# Unified-E App Manager
# Benutzerhandbuch

## HMI-Server für Remote-Kommunikation und zentrale Datenhaltung

Software-Version 3.1.0.0, zuletzt aktualisiert: Juli 2025

Herausgeber: Unified-E AG, Winterthur, Schweiz

# Inhalt

# 1 Einleitung

Der Unified-E App Manager (kurz App-Manager) macht einen Windows-Computer zum HMI-Server und übernimmt die zentrale Verwaltung und Ausführung von HMI-Apps im Unified-E System. Er ist optional einsetzbar – Bediengeräte wie Panel-PCs oder Smartphones können auch ohne App-Manager direkt mit einer Steuerung kommunizieren.

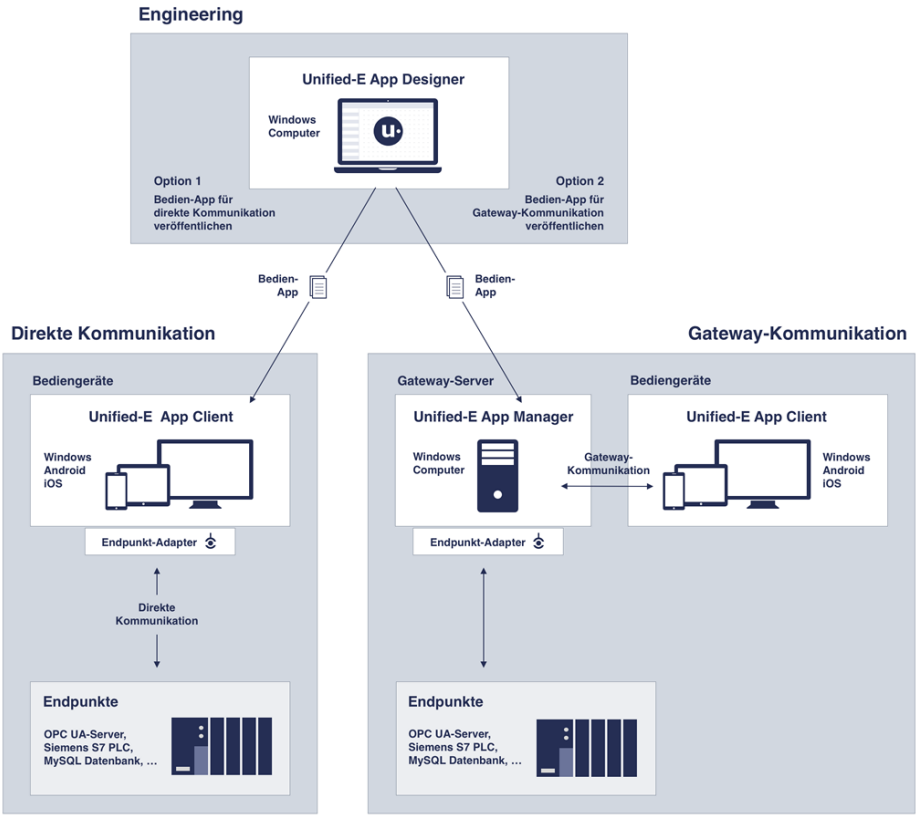
Der Einsatz des App-Managers empfiehlt sich, wenn eine Anlage über mehrere Bedienterminals verfügt, wenn die Bedienung über das Internet erfolgen soll oder wenn Visualisierungen und Daten zentral auf einem Server verwaltet werden sollen. In solchen Fällen fungiert der App-Manager als Gateway-Server: Er empfängt die Anfragen der Bediengeräte und leitet sie an die Zielsysteme wie SPS-Steuerungen weiter.

Dieses Handbuch bietet eine Einführung in Einsatz und Konfiguration des Unified-E App Managers – mit Fokus auf typische Einsatzszenarien in der industriellen Automation.

## 1.1 Softwareübersicht

### 1.1.1 Software-Komponenten

Unified-E besteht aus mehreren Programmen bzw. Softwarekomponenten, die wichtigsten Komponenten werden in folgender Abbildung veranschaulicht. Alle Programme können über die Unified-E Website heruntergeladen werden – für Entwicklungszwecke stehen alle Programme kostenlos zur Verfügung.



Unified-E App Designer:

Der Unified-E App Designer (kurz App-Designer) ist ein HMI-Editor, der zur Konfiguration der Bedien-App bzw. HMI-App verwendet wird. Die Konfiguration wird in einer Projektdatei gespeichert. Für den Einsatz zur Laufzeit erstellt der App Designer über die Funktion «Veröffentlichen» eine App-Paket-Datei, welche die Visualisierung in optimierter Form enthält.

Das Handbuch für den App-Designer kann über die Unified-E Website heruntergeladen werden.

Unified-E Client:

Der Unified-E Client wird als HMI-Client auf dem jeweiligen Bediengerät installiert. Er dient zur Ausführung der im App-Designer erstellten Visualisierung und ermöglicht so die Bedienung und Überwachung von Maschinen und Anlagen.

Die Visualisierung wird über eine App-Paket-Datei im Unified-E Client registriert und anschliessend zur Laufzeit verwendet.

Für Android- und iOS-Geräte ist der Unified-E Client (unter dem Namen «Unified-E App») im Google Play Store bzw. im Apple App Store verfügbar. Die Windows-Version des Clients kann über die Unified-E Website heruntergeladen werden.

Das Handbuch für den Unified-E Client kann über die Unified-E Website heruntergeladen werden.

Unified-E App Manager:

Der optionale Unified-E App Manager fungiert als HMI-Server mit zentraler Datenhaltung. Die Serverfunktion kommt dann zum Einsatz, wenn beispielsweise ein Smartphone über das Internet mit der Anlage kommunizieren soll oder mehrere Bediengeräte gleichzeitig auf eine Anlage zugreifen. Da der HMI-Server aus Sicht der Clients als Gateway fungiert, spricht man hier auch von Gateway-Kommunikation.

In den folgenden Unterkapiteln wird der Unified-E App Manager ausführlich bechrieben.

### 1.1.2 Direkte und Gateway-Kommunikation

Direkte Kommunikation (ohne Unified-E App Manager):

Direkte Kommunikation bedeutet, dass jedes Bediengerät (z. B. ein Panel-PC oder Smartphone) direkt mit der SPS kommuniziert. Diese Variante eignet sich besonders für einfache Anlagen mit wenigen Bediengeräten, da kein zusätzlicher Server benötigt wird und das Bediengerät mit nativen Kommunikationsprotokollen kommuniziert (ohne Web-Server). Bei direkter Kommunikation ist im Gegensatz zur Gateway-Kommunikation eine Direkt-Lizenz pro Bediengerät erforderlich, welche über den Unified-E Client zu registrieren ist.

Gateway-Kommunikation:

Bei der Kommunikation über den Unified-E App Manager spricht man von Gateway-Kommunikation. Alle Bediengeräte kommunizieren ausschliesslich mit dem Unified-E App Manager als Gateway, nicht direkt mit der SPS. In der folgenden Dokumentation geht es ausschliesslich um die Gateway-Kommunikation mit dem Unified-E App Manager.

## 1.2 Wichtige Begriffe

### 1.2.1 App

Bei Unified-E bezeichnet der Begriff «App» eine Bedien- bzw. HMI-App. Solche Apps können im Unified-E App Manager registriert werden und ermöglichen die Gateway-Kommunikation zwischen dem Bediengerät und den Endpunkten. Eine App wird als App-Paket-Datei gespeichert und über den App Manager installiert.

### 1.2.2 Bediengerät / HMI-Gerät

Ein Bediengerät (oder HMI-Gerät) ist aus Unified-E Sicht ein Computer mit einem Windows-, Android- oder iOS-Betriebssystem, auf dem die Visualisierung mit dem Unified-E Client Programm angezeigt wird. Typische Beispiele sind Industrie-Panel-PCs mit Windows, Android-Panels, Tablets, iPads, iPhones oder Smartphones.

Für die Ausführung einer HMI-App auf einem Bediengerät muss die Applikation «Unified-E Client» installiert sein (siehe Kapitel 1.1.1).

### 1.2.3 Endpunkt

Ein Endpunkt bezeichnet in Unified-E typischerweise eine SPS-Steuerung oder eine andere Datenquelle wie einen SQL-Server oder Webserver. Er wurde im App-Designer angelegt und vorkonfiguriert. Weitere Informationen zur Definition und zu unterstützten Adaptern finden Sie im Unified-E App Designer Handbuch.

Im Betrieb kommuniziert der App-Manager bei Gateway-Nutzung mit diesen Endpunkten und leitet die Daten zwischen Bediengeräten und Endpunkten weiter.

### 1.2.4 Gateway-PC

Ein Gateway-PC im Unified-E-Kontext ist ein Windows-Computer, auf dem der Unified-E App Manager als Windows-Dienst läuft. Er fungiert als HMI-Server für die verbundenen Bediengeräte und übernimmt die zentrale Datenhaltung sowie die Kommunikation mit den Endpunkten. Aus Sicht der Bediengeräte stellt der Gateway-PC ein Gateway zu den Endpunkten dar – etwa SPS-Steuerungen oder Datenserver. Die Bediengeräte kommunizieren nicht direkt mit den Endpunkten, sondern ausschliesslich über diesen zentralen Gateway-PC.

### 1.2.5 Gateway-Lizenz

Für den kommerziellen Einsatz des Unified-E App Managers ist eine Gateway-Lizenz erforderlich. Sie bestimmt, wie viele Bediengeräte gleichzeitig registriert sein dürfen und welche Kommunikationsarten freigeschaltet sind (siehe Kapitel 2.2). Eine Gateway-Lizenz kann online über die Unified-E Website erworben werden:

- Basic-Lizenz
  - Einmalige Aktivierung mit Internetverbindung
  - Danach offline nutzbar
  - Für mehrere Geräte im selben Netzwerk
  - Keine jährlichen Kosten (Festpreis-Lizenz)
  - App-Designer und Updates inbegriffen
- Standard-Lizenz
  - Jahresabonnement mit Online-Lizenzprüfung
  - Für mobile Bedienung über das Internet
  - App-Designer, Push-Dienste und Updates inbegriffen
- Pro-Lizenz
  - Wie Standard-Lizenz, zusätzlich:
  - Firewall-freundliche Internetkommunikation ohne Router-Konfiguration
  - Inklusive Relay-Dienst via Microsoft Azure

Für Entwickler steht im Unified-E Portal eine kostenlose Gateway-Lizenz zur Verfügung, die alle Funktionen der Standard-Lizenz abdeckt.

Bediengeräte, die über den Unified-E App Manager kommunizieren, benötigen keine zusätzliche Lizenzierung des Unified-E Clients am Bediengerät.

## 1.3 Einführung der HMI-Server Funktionen

Die folgenden Unterkapitel beschreiben die wichtigsten Funktionen der HMI-Server-Software.

### 1.3.1 Verschlüsselte Kommunikation mit Bediengeräten

Unabhängig von der gewählten Kommunikationsart erfolgt die Verbindung zwischen Bediengeräten und dem App-Manager stets verschlüsselt über das HTTPS-Protokoll. Die SSL-Zertifikate werden automatisch erstellt – mit konfigurierbarer Schlüssellänge – und gewährleisten eine sichere Datenübertragung.

Bei Verwendung einer Standard- oder Pro-Lizenz werden die SSL-Zertifikate regelmässig und automatisch erneuert. Die Bediengeräte erhalten die aktualisierten Zertifikatsinformationen unterbrechungsfrei über den Unified-E Onlinedienst.

### 1.3.2 Optimierte Endpunkt-Kommunikation

Wenn mehrere Bediengeräte oder Bedienterminals gleichzeitig mit einer HMI-App verbunden sind, wird die Kommunikation mit den Endpunkten über den App-Manager optimiert:

- Alle Bediengeräte teilen sich eine zentrale Endpunkt-Verbindung über den App-Manager
- Lese-Anfragen werden gebündelt, um die Anzahl der Zugriffe auf die Endpunkte zu minimieren

### 1.3.3 Unified-E App Manager als Windows Dienst

Der Unified-E App Manager läuft als Windows-Dienst und ist somit auch aktiv, wenn kein Benutzer am System angemeldet ist. Ein Windows-Server-Betriebssystem ist nicht erforderlich. Systemfunktionen wie die Überwachung von Meldungen bleiben aktiv – auch dann, wenn verbundene Bediengeräte ausgeschaltet sind, da die Meldeüberwachung zentral am App-Manager erfolgt.

