Unified-E App Manager
User Manual

HMI Server for Remote Communication and Central Data Storage

Software version 3.1.0.0, last updated: July 2025

Publisher: Unified-E AG, Winterthur, Switzerland

Content

1 Introduction

The Unified-E App Manager (App-Manager for short) turns a Windows computer into an HMI server and takes over the central management and execution of HMI apps in the Unified-E system. It can be used as an option – operator devices such as panel PCs or smartphones can communicate directly with a controller even without an App-Manager.

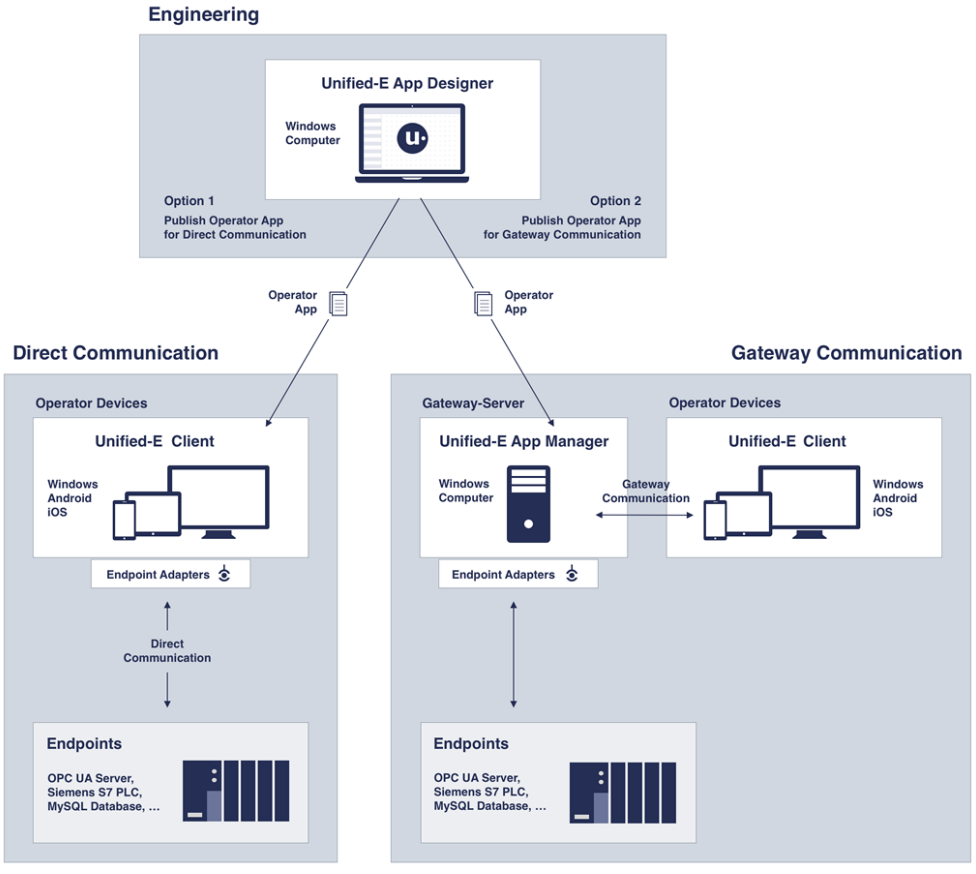
The use of the App-Manager is recommended if a plant has several operating terminals, if operation is to be carried out via the Internet or if visualizations and data are to be managed centrally on a server. In such cases, the App-Manager acts as a gateway server: it receives requests from the operator devices and forwards them to the target systems such as PLC controllers.

This user manual introduces the use and configuration of the Unified-E App Manager – with a focus on typical application scenarios in industrial automation.

1.1 Software Overview

1.1.1 Software Components

Unified-E consists of several programs or software components, the most important components are illustrated in the following figure. All programs can be downloaded from the Unified-E website – for development purposes, all programs are available free of charge.



Unified-E App Designer:

The Unified-E App Designer (App-Designer for short) is an HMI editor that is used to configure the operator app or HMI app. The configuration is stored in a project file. For use at runtime, the App-Designer uses the “Publish” function to create an app package file that contains the visualization in an optimized form.

The App-Designer user manual can be downloaded from the Unified-E website.

Unified-E Client:

The Unified-E Client is installed as an HMI client on the respective operator device. It is used to execute the HMI app created in the App-Designer and thus enables the operation and monitoring of machines and plants.

