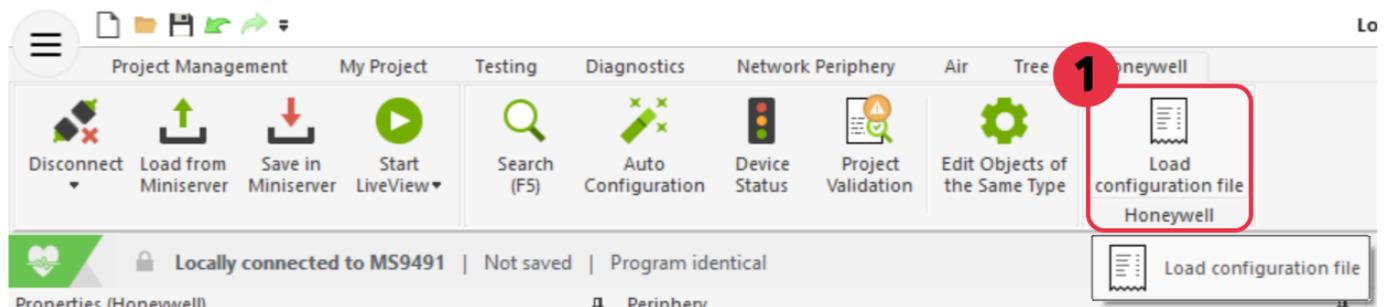
Fügen Sie in Ihrer Konfiguration beim Miniserver aus den **Netzwerkgeräten** das **Honeywell Security Plugin** hinzu.



Tragen Sie in den Einstellungen die **IP-Adresse** der Alarmanlage sowie den **Benutzernamen** und das **Passwort** ein, die Sie zuvor in der Honeywell Security Software erstellt haben.



Importieren Sie die **OPIF-Datei** unter „Konfigurationsdatei laden“ in die Config.



Die Eingänge werden anschließend automatisch erstellt.

Abhängig vom Steuerzugriff werden auch alle verfügbaren Ausgänge eingefügt.