### 1.3.4 Zentrale Datenhaltung

Alle bei einer HMI-App registrierten Bediengeräte greifen auf zentral verwaltete Daten zu – eine lokale Datenspeicherung auf den Bediengeräten erfolgt nicht. Zentral gespeichert werden insbesondere:

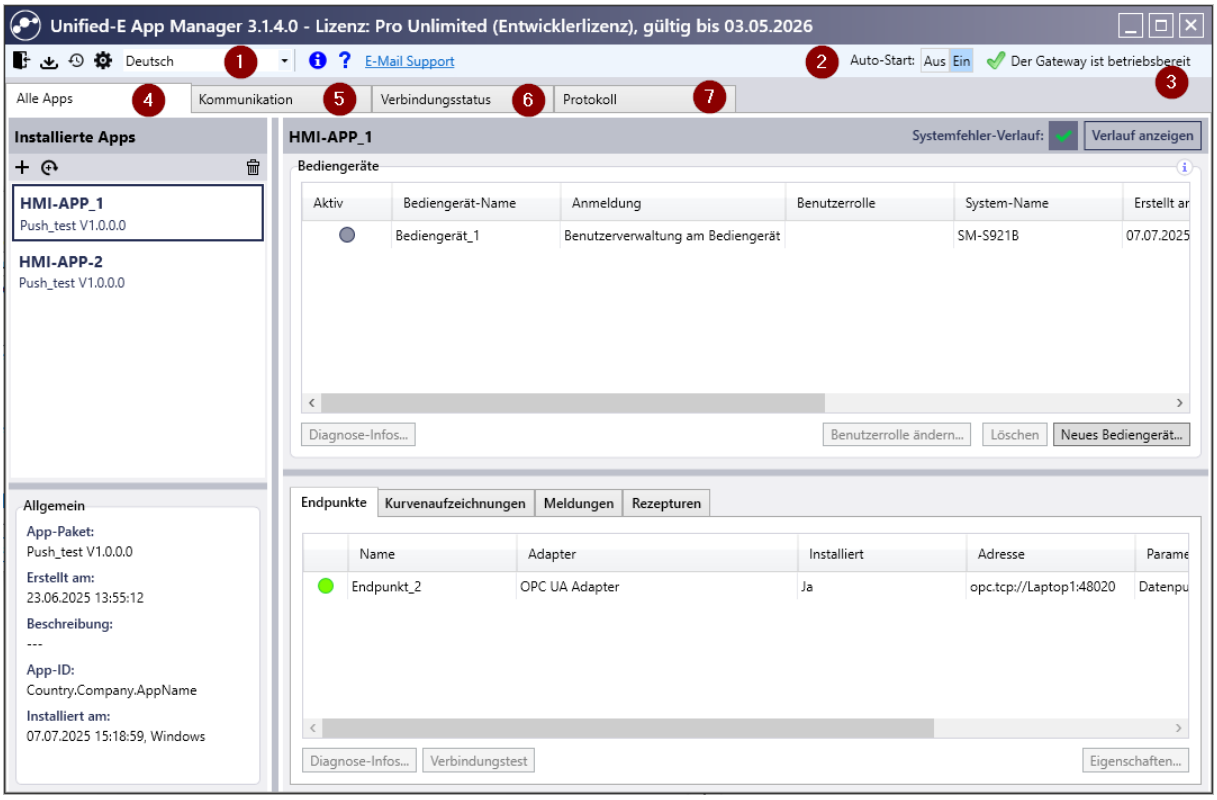
- Melde-Archiv
- Rezeptur-Datensätze
- Kurven-Aufzeichnungen

### 1.3.5 Host für mehrere HMI-Apps

Im App-Manager können mehrere Apps gleichzeitig registriert und ausgeführt werden. Dadurch lassen sich verschiedene Anlagen oder Maschinen mit nur einem App-Manager parallel betreiben. Das Verwalten von Apps wird ausführlich in Kapitel 3 beschrieben.

## 1.4 Die Oberfläche im Überblick

Die wichtigsten Bereiche der Oberfläche werden in folgender Abbildung verdeutlicht:




## Toolbar-Funktionen (Nummerierung gemäss Abbildung):

Folgende Toolbar-Funktionen stehen über Schaltflächen zur Verfügung.

1. Toolbar-Schaltflächen:
   a) Unified-E Windows Dienst herunterfahren:
   Schliesst nicht nur die Oberfläche, sondern beendet den Windows-Dienst. Die installierten Apps sind anschliessend nicht mehr für Bediengeräte erreichbar
   b) Update herunterladen und installieren:
   Lädt das neuste Update herunter (falls vorhanden) und installiert dieses. Der Windows-Dienst wird hier beendet
   c) Versionsverlauf anzeigen:
   Zeigt den Versionsverlauf und zugehörige Bemerkungen zu bisherigen Versionen an
   d) Einstellungen:
   Zeigt den Einstellungen Dialog (siehe Kapitel 6)
   e) Sprache:
   Legt die Sprache der Oberfläche fest (Deutsch, Englisch)
   f) Info:
   Zeigt einen Info-Dialog mit Programm-Informationen
   g) Hilfe:
   Öffnet das Handbuch im PDF-Reader

2. Auto-Start für Windows-Dienst:
   Legt fest, ob der Windows-Dienst automatisch beim Aufstarten von Windows gestartet werden soll
3. Betriebszustand-Anzeige:
   Zeigt den allgemeinen Betriebszustand bezüglich Lizenzierung und Gateway-Kommunikation. Der Verbindungszustand von Endpunkten wird hier nicht berücksichtigt

Verfügbare Register-Laschen (Nummerierung gemäss Abbildung):

4. Alle Apps:
   Hier werden alle HMI-Apps (bzw. Bedien-Apps) und die damit verknüpften Bediengeräte verwaltet (siehe Kapitel 3)
5. Kommunikation:
   Hier wird die Gateway-Lizenz verwaltet und die Kommunikationsart zwischen den Bediengeräten und App-Manager eingerichtet (siehe Kapitel 2)
6. Verbindungsstatus:
   Allgemeine Verbindungsprobleme auch zu den Endpunkten lassen sich hier schnell diagnostizieren
7. Protokoll:
   Wichtige Ereignisse werden hier protokolliert

# 2 Kommunikation mit Bediengeräten einrichten

Im Register «Kommunikation» wird die Gateway-Lizenz verwaltet. Abhängig von der Gateway-Lizenz stehen verschiedene Kommunikationsarten zur Verfügung.

## 2.1 Gateway-Lizenz Anmeldung

### 2.1.1 Aktuelle Lizenz-Informationen anzeigen

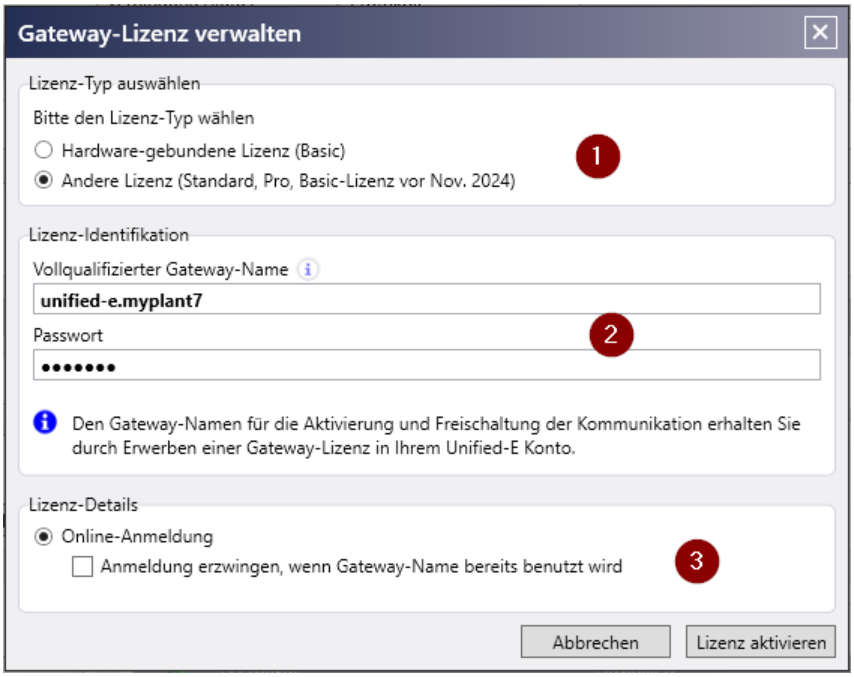
In der Gruppe «Gateway-Lizenz» ist der vollqualifizierte Gateway- bzw. Lizenz-Name der aktivierten Lizenz zu sehen. Der Lizenzname ist eindeutig und enthält daher auch den Unified-E Konto-Namen als Präfix.

Folgende Links sind in dieser Gruppe zu finden:

- Lizenzdetails: Zeigt in einem Dialog Detail-Informationen zur Lizenz, z. B. die erlaubte Bediengeräte-Anzahl
- Mein Konto: Öffnet die «Anmelden» Seite zum Anmelden im Unified-E Konto
- Kostenlose Lizenzen: Öffnet einen Dialog. Neben der Entwicklerlizenz (siehe Kapitel 1.2.5) kann hier einmalig eine 30 Tage Pro-Lizenz kostenlos erworben werden. Die Pro-Lizenz ermöglicht eine unkomplizierte Kommunikation via Internet ohne Router-/Firewall-Konfiguration

### 2.1.2 Lizenz aktivieren

Beim ersten Start des App-Managers muss die Gateway-Lizenz einmalig aktiviert werden, um alle Funktionen freizuschalten. Gehen Sie dazu im Register «Kommunikation» zur Gruppe «Gateway-Lizenz» und klicken Sie auf die Schaltfläche «Gateway-Lizenz verwalten…». Im angezeigten Dialog geben Sie die Lizenzdaten ein und führen die Aktivierung durch.

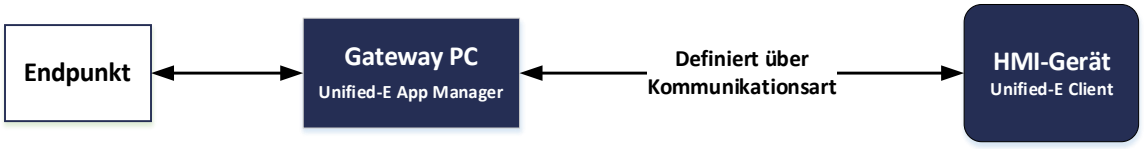



Bereiche (Nummerierung gemäss Abbildung):

1. Lizenz-Typ auswählen:
   Der Lizenztyp ist hier zu wählen. Hardware-gebundene Lizenzen sind an der Hardware-gebunden und können nur eine begrenzte Anzahl übertragen werden.
2. Lizenz-Identifikation:
   Für die Lizenz-Identifikation wird der Lizenzname benötigt, der online beim Erwerben der kommerziellen oder Entwickler-Lizenz vergeben wurde.
   a) Vollqualifizierter Gateway-Name: Der vollqualifizierte Gateway-Name hat die folgende Struktur: <Unified-E-Kontoname>.<Lizenz-Name>
   Beispiel: mycompany.mygateway1
   b) Passwort: Das Passwort, das für die Lizenz gesetzt wurde.
3. Lizenz-Details (Abo-Lizenz):
   Aktivieren Sie das Kontrollkästchen «Anmeldung erzwingen, wenn Gateway-Name bereits benutzt wird», wenn die eingegebene Lizenz bereits früher bei einem anderen Gateway-PC vergeben wurde. Abo-Lizenzen sind beliebig übertragbar, aber nur ein Gateway-PC kann gleichzeitig für eine Abo-Lizenz verknüpft sein.

## 2.2 Kommunikationsart mit Bediengerät festlegen

Bei Verwendung des App-Managers läuft die Kommunikation zwischen dem HMI-Gerät (z. B. Smartphone, HMI-Panel-PC) und den Endpunkten immer über den App-Manager, welcher als Gateway fungiert.




Der App-Manager bietet mehrere Kommunikationsarten, die die Kommunikation zwischen Gateway-PC und HMI-Gerät bestimmen, die in folgenden Unterkapiteln vorgestellt werden.

Konfigurieren der Kommunikationsart:

Die Kommunikationsart muss im Register «Kommunikation» in der Gruppe «Kommunikation Grundeinstellungen» festgelegt werden.

Je nach Lizenztyp sind nicht alle Kommunikationsarten einstellbar. Die verschiedenen Kommunikationsarten werden in den folgenden Kapiteln genauer beschrieben.

### 2.2.1 Kommunikationsart «Internet (Firewall-freundlich)»

Diese Kommunikationsart erlaubt Zugriffe auf Endpunkte aus dem Internet, ohne dass eingehende Verbindungsanfragen über das Internet behandelt werden müssen, hierfür müssen keine Ports geöffnet werden. Diese Kommunikationsart ist ohne jegliche Netzwerk-Konfiguration sofort aktivierbar und steht nur bei der Pro-Gateway-Lizenz zur Verfügung.

Da die Kommunikation immer über einen Relay-Messaging Service (Zusatz-Server im Internet) abgewickelt wird (also indirekt erfolgt), ist die Geschwindigkeit etwas langsamer als bei der der Kommunikationsart «Internet (Direkt)».

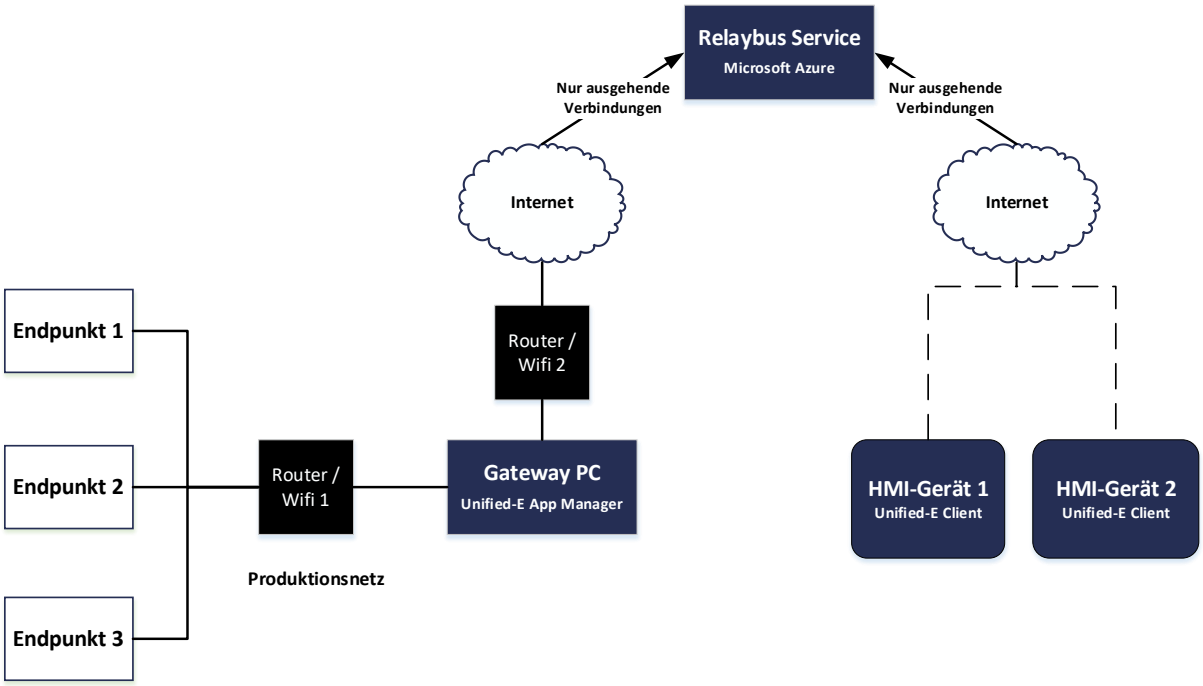
Sicherheit:

Da keine eingehenden Internet-Verbindungen notwendig sind und keine Ports geöffnet werden müssen, wird diese Kommunikationsart als sehr sicher betrachtet. Der Relay-Messaging-Service aktualisiert ebenfalls regelmässig das SSL-Zertifikat und benutzt eine hohe Verschlüsselung.