The visualization is registered in the Unified-E Client via an app package file and then used at runtime.

For Android and iOS devices, the Unified-E Client (under the name “Unified-E App”) is available in the Google Play Store and the Apple App Store, respectively. The Windows version of the client can be downloaded from the Unified-E website.

The user manual for the Unified-E client can be downloaded from the Unified-E website.

Unified-E App Manager:

The optional Unified-E App Manager acts as an HMI server with central data storage. The server function is used when, for example, a smartphone is to communicate with the plant via the Internet or several operator devices access a plant at the same time. Since the HMI server acts as a gateway from the client's point of view, this is also referred to as gateway communication.

In the following subchapters, the Unified-E App Manager is described in detail.

1.1.2 Direct and Gateway Communication

Direct communication (without Unified-E App Manager):

Direct communication means that every operator device (e.g. a panel PC or smartphone) communicates directly with the PLC. This variant is particularly suitable for simple plants with a few operator devices, as no additional server is required and the operator device communicates with native communication protocols (without a web server). In contrast to gateway communication, direct communication requires a direct license per operator device, which must be registered via the Unified-E Client.

Gateway communication:

Communication via the Unified-E App Manager is referred to as gateway communication. All operator devices communicate exclusively with the Unified-E App Manager as a gateway, not directly with the PLC. The following documentation is exclusively about gateway communication with the Unified-E App Manager.

1.2 Important Terms

1.2.1 App

In Unified-E, the term “app” refers to an operator app or HMI app. Such apps can be registered in the Unified-E App Manager and enable gateway communication between the operator and the endpoints. An app is saved as an app package file in the App-Designer (“Publish” workflow) and installed on the App-Manager.

1.2.2 Operator Device / HMI Device

From a Unified-E point of view, an operator device (or HMI device, control panel) is a computer with a Windows, Android or iOS operating system on which the visualization is displayed with the Unified-E Client program. Typical examples are industrial panel PCs with Windows, Android panels, tablets, iPads, iPhones or smartphones.

To run an HMI app on an operator device, the “Unified-E Client” application must be installed (see chapter 1.1.1).

1.2.3 Endpoint

In Unified-E, an endpoint typically refers to a PLC controller or other data source such as an SQL server or web server. It was created and preconfigured in the App-Designer. For more information on the definition and supported adapters, see the Unified-E App Designer user manual.

During operation, the App-Manager communicates with these endpoints when using the gateway and forwards the data between HMIs and endpoints.

1.2.4 Gateway PC

A gateway PC in the Unified-E context is a Windows computer on which the Unified-E App Manager runs as a Windows service. It acts as an HMI server for the connected operator devices and takes care of central data storage and communication with the endpoints. From the point of view of the operator devices, the gateway PC represents a gateway to the endpoints – such as PLC controllers or data servers. The operator devices do not communicate directly with the endpoints, but exclusively via this central gateway PC.

1.2.5 Gateway License

A gateway license is required for commercial use of the Unified-E App Manager. It determines how many operator devices may be registered at the same time and which communication types are supported (see chapter 2.2). A gateway license can be purchased online via the Unified-E website:

- Basic license
    - One-time activation with internet connection

    - Afterwards usable offline
    - For multiple HMI devices on the same network
    - No annual costs (fixed price license)
    - App-Designer and updates included
- Standard license
    - Annual subscription with online license check
    - For mobile operation via the Internet
    - App-Designer, push services and updates included
- Pro license
    - Same as Standard license, in addition:
    - Firewall-friendly Internet communication without router configuration
    - Includes relay service via Microsoft Azure

For developers, a free gateway license is available in the Unified-E Portal, which covers all the functions of the Standard license.

Operator devices that communicate via the Unified-E App Manager do not require any additional licensing of the Unified-E Client on the operator device.

1.3 Introduction of HMI Server Functions

The following subchapters describe the most important functions of the HMI server software.

1.3.1 Encrypted Communication with Operator Devices

Regardless of the communication type selected, the connection between operator devices and the App-Manager is always encrypted via the HTTPS protocol. The SSL certificates are created automatically – with configurable key length – and ensure secure data transmission.

If you use a Standard or Pro license, the SSL certificates are renewed regularly and automatically. The operator devices receive the updated certificate information without interruption via the Unified-E online service.

1.3.2 Streamlined Endpoint Communication

If several HMIs or operator terminals are connected to an HMI app at the same time, communication with the endpoints via the App-Manager is optimized:

- All operator devices share a central endpoint connection via the App-Manager
- Read requests are bundled to minimize the number of accesses to the endpoints

1.3.3 Unified-E App Manager as a Windows Service

The Unified-E App Manager runs as a Windows service and is therefore active even when no user is logged on to the system. A Windows server operating system is not required. System functions such as monitoring messages remain active – even when connected operator devices are switched off, as message and alarm monitoring is carried out centrally in the App-Manager.

1.3.4 Central Data Storage

All operator devices registered with an HMI app access centrally managed data – there is no local data storage on the operator devices. In particular, the following are stored centrally:

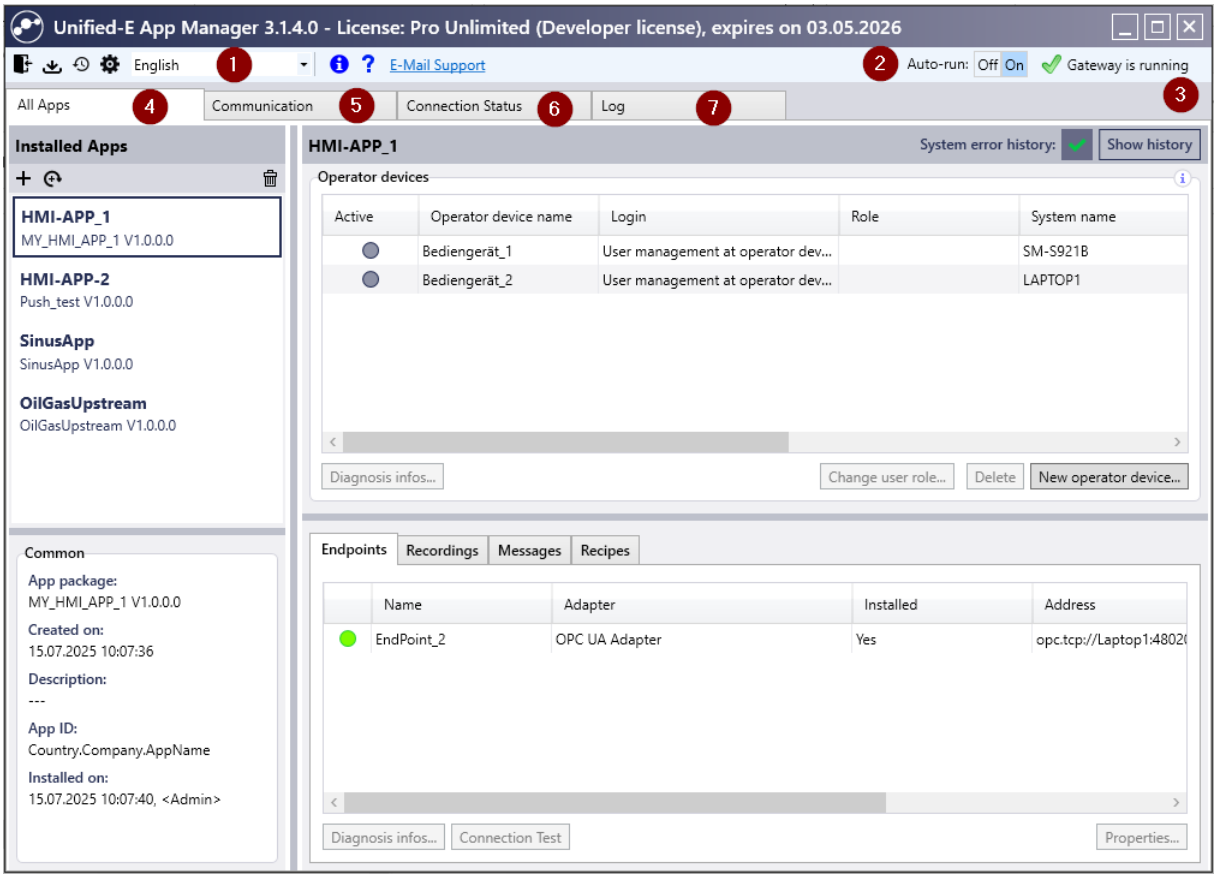
- Message Archive (Alarms)
- Recipe datasets
- Curve Recordings

1.3.5 Host Multiple HMI Apps

In the App-Manager, multiple apps can be registered and run at the same time. This allows different plants or machines to be operated in parallel with just one App-Manager. Managing apps is described in detail in chapters 3 described.