Zusätzliche Konfigurationen im Netzwerk:

Es sind keine zusätzlichen Konfigurationen wie Port-Weiterleitungen erforderlich. Auch die öffentliche IP-Adresse des Routers ist irrelevant.

Topologie-Beispiel:




Anwendungsfall:

Die Anlage soll mobil via Internet am Smartphone überwacht werden, ohne Port- oder Firewall-Konfigurationen durchführen zu müssen.

Notwendiger Lizenztyp:

Für diese Kommunikationsart ist die Pro-Gateway-Lizenz erforderlich.

### 2.2.2 Kommunikationsart «Internet (Direkt)»

Das Smartphone kommuniziert direkt mit dem App-Manager (Gateway-PC), welcher sowohl am Internet als auch im lokalen (Produktions-)Netz angebunden ist. Diese Kommunikationsart erfordert das Einrichten von Port-Weiterleitungen beim Router oder der Firewall.

Sicherheit:

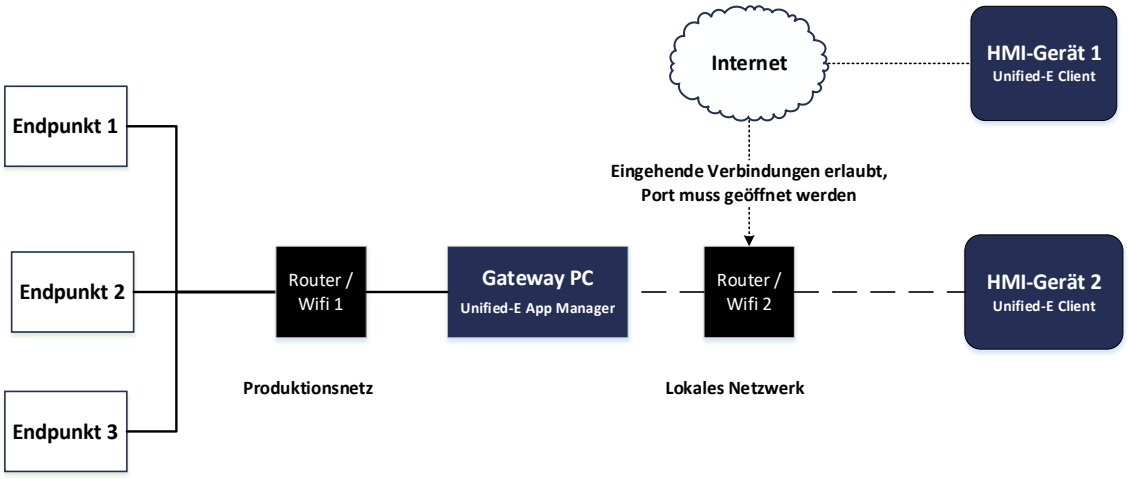
Es müssen eingehende Verbindungsanfragen aus dem Internet behandelt werden, so dass eine Port-Weiterleitung beim Router eingerichtet werden muss.

Offene Ports ohne weitere Massnahmen werden grundsätzlich als potenzielles Risiko angesehen. Diese Betriebsart sollte daher nur von IT-Administratoren mit Netzwerkkenntnissen eingerichtet werden.

Mögliche Massnahmen, um die Sicherheit zu erhöhen:

- App-Manager in einer DMZ (demilitarized Zone) betreiben
- Einsatz zusätzlicher Firewalls

Topologie-Beispiel:




Anwendungsfall:

Die Anlage soll stationär auf einer Bedienstation und zusätzlich mobil via Internet am Smartphone überwacht werden. Ein VPN wird nicht benötigt, die Anlage befindet sich in einem einfachen Netzwerk mit uPnP-Router. Meldungen sollen in Form von Push-Benachrichtigungen an das Smartphone gesendet werden.

Notwendiger Lizenztyp:

Für diese Kommunikationsart ist die Standard-Gateway-Lizenz erforderlich.

Die Kommunikationsart «Internet (Direkt)» wird in zwei Unter-Modi unterteilt – «Manuell» und „Automatisch (UPnP)“. Diese werden in den Folgekapiteln beschrieben und unterscheiden sich darin, ob eine statische oder dynamische öffentliche IP-Adresse vorliegt und ob der Router einen uPnP-Zugriff erlaubt.

#### 2.2.2.1 Port-Weiterleitung einrichten «Manuell»

Bei dieser Kommunikationsart ist der Hostname (externe IP-Adresse, DNS-Adresse, DynDNS-Adresse) manuell in der Gruppe «Gateway-Adresse» einzutragen.

Zusätzliche Konfigurationen im Netzwerk:

- Port-Weiterleitung
    - Einrichten beim WAN-Router
    - Einrichten bei beteiligten Firewalls/interne Router

- Externe (öffentliche) IP-Adresse
    - Variante 1: Eine statische IP-Adresse verwenden
    - Variante 2: Dynamische IP-Adresse verwenden
        - Variante 1: DynDns-Adresse verwenden (z. B. no-ip.org)
        - Variante 2: Update-URL, wie unten beschrieben, beim Router setzen

Dynamische externe IP-Adresse & Update-URL:

Falls der WAN-Router individuelle Update-URLs unterstützt, dann ist keine DynDNS - Adresse oder statische feste Adresse notwendig. Mit folgender Update-URL wird die IP-Adresse zum Gateway-Namen automatisch beim Unified-E Onlinedienst aktualisiert, so dass Smartphones auch nach einer IP-Adressänderung mit dem App-Manager kommunizieren kann.

Aufbau der Update-URL für Unified-E:

https://unified-e.com/api/Gateways/UpdatePublicIp?account=<Account-Name>&gateway=<Gateway-Name>&password=<Passwort>

Update-URL beim DynDNS-Router eintragen:

Tragen Sie Ihren Konto- und Gateway-Namen in die jeweiligen Platzhalter der URL ein. Diese URL ist dann beim WAN-Router einzutragen und wird immer dann aufgerufen, wenn sich die externe IP-Adresse geändert hat.

Gateway-Adresse im App-Manager löschen:

Beim Verwenden der Update-URL muss der Eintrag „DNS- oder IP-Adresse“ in der Gruppe „Gateway-Adresse“ gelöscht werden.

#### 2.2.2.2 Port-Weiterleitung automatisch einrichten «Automatisch (UPnP)»

Folgende Voraussetzungen müssen für diese Kommunikationsart erfüllt sein:

- Der Gateway-PC muss direkten Zugriff zum WAN-Router haben, der eine öffentliche (dynamische) IP-Adresse hat
- Beim WAN-Router muss UPnP zum Schreiben aktiviert sein

Beim Verwenden dieser Betriebsart sind keine weiteren manuellen Netzwerk-Konfigurationen erforderlich, da die Port-Weiterleitung am Router automatisch mittels UPnP erfolgt.

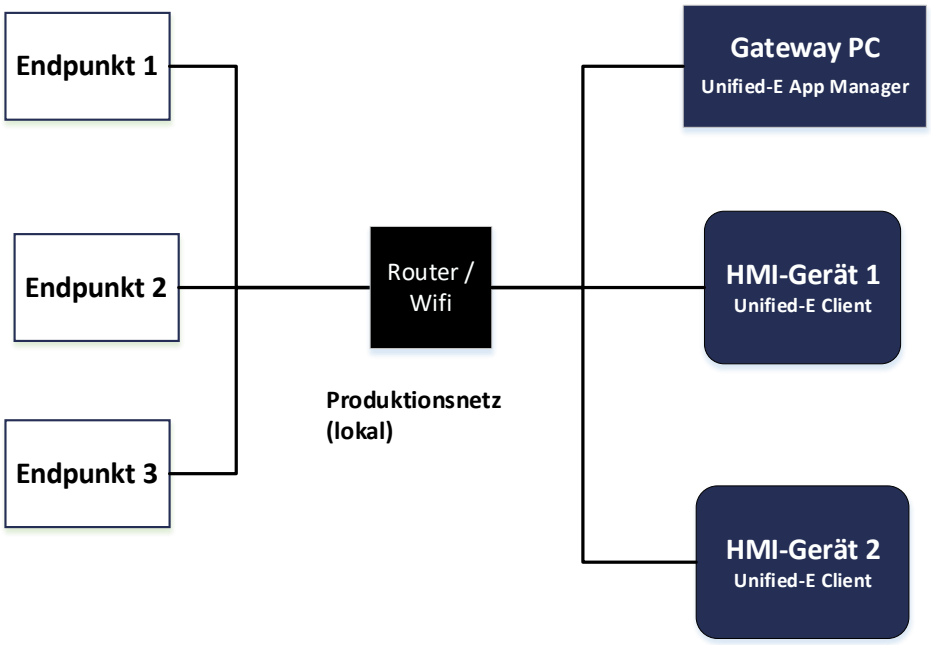
Informationen für weitere Kommunikationseinstellungen im App-Manager finden Sie in Kapitel 2.2.5.

### 2.2.3 Kommunikationsart «Offline (kein Internet)»

Diese Kommunikationsart ist nur kombiniert mit einer Basic-Gateway-Lizenz (Hardware-gebundenen Festpreis-Lizenz) verwendbar. Der App-Manager benötigt keine Internet-Anbindung – ausser für die Lizenz-Aktivierung. Online-Dienste von Unified-E werden hier nicht unterstützt – beispielsweise können keine Push-Benachrichtigungen via Internet an ein Smartphone versendet werden.

Diese Kommunikationsart ist geeignet, wenn sich alle HMI-Bediengeräte im selben Netzwerk wie der App-Manager befinden. Dies könnte via Internet auch im VPN ermöglicht werden.

Topologie-Beispiel:




Anwendungsfall:

Alle Bediengeräte befinden sich im Produktionsnetz ohne Internet. Unified-E Online-Dienste wie Push-Benachrichtigungen via Internet sind nicht notwendig.

Notwendiger Lizenztyp:

Für diese Kommunikationsart ist die Basic-Gateway-Lizenz erforderlich.

### 2.2.4 Kommunikationsart «Lokales Netzwerk»

Bei dieser Kommunikation müssen sich die verknüpften HMI-Geräte und der Gateway-PC mit dem App-Manager im selben Subnetz befinden. Der App-Manager ist hier über das Internet verbunden, Port-Weiterleitungen beim Router werden nicht manuell oder automatisch konfiguriert.

Im Gegensatz zur Kommunikationsart „Offline“ muss der App-Manager regelmässig mit dem Internet verbunden sein. Je nach App-Konfiguration werden Push-Nachrichten über den Unified-E Onlinedienst beim Eintreffen von Meldungen an das Smartphone verschickt.

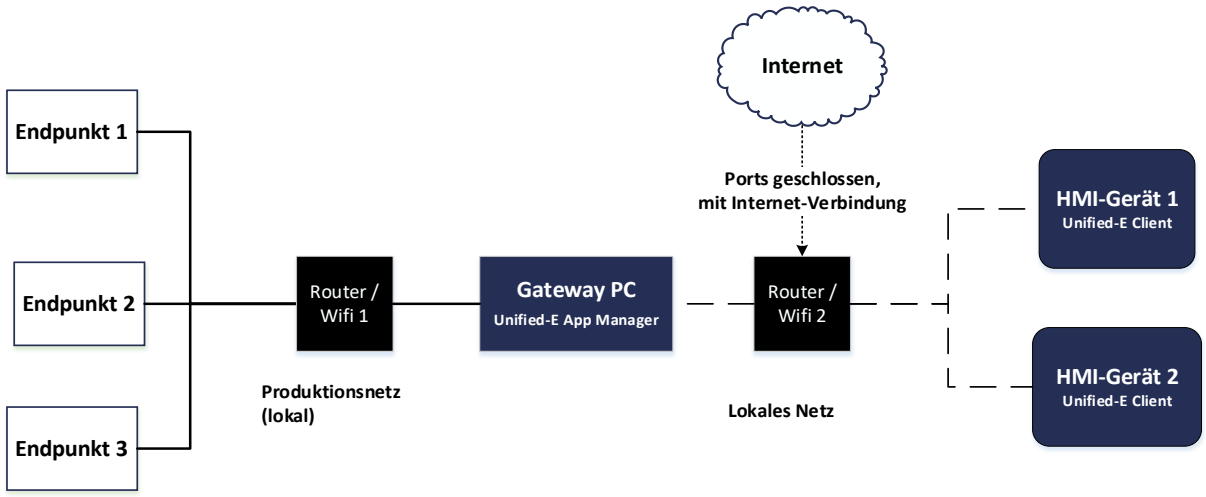
Sicherheit:

Da bei dieser Kommunikationsart keine eingehenden Verbindungen über das Internet verwendet werden, kann der App-Manager im Netzwerk mit ein- oder mehrstufigem Firewall-Konzept ohne Sicherheitsbedenken in der Intranet-Zone betrieben werden.