1.4 The User Interface at a Glance

The most important areas of the user interface are illustrated in the following figure:



Toolbar functions (numbering according to figure):

The following toolbar functions are available via buttons.

1. Toolbar buttons:

   a) Unified-E Windows Service Shutdown:
   Not only closes the user interface, but also terminates the Windows service. The installed apps are then no longer accessible to operator devices

   b) Download and install update:
   Download and install the latest update (if available). The Windows service will stop here

   c) View version history:
   Displays version history and related notes about previous versions

   d) Settings:
   Displays the Settings dialog (see chapter 6)

   e) Language:
   Specifies the language of the user interface (German, English)

   f) Info:
   Displays an info dialog with program information

   g) Help:
   Opens help in PDF reader

2. Auto-run (Windows service):
   Specifies whether the Windows service should start automatically when Windows starts
3. Operating status display:
   Shows the general operating status regarding licensing and gateway communication. The connection state of endpoints is not taken into account here

Available register tabs (numbering according to figure):

4. All Apps:
   This is where all HMI apps (or operator apps) and the registered operator devices are managed (see chapter 3)
5. Communication:
   Here, the Gateway license is managed and the communication type between the operator devices and the App-Manager is set up (see chapter 2)
6. Connection Status:
   General connection problems to the endpoints can be quickly diagnosed here
7. Log:
   Important events are logged here

2 Set Up Communication with Operator Devices

The Gateway license is managed in the “Communication” tab. Depending on the Gateway license, different communication types are supported.

2.1 Gateway License Login

2.1.1 View Current License Information

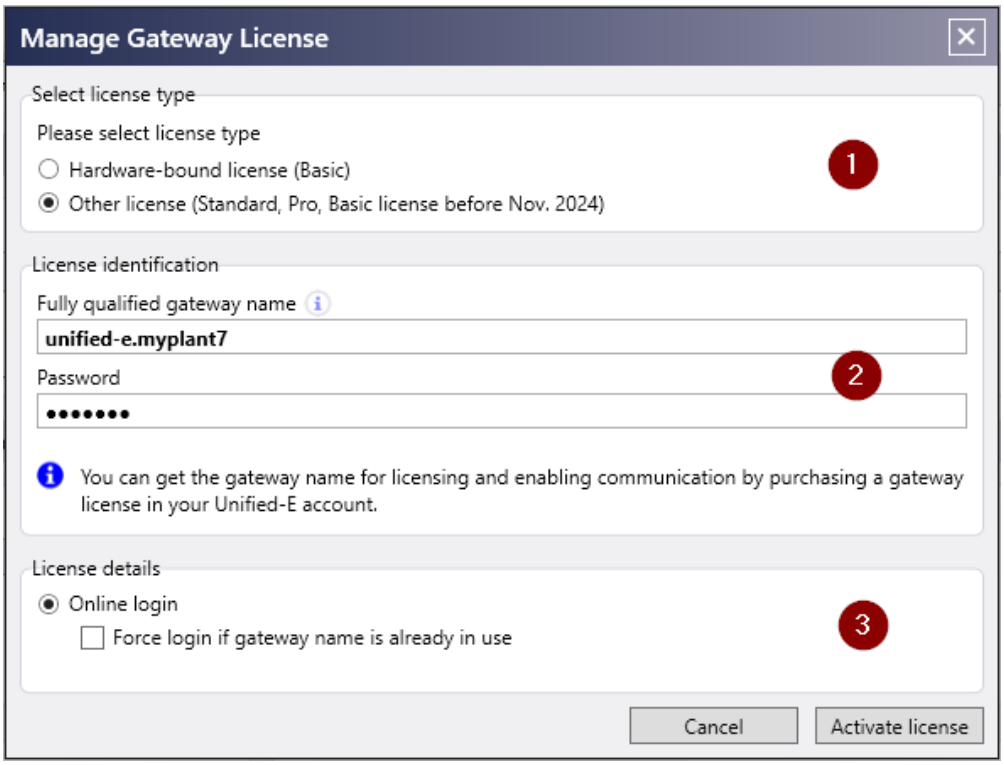
In the “Gateway License” group, the fully qualified gateway or license name of the activated license can be seen. The license name is unique and therefore also contains the Unified-E account name as a prefix.