Zusätzliche Netzwerkkonfigurationen:

Es sind keine Einstellungen am WAN-Router vorzunehmen, da über das Internet keine eingehenden Anfragen behandelt werden müssen. Es müssen auch keine externen Firewalls konfiguriert werden.

Topologie-Beispiel:




Anwendungsfall:

Alle Bediengeräte befinden sich im Produktionsnetz und zusätzlich im Internet – eine Port-Weiterleitung muss nicht eingerichtet werden. Unified-E Online-Dienste wie Push-Benachrichtigungen via Internet sind möglich.

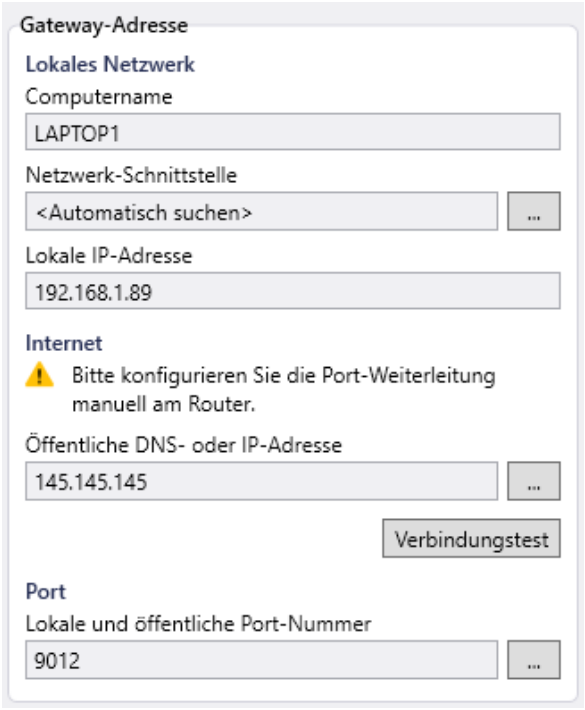
Notwendiger Lizenztyp:

Für diese Kommunikationsart ist die Standard-Lizenz notwendig.

## 2.2.5 HTTPS-Server Einstellungen für eingehende Verbindungen

### 2.2.5.1 Gateway-Adresse konfigurieren

Für alle Kommunikationsarten - ausser «Internet (Firewall-freundlich)» - muss die Gateway-Adresse in der Gruppe «Gateway-Adresse» konfiguriert werden.




Netzwerk-Schnittstelle auswählen:

Die gewählte Netzwerk-Schnittstelle bestimmt, welche IP-Adressen für den Gateway (Gateway-Namen) veröffentlicht wird.

Öffentliche DNS- oder IP-Adresse ändern:

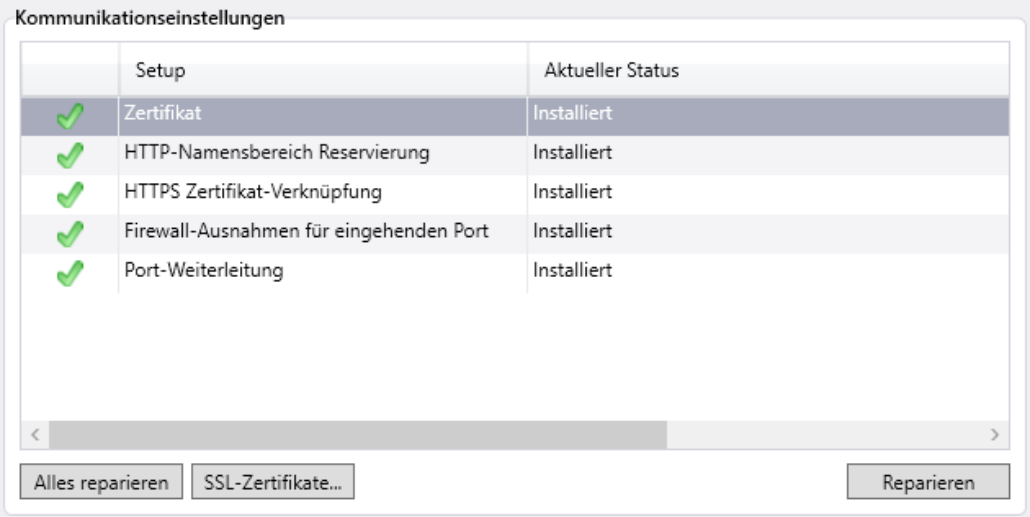
Dieses Feld ist nur für «Internet (Direkt) ->Manuell» einstellbar. Damit wird die externe IP-Adresse des Gateways manuell gesetzt (siehe auch Kapitel 2.2.2.12.2.2.1).

Port ändern:

Dort ist die Port-Nummer zu setzen, auf die der HTTPS-Server im Windows-Dienst für eingehende Verbindungen lauscht. Die Port-Nummer wird sowohl für die Kommunikation im LAN als auch über das Internet verwendet (symmetrisch).

### 2.2.5.2 Erweiterte Kommunikationseinstellungen

Die erweiterten Kommunikationseinstellungen werden automatisch eingerichtet. Die Liste in der Gruppe «Kommunikationseinstellungen» dient der Überprüfung, ob die automatische Einrichtung erfolgreich war.




Mögliche Status-Zeilen für die Kommunikationsvoraussetzungen:

- Zertifikat: Prüft, ob das SSL-Zertifikat erfolgreich erstellt wurde.
    - Die Smartphones überprüfen die Gültigkeit des Zertifikats unter anderem über den Fingerabdruck
    - Bei Kommunikationsart «Offline» gilt: Wenn das Zertifikat erneuert wird, dann müssen sich alle Bediengeräte erneut registrieren
- HTTP-Namensbereich Reservierung: Prüft, ob dem Windows-Dienst „Unified-E Server“ die Rechte für das Lauschen am Port zugeteilt wurden
- HTTPS Zertifikat-Verknüpfung: Prüft, ob der Port mit dem richtigen SSL-Zertifikat verknüpft ist
- Firewall-Ausnahmen für eingehenden Port: Prüft, ob bei der Windows-Firewall die Ausnahme-Regel für eingehende Verbindungen am eingestellten Port unter „Gateway-Adresse“ eingetragen ist
- Port-Weiterleitung (nur bei UPnP): Prüft, ob die Port-Weiterleitung beim WAN-Router erfolgreich eingetragen wurde

Alle Kommunikationsvoraussetzungen werden vom Unified-E Dienst automatisch eingerichtet. Diese könnten gestört werden durch das Installieren anderen anderer Anwendungen (z. B. andere Server-Applikation benutzt denselben Port) oder durch fehlende Berechtigungen des Windows-Dienstes.

#### 2.2.5.3 Kommunikations-Komponenten reparieren

Bei Fehlerzuständen in der obigen Liste kann eine erste Abhilfe eine «Reparieren»-Aufforderung sein, welche über Schaltflächen gestartet werden kann:

- Schaltfläche «Alles reparieren»: Es wird versucht, die gestörte Kommunikation zu reparieren bzw. wiederherzustellen, so dass alle Kommunikationsvoraussetzungen erfüllt sind

- Schaltfläche «Reparieren»: Die ausgewählte Zeile in der Liste (Kommunikations-Komponente) wird automatisch repariert, wenn möglich

Mögliche Ursachen für eine nicht korrekte Installation der Kommunikation:

- Port-Konflikt mit einer anderen Anwendung
- Spezielle Windows-Firewall oder nur eingeschränkte Rechte, die Firewall zu konfigurieren
- Kein UPnP-Zugang zum Router (bei UPnP-Betriebsart)

Mögliche Massnahmen bei Fehlern:

Häufig reicht es, den Port zu ändern. Nach einigen Sekunden wird die Spalte „Aktueller Status“ aktualisiert.

#### 2.2.5.4 SSL-Zertifikate

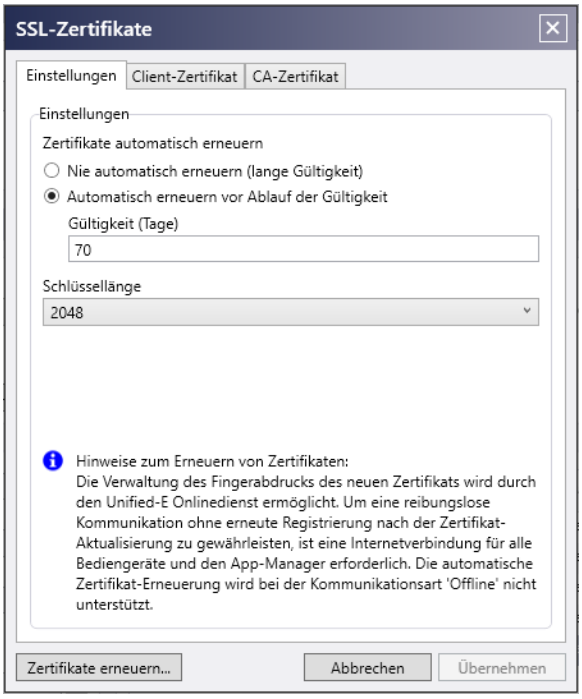
Der im App-Manager eingebettete HTTPS-Server muss für die verschlüsselte Kommunikation ein Zertifikat bereitstellen. Dies gilt für alle Kommunikationsarten, ausser bei Firewall-freundlicher Kommunikation.

Sichere, selbst-signierte Zertifikate:

Der App-Manager erstellt die Zertifikate selbst und hinterlegt im Unified-E Onlinedienst den Zertifikat-Fingerabdruck zum Gateway-Namen des App-Managers. Der Unified-E Client prüft beim Verbinden über den Fingerabdruck, ob die Kommunikation mit dem richtigen Server verbunden ist und kann so sicher und verschlüsselt kommunizieren.

SSL-Zertifikat-Erneuerung konfigurieren:

In der Gruppe «Kommunikations-Einstellungen» kann über die Schaltfläche «SSL-Zertifikate» der Dialog für die Konfiguration der Zertifikat-Erneuerung geöffnet werden.




In diesem Dialog konfigurieren Sie Einstellungen zur Verwaltung und Erneuerung von SSL-Zertifikaten, die für die verschlüsselte Kommunikation mit dem Unified-E App Manager verwendet werden.

- Zertifikate automatisch erneuern: Legt fest, ob und wann ein neues Zertifikat automatisch erstellt und installiert wird:
    - Nie automatisch erneuern (lange Gültigkeit): Das Zertifikat bleibt über die gesamte Gültigkeitsdauer aktiv. Es erfolgt keine automatische Erneuerung
    - Automatisch erneuern vor Ablauf der Gültigkeit: Der App Manager erneuert das SSL-Zertifikat automatisch, sobald die verbleibende Gültigkeitsdauer unterschritten wird
- Gültigkeit (Tage): Anzahl Tage vor Ablauf des aktuellen Zertifikats, ab wann die Erneuerung ausgelöst wird
- Schlüssellänge: Wählen Sie die gewünschte Schlüssellänge für das Zertifikat aus. Die Standardlänge beträgt 2048 Bit. Grössere Schlüssellängen erhöhen die Sicherheit, können aber die Performance leicht beeinträchtigen

Hinweis zur Zertifikat-Erneuerung:

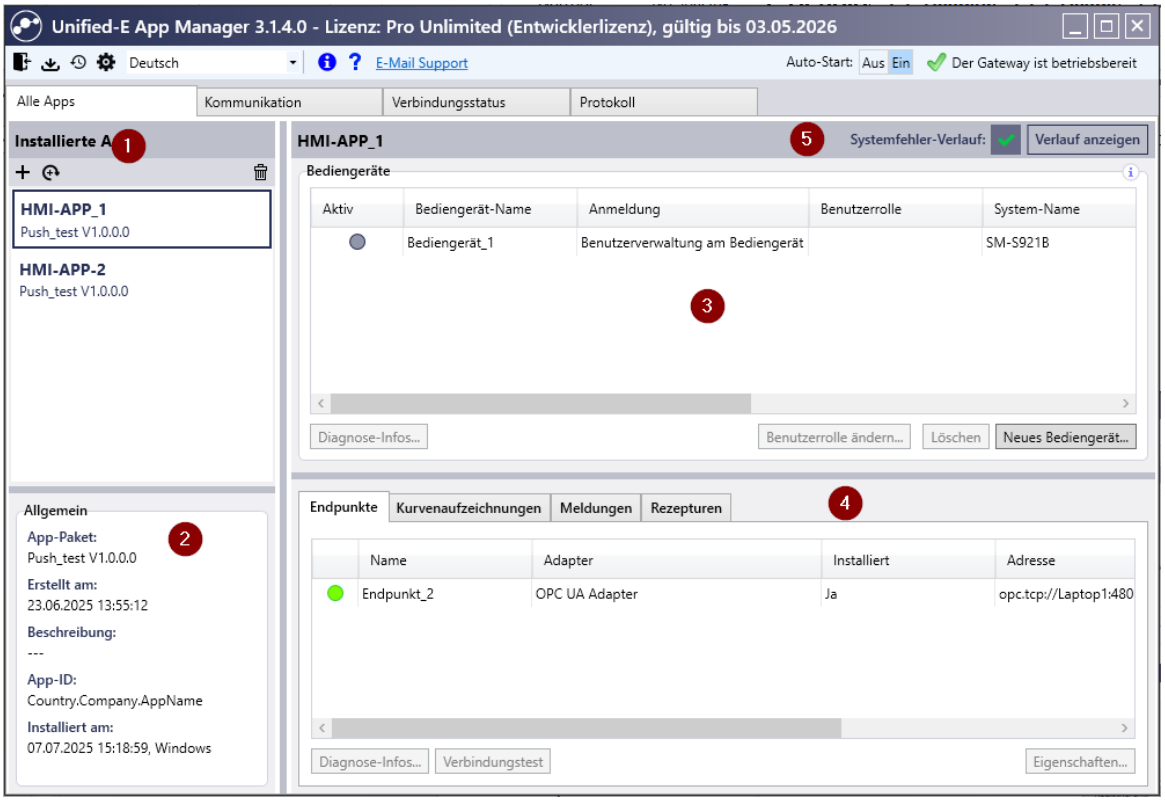
Die Erneuerung und Registrierung neuer Zertifikate erfordert eine funktionierende Internet-Verbindung zu den Unified-E Onlinediensten.

Bei Verwendung der Kommunikationsart «Offline» ist die automatische Erneuerung von Zertifikaten nicht sinnvoll, da der Online-Dienst hier nicht zur Verfügung steht. Nach einer Erneuerung müssen sich alle Bediengeräte erneut registrieren.

# 3 HMI-Apps verwalten

## 3.1 Überblick

Die gehosteten Apps werden im Register «Alle Apps» verwaltet. Es können mehrere Apps gleichzeitig betrieben werden, z. B. eine spezifische App pro Anlage oder Maschine innerhalb einer Produktionshalle.




Bereiche (Nummerierung gemäss Abbildung):

1. Installierte Apps:
   Hier lassen sich Apps installieren oder auch löschen. Beim Auswählen einer App werden unten und rechts weitere Funktionen für die ausgewählte App angezeigt.
2. Allgemein:
   Zeigt allgemeine App-Eigenschaften an.
3. Bediengeräte:
   Hier werden neue Bediengeräte registriert bzw. mit dem App-Manager verknüpft. Für die Registrierung muss beim Bediengerät die Unified-E Client Anwendung (bzw. «Unified-E» App bei Android- und iOS-Geräten) installiert sein. Nach der einmaligen Registrierung kann die App am Bediengerät beliebig oft gestartet bzw. ausgeführt werden.
4. Weitere Funktionen:
   Hier sind weitere Funktionen der ausgewählten App zu finden, welche in folgenden Unterkapiteln detailliert beschrieben werden.

### 3.1.1 HMI-App hinzufügen

Das Hinzufügen einer App erfolgt im Bereich «Alle Apps». Über das Kontextmenü oder auch mit dem «+»-Symbol in der lokalen Toolbar kann das Hinzufügen gestartet werden.

App hinzufügen:

1. Klicken Sie auf die Toolbar-Schaltfläche «+».
2. Wählen Sie die App-Paket-Datei der gewünschten App im Öffnen-Dialog, für das eine neue App-Instanz angelegt werden soll (die App-Paket-Datei wird im App-Designer beim «Veröffentlichen»-Vorgang generiert).
3. Wählen Sie einen App-Namen. Dieser muss innerhalb des App-Managers eindeutig sein.
4. Setzen Sie die Endpunkt-Parameter, falls notwendig (Kapitel 3.1.3).
5. Registrieren Sie neue Bediengeräte. (Kapitel 3.1.2.1)

App löschen:

Die ausgewählte App kann über das Kontextmenü gelöscht werden. Registrierte Bediengeräte können anschliessend nicht mehr auf diese App zugreifen.

App aktualisieren:

Ein App-Aktualisierung kann über das Kontextmenü unter dem Eintrag «Ausgewählte App aktualisieren» gestartet werden.

Beim Aktualisieren einer App (z. B. Änderungen in den Ansichten) ist die neue App-Paket-Datei auszuwählen. Bediengeräte erhalten beim Verbinden die Aktualisierungen automatisch, dafür ist keine Neuregistrierung der Bediengeräte erforderlich.

### 3.1.2 Bediengeräte verwalten

Im Bereich «Bediengeräte» verwalten Sie alle verknüpften Bediengeräte der ausgewählten App. Sie können neue Bediengeräte hinzufügen oder vorhandene löschen. Die Anzahl zulässiger Bediengeräte richtet sich nach der in der Lizenz festgelegten Obergrenze. Entscheidend ist dabei die Gesamtanzahl aller registrierten Bediengeräte über alle Apps hinweg.

Bediengeräte-Tabelle:

Die Tabelle zeigt alle registrierten Bediengeräte an und hat folgende Spalten:

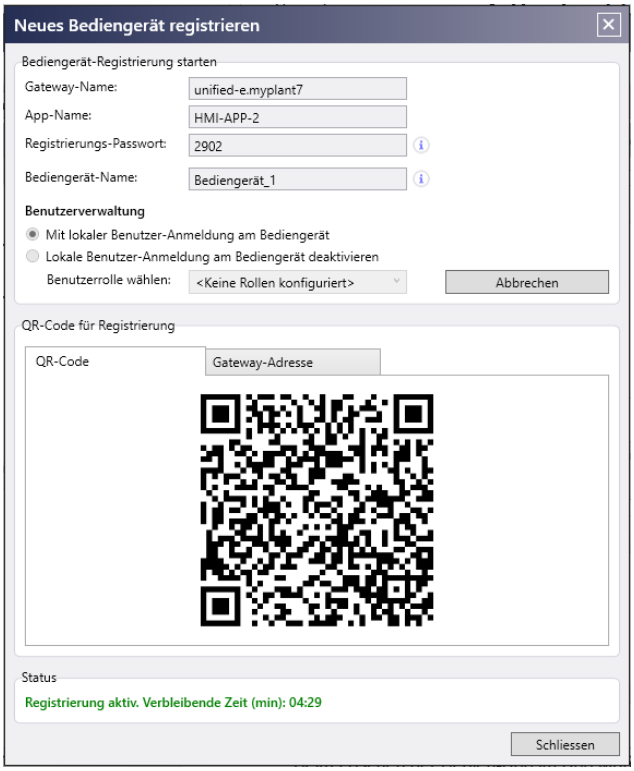
- Aktiv: Zeigt an, ob das Bediengerät gerade verbunden ist. Im Tooltip des Symbols können Status-Details eingesehen werden oder auch der Diagnose-Infos-Dialog geöffnet werden, um verschiedene Statistik-Werte für Diagnosezwecke anzuzeigen

- Bediengerät-Name: Name des Bediengeräts, der beim Registrieren vergeben wurde
- Anmeldung: Zeigt an, ob die lokale Benutzerverwaltung am Bediengerät aktiv ist
- Benutzerrolle: Zeigt die Benutzerrolle, die am Bediengerät für alle Benutzer gilt (falls die lokale Benutzerverwaltung deaktiviert ist und Benutzerrollen definiert wurden)
- System-Name: Bediengerät-Typ-Name
- Erstellt am: Datum, wann das Bediengerät hinzugefügt wurde
- Letzter Zugriff: Letzte Verbindung des Bediengeräts mit dem App-Manager
- Sprache: Aktuell gesetzte Sprache der App beim Start

#### 3.1.2.1 Bediengerät hinzufügen

Schritt 1: Bediengerät-Registrierung im App-Manager vorbereiten

Der Dialog «Neues Bediengerät registrieren» wird mit der Schaltfläche «Neues Bediengerät…» geöffnet.




Schritt 2: Allgemeine Registrierungsparameter im Dialog setzen:

- Gateway-Name (schreibgeschützt): Name des Gateways, über das das Bediengerät kommuniziert. Der Name wird über den Lizenz-Namen vorgegeben (siehe Kapitel 2.1.1)
- App-Name (schreibgeschützt): Der Name der App, die auf dem neuen Bediengerät registriert bzw. installiert werden soll. Dieser wird bei der Registrierung an das Gerät übermittelt und dort angezeigt

- Registrierungs-Passwort (schreibgeschützt): Sicherheitscode zur Anmeldung des Geräts am Gateway. Dieses Passwort muss beim Registrierungsprozess am Bediengerät eingegeben oder durch den QR-Code automatisch übernommen werden. Das Passwort wird erst beim Starten des Registrierungsvorgangs vergeben (nachdem die «Starten»-Schaltfläche geklickt wurde)
- Bediengerät-Name: Eindeutiger Name für das Bediengerät innerhalb der HMI-App. Dieser Name erscheint später z. B. in der Liste der registrierten Bediengeräte
- Benutzerverwaltung: Steuert die Berechtigungen oder die lokale Benutzeranmeldung am Bediengerät
    - Mit lokaler Benutzer-Anmeldung am Bediengerät: Das Bediengerät verlangt beim Start eine Benutzerauthentifizierung. Die Benutzer werden lokal im Bediengerät verwaltet. Nur möglich, wenn Benutzerrollen vorhanden und die lokale Benutzerverwaltung im HMI-Projekt nicht deaktiviert wurde
    - Lokale Benutzer-Anmeldung am Bediengerät deaktivieren: Es erfolgt keine Benutzeranmeldung am Bediengerät. Die Visualisierung startet sofort nach dem Öffnen
        - Benutzerrolle wählen: Wenn Benutzerrollen konfiguriert sind, kann hier die Rolle gewählt werden, die dem Bediengerät beim Starten zugewiesen wird

Schritt 3: Bediengerät-Registrierung starten (Pairing):

Sind alle oben gelisteten Parameter gesetzt, dann kann die Registrierung mit der Schaltfläche «Starten» gestartet werden. Es stehen 5 Minuten für die Bediengerät-Registrierung zur Verfügung, die am Bediengerät wie unten beschrieben via QR-Code oder manuell erfolgen kann.

Registrierung via QR-Code:

Für Smartphone und Tablets bietet sich die Bedienregistrierung via QR-Code an. Dazu muss im Unified-E Client (Unified-E App) wie folgt vorgegangen werden:

1. «+» Symbol wählen bzw. «Neue App hinzufügen» im Menü wählen
2. Unter «Gateway-Kommunikation» die Schaltfläche «Scannen» wählen
3. Den im App-Manager-Dialog angezeigten QR-Code scannen
4. Die HMI-App ist registriert und kann durch Anklicken gestartet werden

Ist das QR-Code-Einscannen nicht möglich (z. B. Unified-E Client für Windows), dann sind die Registrierungsdaten im Unified-E Client manuell einzugeben (siehe auch Handbuch des Unified-E Clients).

Registrierung via Gateway-Adresse:

Bei der Basic-Lizenz muss die Registrierung am Bediengerät anstatt mit dem Gateway-Namen mit der IP-Adresse und Port erfolgen, da der Unified-E Onlinedienst als Adress-

Verzeichnis für die Gateway-Namen bei diesem Lizenztyp nicht verfügbar ist. Die IP-Adresse ist im Registrierungs-Dialog unter dem Register «Gateway-Adresse» zu finden.

#### 3.1.2.2 Bediengerät löschen

Normalerweise initiiert man das Löschen eines Bediengeräts, indem man im Unified-E Client die entsprechende App entfernt – das Bediengerät verschwindet anschliessend automatisch aus der Liste der registrierten Bediengeräte.

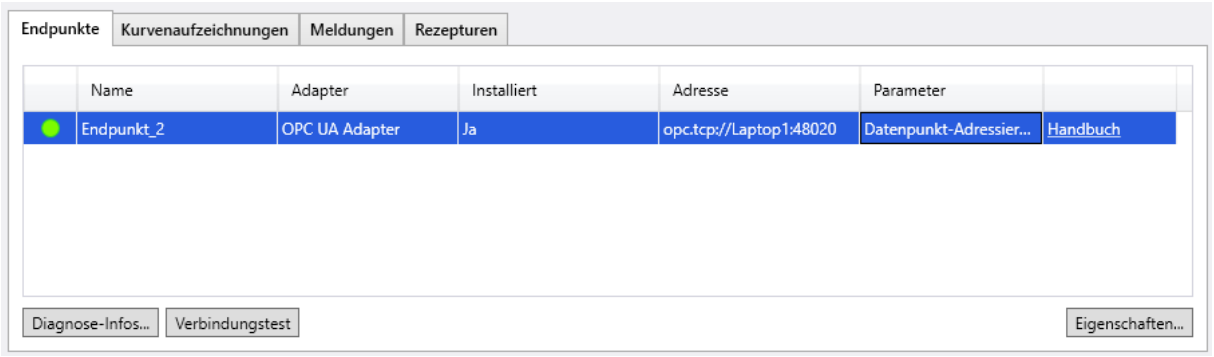
Alternativ kann das Bediengerät in der Bediengeräte-Liste der App im App-Manager über die Schaltfläche «Löschen» entfernt werden.

#### 3.1.2.3 Benutzerrolle ändern

Bei einer HMI-App mit mehreren Benutzerrollen kann die Benutzerrolle über die Schaltfläche «Benutzerrolle ändern…» nachträglich angepasst werden. Eine Neuregistrierung des Bediengeräts ist hierfür nicht erforderlich.

### 3.1.3 Endpunkte konfigurieren

In der Endpunkte-Tabelle sind alle Endpunkte der ausgewählten App gelistet, die im HMI-Projekt im App-Designer konfiguriert wurden.




Spalten:

- Status: Zeigt den Status, z. B. verbunden, Fehler als Farb-Symbols. Details können dem Tooltip entnommen werden
- Name: Eindeutiger Objektname, so wie er konfiguriert wurde
- Adapter: Adapter-Bezeichnung
- Installiert: Falls «Nein», dann sind beim Installieren Fehler aufgetreten. Eine erneute Installation des App-Managers behebt häufig das Problem
- Adresse: Aktuell konfigurierte Adresse des Endpunkts
- Parameter: Zeigt die Parameterliste komma-getrennt

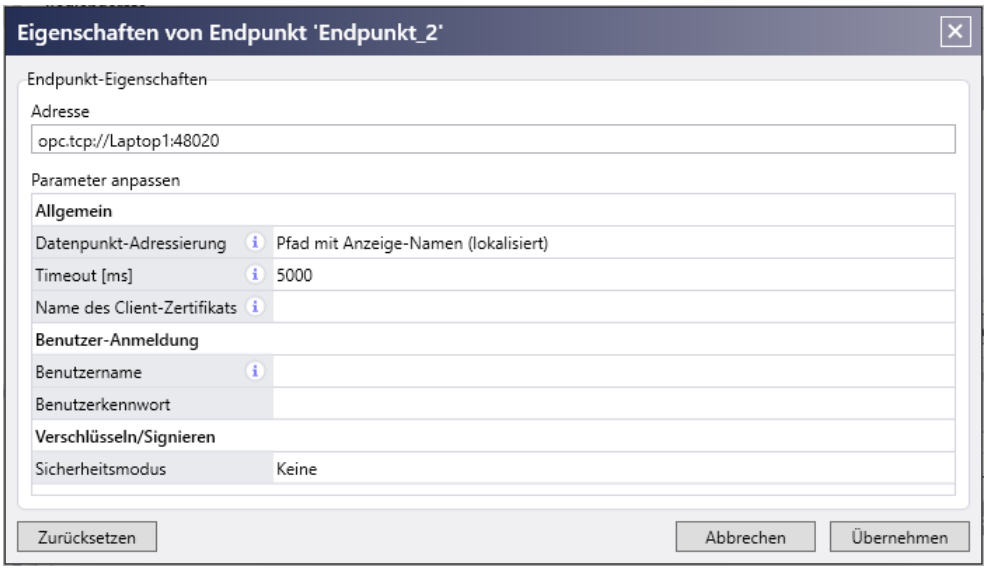
- Handbuch: Hier kann das PDF-Handbuch des Adapters geöffnet werden, welches die Adresse und Parametrierung im Detail beschreibt

Diagnose-Infos anzeigen:

Mit der Schaltfläche «Diagnose-Infos…» öffnet sich ein Dialog, der diverse Statistik-Werte zum Lesen und Schreiben zeigt. Diese Werte können bei der Suche nach z. B. Performance-Problemen helfen.

### 3.1.3.1 Endpunkt-Eigenschaften anpassen

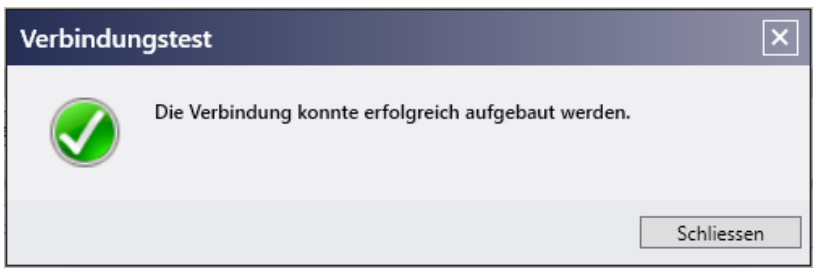
Die im App-Designer Endpunkt-Eigenschaften lassen sich mit der Schaltfläche «Eigenschaften…» im Eigenschaften-Dialog überschreiben.




Die Parameter sind im jeweiligen Adapter-Handbuch beschrieben und je nach Adapter individuell. Mit der «Zurücksetzen» Schaltfläche können alle Eigenschaften auf die ursprünglichen Werte des HMI-Projekts zurückgesetzt werden.

### 3.1.3.2 Verbindungstest

Mit der Schaltfläche «Verbindungstest» lässt sich ein Verbindungstest durchführen, um beispielsweise angepasste Endpunkt-Parameter zu prüfen.



### 3.1.4 Kurvenaufzeichnungen verwalten

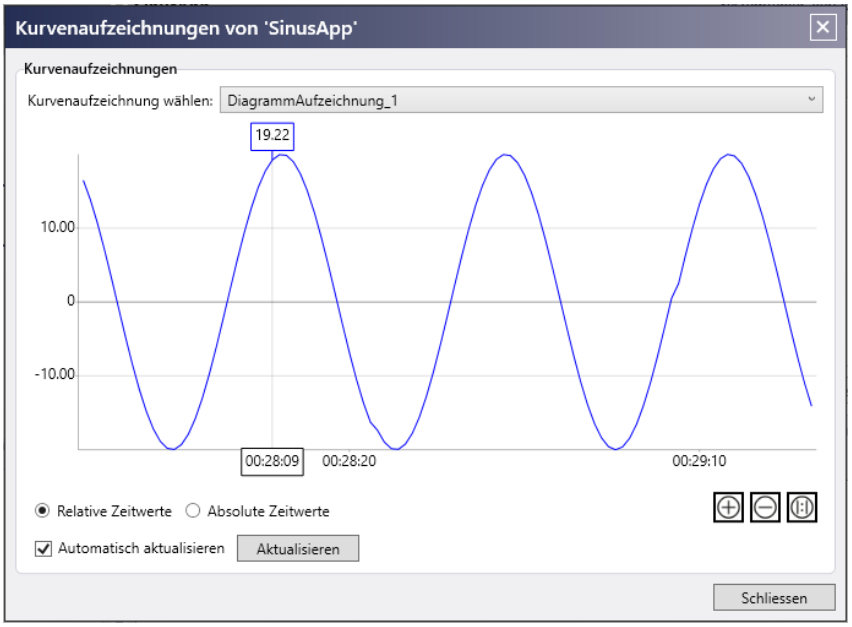
Im Register «Kurvenaufzeichnungen» verwalten Sie Diagramm-Aufzeichnungen sowie die generierten CSV-Aufzeichnungen der ausgewählten App.

Folgende Funktionen stehen zur Verfügung:

- Diagramm-Aufzeichnungen verwalten:
    - Schaltfläche «Diagramm-Aufzeichnungen…»: Öffnet den Dialog zur Anzeige vorhandener Diagramm-Aufzeichnungen (siehe unten)
    - Schaltfläche «Ordner öffnen»: Öffnet den Ordner im Dateisystem, in dem die Diagramm-Aufzeichnungen gespeichert werden. So haben Sie direkten Zugriff auf die Rohdaten
- CSV-Aufzeichnungen verwalten:
    - Schaltfläche «CSV-Ausgabeformat…»: Öffnet einen Dialog zur Konfiguration des Ausgabeformats für CSV-Aufzeichnungen.
        - Option «Lokale Ländereinstellungen verwenden»: Die Windows-Regionseinstellungen für Systemkonten werden verwendet, wenn der Unified-E Windows-Dienst unter 'Lokales System' angemeldet ist
        - Option «Länder-übergreifende Einstellungen verwenden: Verwendet die «Invariant Culture», welche an die US-Kultur geknüpft ist (z. B. «,» für Trennzeichen, «.» für Dezimaltrennzeichen)
    - Schaltfläche «Ordner öffnen»: Öffnet den Zielordner der erzeugten CSV-Dateien im Windows-Explorer
- Diagnose:
    - Schaltfläche «Diagnose-Infos…»: Öffnet ein separates Fenster mit detaillierten Informationen, um detaillierte Fehler zu Aufzeichnungen zu erhalten, z. B. wenn Datenpunkte nicht erreichbar sind

Diagramm-Aufzeichnungen:

Die Diagramm-Aufzeichnungen lassen sich über die Schaltfläche «Diagramm-Aufzeichnungen...» im Dialog auswählen und anzeigen.




### 3.1.5 Meldungen verwalten

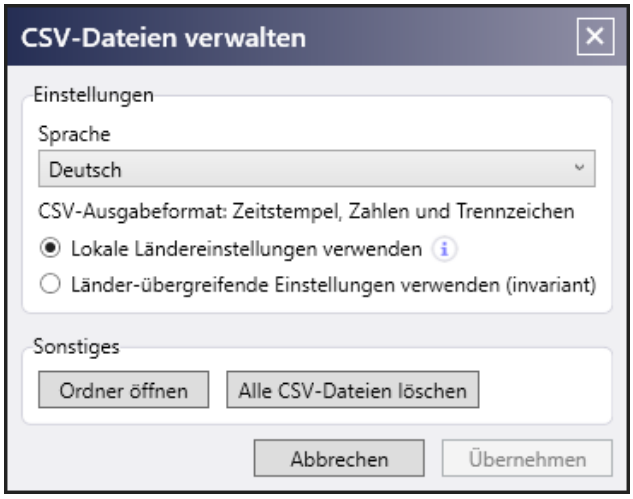
Im Register «Meldungen» wird das zentral gespeicherte Melde-Archiv und die generierten CSV-Melde-Dateien der ausgewählten App verwaltet. Weiterhin können hier die E-Mails mit Rollenzuordnung festgelegt werden, die dann beim Auftreten von Meldungen mit E-Mail-Versand berücksichtigt werden sollen. Zusätzlich stehen Diagnosefunktionen zur Verfügung, um Probleme im Meldesystem zu identifizieren.

Melde-Archiv verwalten:

Über die Schaltfläche «Melde-Archiv…» können im Dialog die SQLite-Dateien des Melde-Archivs eingesehen werden. Zusätzlich besteht die Möglichkeit, das Melde-Archiv vollständig zu löschen (z. B., nachdem ein Backup erstellt wurde).


CSV-Dateien verwalten:

Melde-CSV-Dateien werden im Register «Meldungen» über die Schaltfläche «CSV-Dateien…» verwaltet.



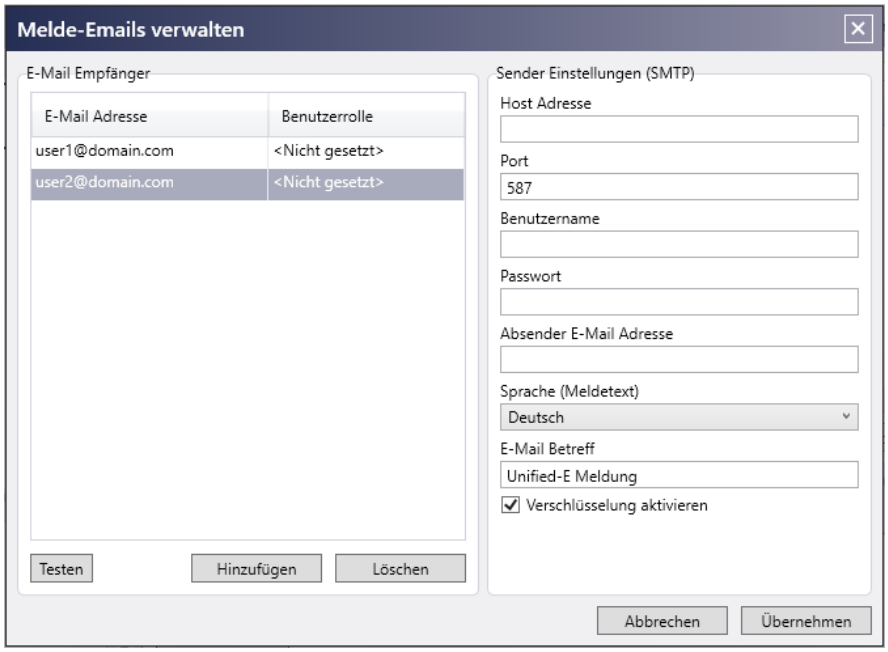

Konfiguration:

- Sprache: Hier wird die App-Sprache ausgewählt, die für die CSV-Protokollierung verwendet werden soll. Auswählbar sind alle im HMI-Projekt definierten App-Sprachen
- CSV-Ausgabeformat: Bestimmt die Formatierung der Werte, siehe Kapitel 3.1.4
- Schaltfläche «Ordner öffnen»: Öffnet das Haupt-Verzeichnis der CSV-Melde-Dateien im Windows-Explorer
- Schaltfläche «Alle CSV-Dateien löschen»: Löscht alle CSV-Melde-Dateien aus dem Haupt-Verzeichnis für die CSV-Protokollierung

E-Mails verwalten:

Im App-Designer können Meldungen mit der Zusatz-Option «Versenden von E-Mails» konfiguriert werden (siehe Handbuch «Unified-E App Designer). Sowohl die SMTP-Verbindungsdaten als auch die gewünschten E-Mail-Empfänger werden ausschliesslich im E-Mails-Dialog im App-Manager wie folgt konfiguriert und einer Benutzerrolle zugewiesen (falls vorhanden).

Der Dialog «Melde-E-Mails verwalten» wird im Register «Meldungen» über die Schaltfläche «E-Mails…» geöffnet.




E-Mail-Empfänger-Bereich: Im linken Bereich wird eine Liste aller definierten E-Mail-Empfänger angezeigt:

- Spalten der «E-Mail-Empfänger»-Liste:
  - E-Mail-Adresse: Zieladresse (Empfänger der Melde-E-Mail)
  - Benutzerrolle: Optional kann eine Benutzerrolle zugewiesen werden
- Schaltflächen:
  - Testen: Sendet eine Testnachricht an die ausgewählte E-Mail-Adresse, um die SMTP-Einstellungen zu überprüfen
  - Hinzufügen: Fügt eine neue Empfängerzeile hinzu
  - Löschen: Entfernt den aktuell ausgewählten Empfänger

Sender-Einstellungen (SMTP) Bereich: Im rechten Bereich definieren Sie die Sender-Einstellungen (SMTP) und die Absenderinformationen für den E-Mail-Versand:

- Host Adresse: Adresse des SMTP-Servers (z. B. smtp.domain.com)
- Port: Portnummer des SMTP-Servers (Standard: 587 für TLS)
- Benutzername / Passwort: Anmeldedaten für den SMTP-Zugang
- Absender E-Mail Adresse: Adresse, die im E-Mail als Absender angezeigt wird
- Sprache (Meldetext): App-Sprache, in der der Text der Meldung versendet wird
- E-Mail-Betreff: Betreffzeile der versendeten Meldung
- Verschlüsselung aktivieren: Aktiviert die Transportverschlüsselung (TLS) für den Versand

Diagnose-Infos anzeigen:

Die Schaltfläche «Diagnose-Infos…» öffnet ein separates Fenster mit detaillierten Informationen zur Analyse von Problemen bei der Meldungsverarbeitung, z. B. wenn der E-Mail-Versand fehlschlägt oder Meldungen nicht aufgezeichnet werden.

### 3.1.6 Rezepturen verwalten

Rezeptur-Datensätze werden in Unified-E als XML-Dateien gespeichert. Pro Datensatz – oder pro Version, abhängig von der Konfiguration im HMI-Projekt – wird eine separate Datei erzeugt und zentral im App-Manager für alle Bediengeräte verwaltet.

Im Register «Rezepturen» erhalten Sie Zugriff auf die im Betrieb erzeugten Rezeptur-Datensätze. Mit der Schaltfläche «Ordner öffnen» lässt sich der Hauptordner im Windows-Explorer öffnen. Die Rezeptur-Dateien können dort manuell hinzugefügt oder gelöscht werden (Import/Export) oder regelmässig gesichert werden.

## 3.2 Systemfehler-Verlauf

Systemfehler sind interne Fehlerzustände des Unified-E Systems, z. B. Verbindungsprobleme zu Endpunkten oder Fehler beim Schreiben von Dateien. Sie werden automatisch erkannt und protokolliert. Systemfehler betreffen den technischen Betrieb des App-Managers selbst.

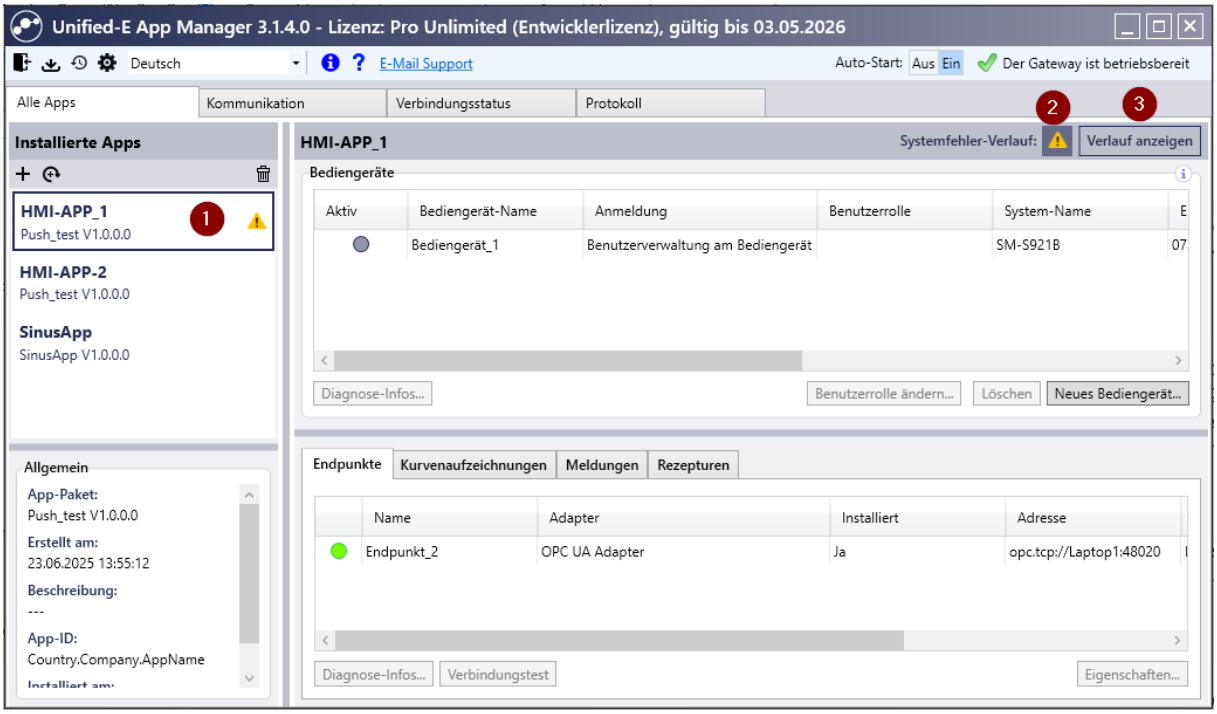
Meldungen hingegen sind benutzerdefinierte Ereignisse, die im HMI-Projekt gezielt für die Visualisierung konfiguriert wurden – etwa Maschinenzustände, Warnungen oder Anlagen-Fehler. Sie dienen der Überwachung der Anlage.

Zusammengefasst:

- Systemfehler = technische Störungen im App-Manager
- Meldungen = projektspezifische Informationen aus der Maschine oder Anlage

Systemfehler-Anzeige:

Anstehende Systemfehler werden mit einem Warnsymbol angezeigt.



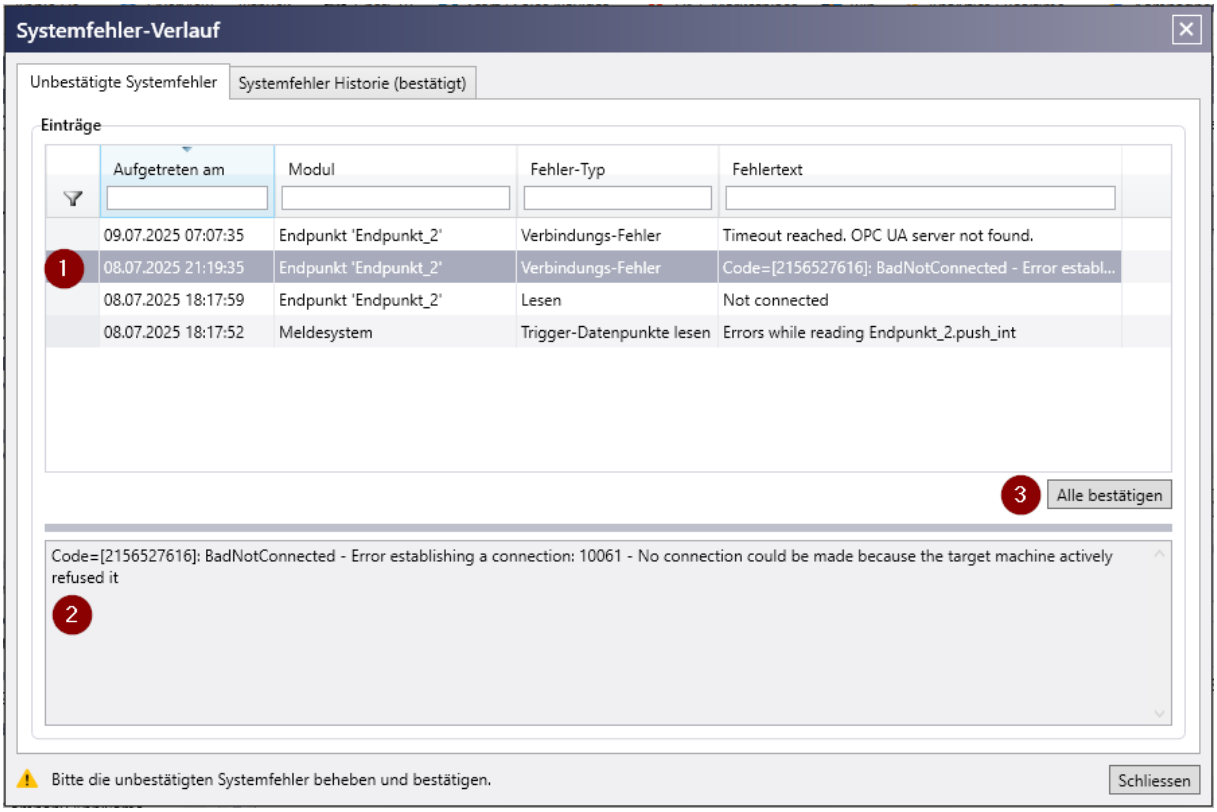

Systemfehler-Elemente (Nummerierung gemäss Abbildung):

1. Warnsymbol (App-Auswahl): Das Warnsymbol wird rechts neben dem App-Namen angezeigt, wenn unbestätigte Systemfehler bei der App vorliegen
2. Warnsymbol (Kopfzeile): Das Warnsymbol wird angezeigt, wenn die ausgewählte App unbestätigte Systemfehler hat
3. Schaltfläche «Verlauf anzeigen»: Öffnet einen Dialog mit den Systemfehlern. Hier lassen sich Systemfehler bestätigen (siehe unten)

Systemfehler bestätigen und Verlauf:

Systemfehler können sowohl in der HMI-App als auch im App-Manager bestätigt (d. h, quittiert bzw. zur Kenntnis genommen) werden. Für das Bestätigen im App-Manager öffnet sie den Dialog über die Schaltfläche «Verlauf anzeigen».

Unbestätigte Systemfehler lassen sich im Dialog wie folgt anzeigen oder auch bestätigen.




Elemente des Systemfehler-Verlauf-Dialogs (Nummerierung gemäss Abbildung):

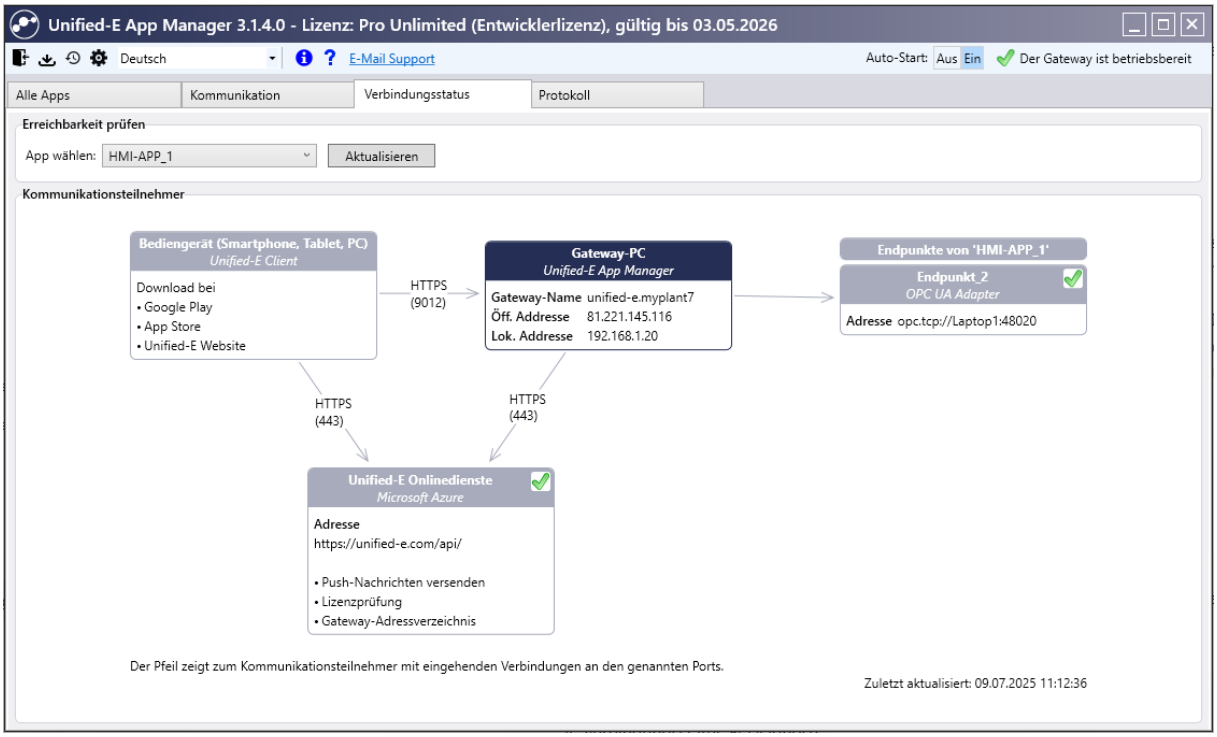
1. Systemfehler-Liste: Enthält alle anstehenden bzw. unbestätigten Systemfehler
2. Details-Bereich: Dort wird der Fehlertext des ausgewählten Systemfehlers mehrzeilig angezeigt wird
3. Schaltfläche «Alle bestätigen»: Alle Systemfehler werden bestätigt, das heisst, aus der Liste gelöscht. Falls ein bestätigter Systemfehler erneut auftritt, dann erfolgt erneut ein Eintrag in die Systemfehler-Liste

# 4 Verbindungsstatus & Diagnose

Im Register «Verbindungsstatus» erhalten Sie wichtige Informationen darüber, wie die Kommunikation zwischen den Verbindungsteilnehmern der ausgewählten App erfolgt und ob diese erreichbar sind.

Die Ansicht zeigt zudem, über welche Ports eingehende bzw. ausgehende Verbindungen abgewickelt werden. Um die Erreichbarkeit zu prüfen, wählen Sie oben die gewünschte App aus. Dabei werden auch die Endpunkt-Verbindungen der gewählten App überprüft.

Beispielkonfiguration:




# 5 Protokoll anzeigen

Wichtige Aktivitäten wie die Bedienung (Sollwert-Änderung) werden im Protokoll detailliert aufgezeichnet.

Es gibt folgende Kategorien:

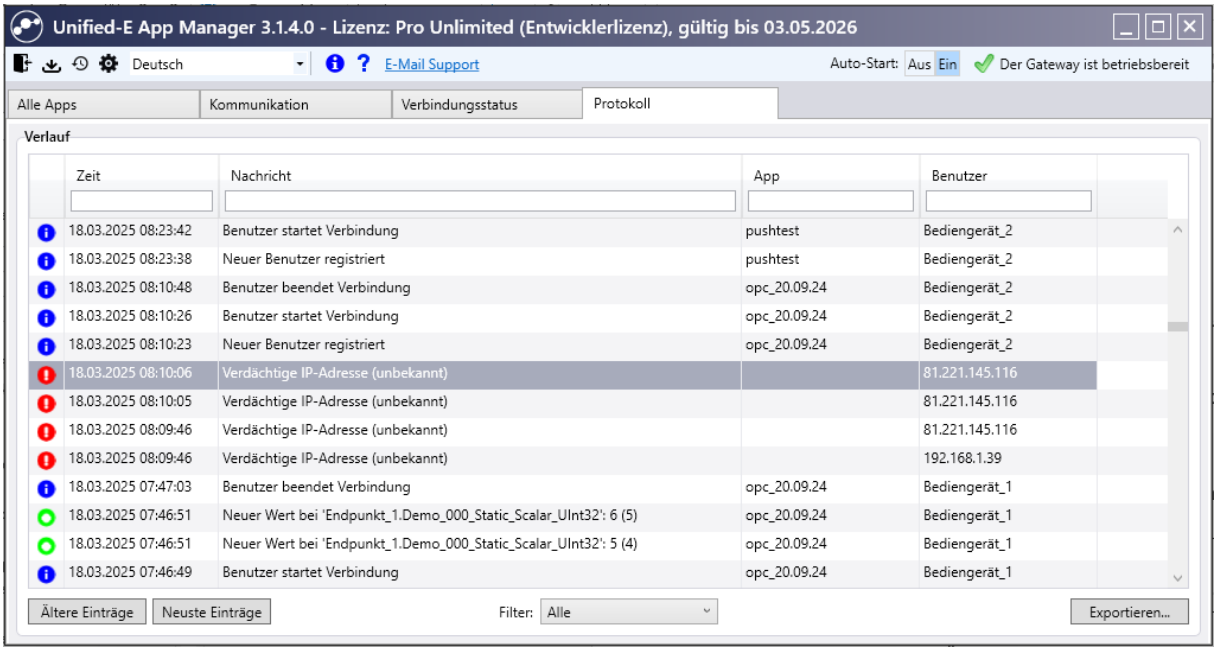
- Information (blaues «i»-Symbol): Allgemeine Informationen, z. B. «Benutzer startet Verbindung»
- Bedienung (grünes Symbol): Ein Benutzer hat einen Wert geändert. Sowohl der alte als auch der neue Wert werden aufgeführt
- Wichtig (rotes «!»-Symbol): Ereignisse, die erhöhte Aufmerksamkeit erfordern, z. B. wenn unberechtigte Anfragen erkannt wurden

Die Protokolleinträge werden in signierten XML-Dateien gespeichert. Damit die Dateien eine handhabbare Grösse behalten, wird pro Monat eine separate Protokolldatei verwendet.

Im Einstellungsdialog lässt sich konfigurieren, ob bzw. wann ältere Protokolleinträge oder Monatsdateien gelöscht werden sollen (siehe Kapitel 6.1).

Protokoll-Liste:

Die Liste zeigt stets nur die Anzahl Einträge an, die in den Protokoll-Einstellungen definiert ist.




Fusszeile der Protokoll-Liste:

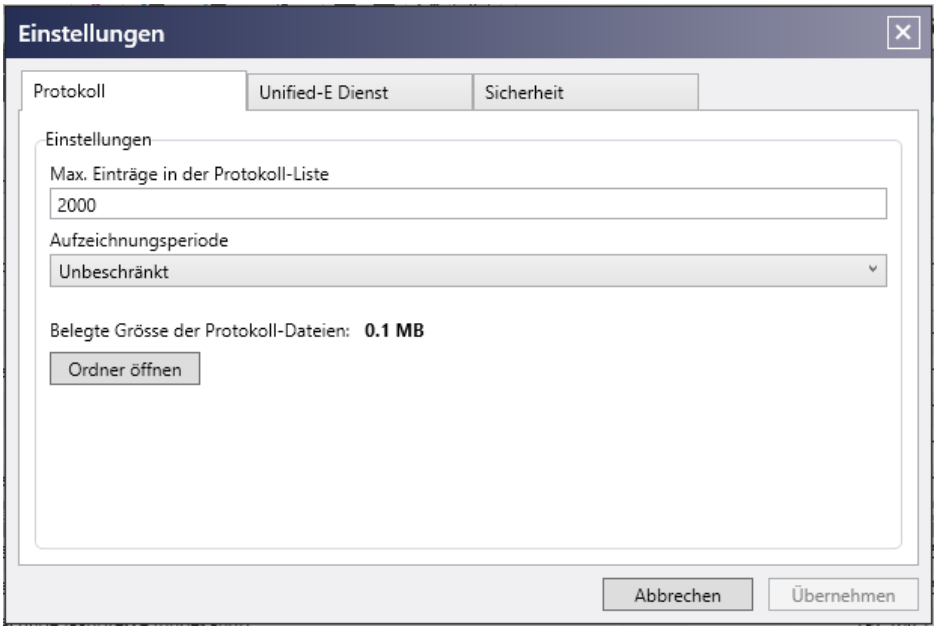
- Schaltfläche «Ältere Einträge»: Lädt ältere Einträge ausgehend von der aktuellen Liste (blättert nach unten)
- Schaltfläche «Neuere Einträge»: Lädt neuere Einträge (blättert nach oben)
- Filter: Ermöglicht das Filtern der Liste nach Kategorie
- Exportieren: Exportiert die Liste in die Zwischenablage (z. B. für Excel) oder als CSV-Datei

# 6 Einstellungen-Dialog

Im Einstellungen-Dialog lassen sich allgemeine Einstellungen konfigurieren. Der Dialog lässt sich über die Toolbar (Zahnrad-Symbol) öffnen. Die verschiedenen Einstellungen sind in Register gruppiert und sind in den folgenden Unterkapiteln beschrieben.

## 6.1 Protokoll-Einstellungen

Im Register «Protokoll» des Einstellungs-Dialogs können Sie konfigurieren, wie viele Einträge in der Protokoll-Liste angezeigt werden und wie lange Protokolldateien gespeichert bleiben.



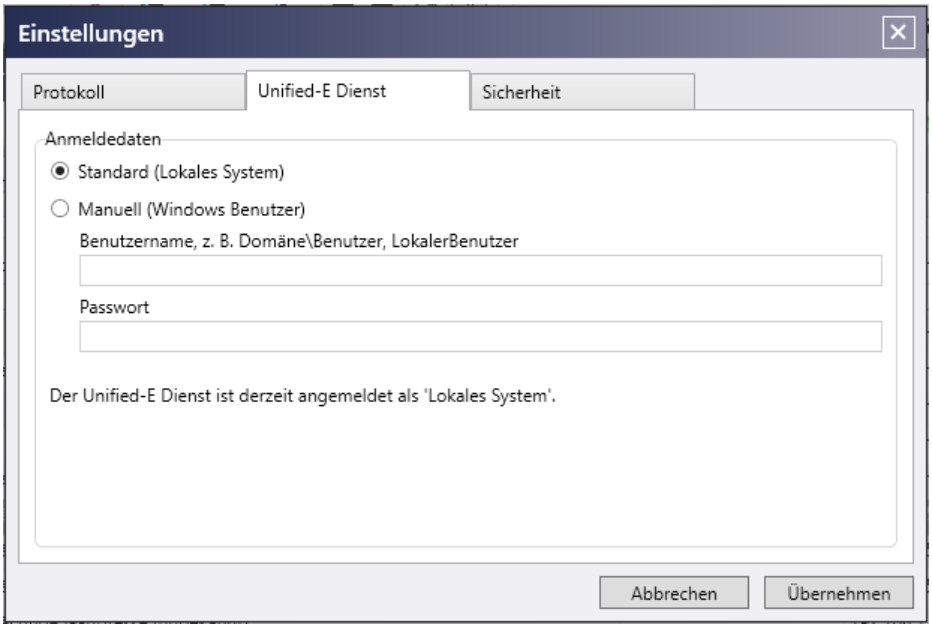

Protokoll-Einstellungen konfigurieren:

- Max. Einträge in der Protokoll-Liste: Legt fest, wie viele Einträge maximal in der Protokoll-Liste (Register «Protokoll») gleichzeitig angezeigt werden. Ältere Einträge werden bei Bedarf automatisch ausgeblendet, jedoch nicht gelöscht.
- Aufzeichnungsperiode: Bestimmt, wie lange Protokolldateien aufbewahrt werden:
    - Unbeschränkt: Keine automatische Löschung
    - 6 Monate / 12 Monate / 24 Monate: Ältere Monatsdateien werden nach Ablauf der gewählten Frist automatisch gelöscht
- Belegte Grösse der Protokoll-Dateien: Zeigt an, wie viel Speicherplatz die bisher erzeugten Protokolldateien belegen
- Schaltfläche «Ordner öffnen»: Öffnet den Speicherort der signierten XML-Protokolldateien im Windows-Explorer

## 6.2 Unified-E Dienst Einstellungen

In diesem Register legen Sie fest, mit welchen Windows-Anmeldedaten der Unified-E Dienst, welche die HMI-App Anfragen behandelt und Melde-Ereignisse überwacht, auf dem System ausgeführt wird.

Setzen Sie die Anmelde-Daten auf «Manuell», wenn der Standard-Benutzer «Lokales System» nicht über genügend Berechtigungen verfügt, um beispielsweise auf Dateien (z. B. Datenbank-Dateien) zuzugreifen.

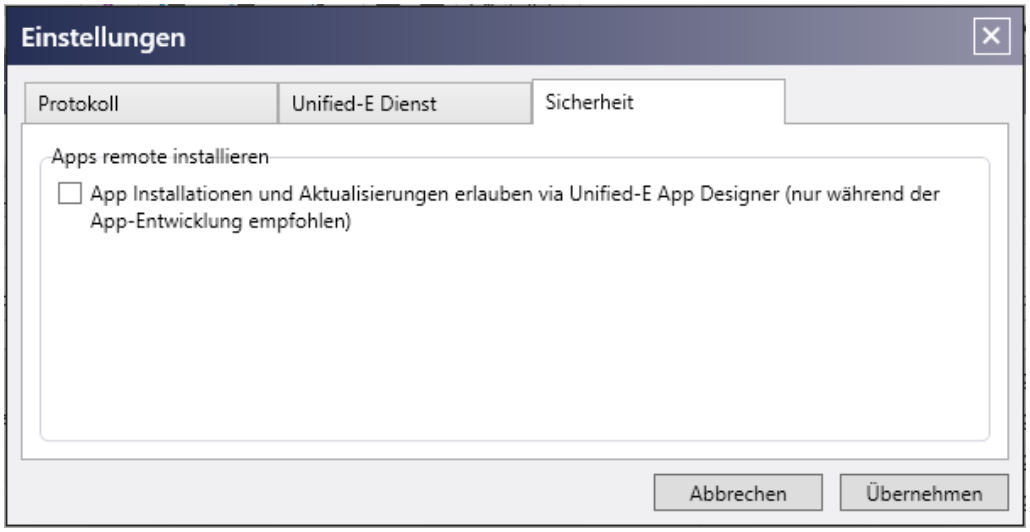



Anmeldedaten setzen:

- Standard (Lokales System): Der Unified-E Dienst wird unter dem integrierten Windows-Konto «Lokales System» ausgeführt. Diese Einstellung ist standardmässig aktiv und für die meisten Installationen ausreichend.
- Manuell (Windows Benutzer): Alternativ kann ein benutzerdefiniertes Windows-Konto verwendet werden. Dies kann z. B. erforderlich sein, wenn der Dienst auf Netzwerkressourcen zugreifen muss, für die der Benutzer «Lokale System» keine Berechtigung besitzt. Geben Sie dazu folgende Informationen ein:
    - Benutzername (im Format Domäne\Benutzer oder LokalerBenutzer)
    - Passwort des angegebenen Benutzers

## 6.3 Sicherheits-Einstellungen

In diesem Register legen Sie fest, ob App-Installationen und -Aktualisierungen remote über den Unified-E App Designer beim «Veröffentlichen»-Vorgang erlaubt sind. Diese Option ist ausschliesslich für Entwicklungs- oder Testzwecke vorgesehen und sollte aus Sicherheitsgründen im Produktionsbetrieb deaktiviert bleiben.




# 7 Anhang

## 7.1 Support und weitere Informationen

Für weiterführende Informationen zur Nutzung des Unified-E App Managers steht Ihnen unsere Website unter www.unified-e.com zur Verfügung. Insbesondere der Bereich «Erste Schritte» bietet einen kompakten Einstieg mit anschaulichen Beispielen und häufig gestellten Fragen.

Falls Sie technische Unterstützung benötigen oder spezifische Fragen zu Ihrer Konfiguration haben, können Sie sich jederzeit an unser Support-Team wenden. Senden Sie dazu bitte eine E-Mail an:

support@unified-e.com

Wir bemühen uns, Ihre Anfrage so rasch wie möglich zu bearbeiten. Bitte fügen Sie Ihrer E-Mail – sofern vorhanden – relevante Screenshots oder eine kurze Beschreibung Ihrer Projektstruktur bei, um eine effiziente Bearbeitung zu ermöglichen.