The following links can be found in this group:

- License details: Displays detailed information about the license in a dialog, e.g. the permitted number of operator devices
- My account: Opens the “Login” page to log in to the Unified-E account
- Free License: Opens a dialog. In addition to the developer license (see chapter 1.2.5), a 30-day Pro license can be purchased here free of charge. The Pro license enables uncomplicated communication via the Internet without router/firewall configuration

2.1.2 Activate License

When starting the App-Manager for the first time, the gateway license must be activated once to unlock all functions. To do this, go to the “Gateway license” group in the “Communication” tab and click on the “Manage gateway license...” button. In the dialog that appears, enter the license data and perform the activation.

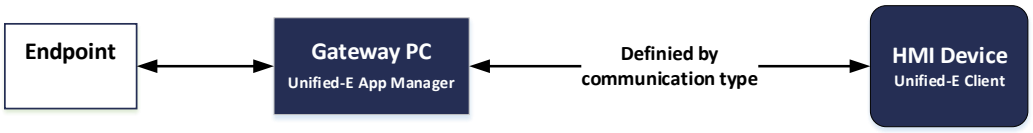


Areas (numbering as shown in the figure):

1. Select license type:The license type is to be selected here. Hardware-bound licenses are hardware-bound and can only be transferred to a limited number to another gateway PC.
2. License identification:
   License identification requires the license name that was assigned online when purchasing (or registering) the commercial or developer license.
   a) Fully qualified gateway name: The fully qualified gateway name has the following structure: <Unified E Account Name>.<License Name>
   Example: mycompany.mygateway1
   b) Password: The password that was set for the license.
3. License details (subscription license):
   Select the “Force login if gateway name is already in use” checkbox if the entered license has already been assigned to another gateway PC. Subscription licenses are transferable, but only one gateway PC can be linked to a subscription license at a time.

2.2 Define Communication Type with HMI Devices

When using the App-Manager, communication between the HMI device (e.g. smartphone, HMI panel PC) and the endpoints always runs through the App-Manager, which acts as a gateway.



The App-Manager provides several communication types that determine the communication between the gateway PC and the HMI device, which are presented in the following subchapters.

Configure the communication type:

The communication type must be defined in the “Communication” tab in the “Communication basic settings” group.

Depending on the license type, not all communication types can be adjusted. The different types of communication are described in more detail in the following chapters.

2.2.1 Communication Type “Internet (firewall-friendly)”

This communication type allows access to endpoints from the Internet without having to handle incoming connection requests over the Internet, and no ports need to be opened. This communication type can be activated immediately without any network configuration and is only available with the Pro Gateway license.

Since communication is always handled via a relay messaging service (additional server on the Internet) (i.e. indirect), the speed is somewhat slower than that of the “Internet (Direct)” communication type.

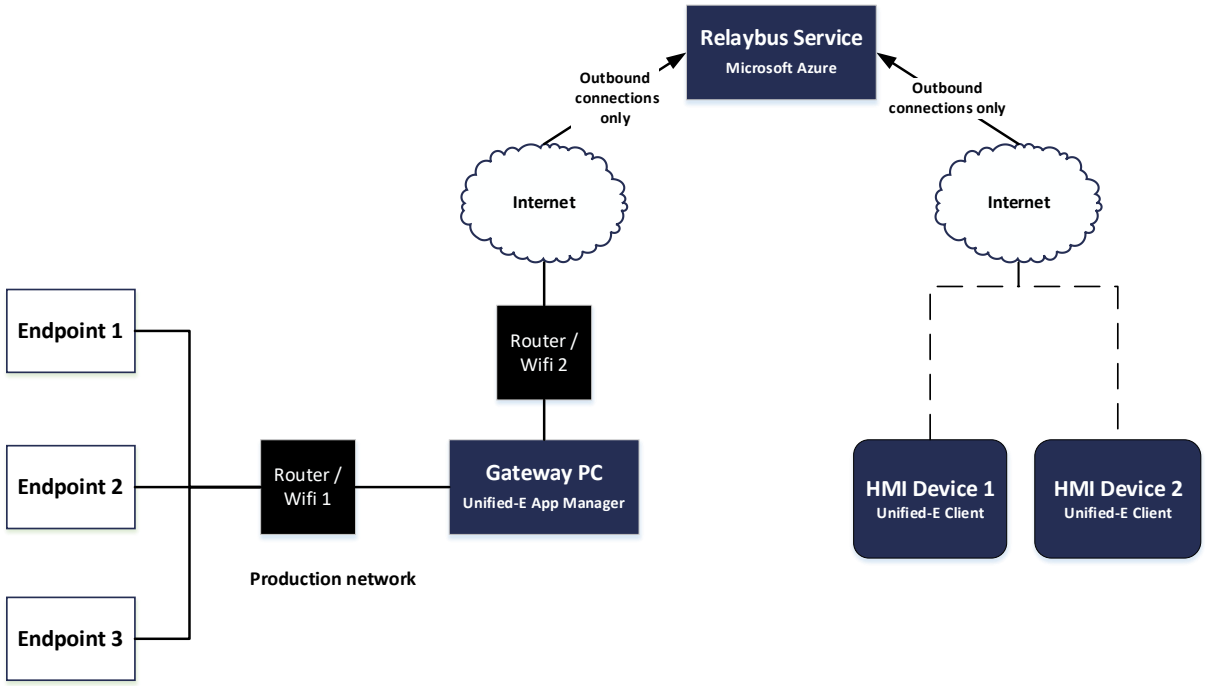
Security:

Since no incoming Internet connections are necessary and no ports need to be opened, this communication type is considered very secure. The relay messaging service also regularly updates the SSL certificate and uses high encryption.

Additional configurations in the network:

No additional configurations such as port forwarding are required. The public IP address of the router is also irrelevant.

Topology example:



Use case:

The plant is to be monitored remotely via the Internet on a smartphone, without having to carry out port or firewall configurations.

Required license type:

This communication type requires the Pro Gateway license.

2.2.2 Communication Type “Internet (Direct)”

The smartphone communicates directly with the App-Manager (gateway PC), which is connected to the Internet as well as to the local (production) network. This communication type requires setting up port forwarding on the router or firewall.

Security:

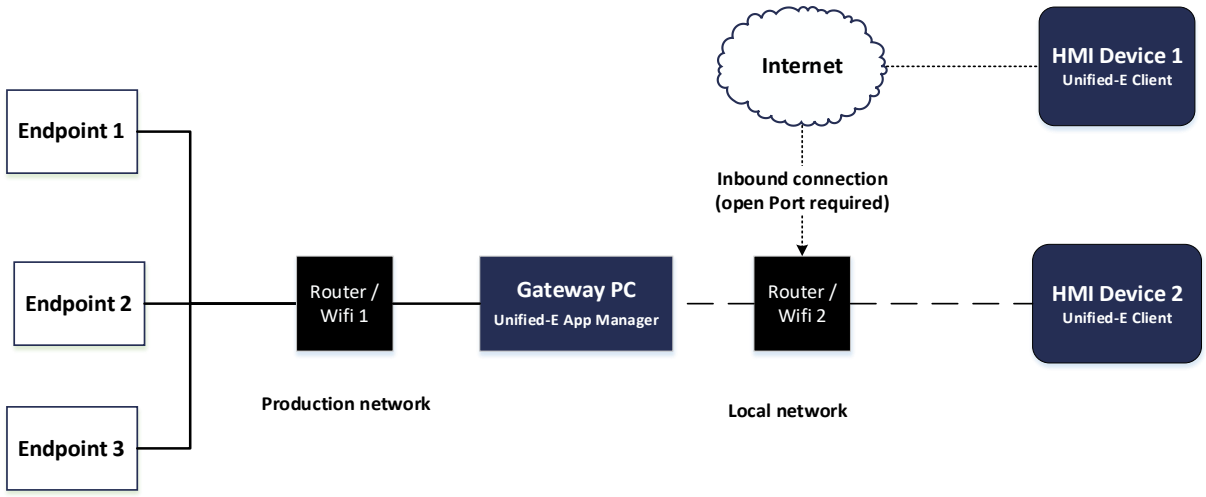
Incoming connection requests from the Internet must be handled, so port forwarding must be set up with the router.

Open ports without further measures are generally considered a potential risk. This mode of operation should therefore only be set up by IT administrators with network knowledge.

Possible measures to increase security:

- Run App-Managers in a DMZ (demilitarized zone)
- Use of additional firewalls

Topology example:



Use case:

The plant is to be monitored stationary on an operating station and additionally mobile via the Internet on a smartphone. A VPN is not required, the plant is in a simple network with a UPnP router. Alarms are to be sent to the smartphone in the form of push notifications.

Required license type:

For this communication type, the Standard Gateway license is required.

The “Internet (Direct)” communication type is divided into two sub-modes – “Manual” and “Automatic (UPnP)”. These are described in the following chapters and differ in whether there is a static or dynamic public IP address and whether the router allows UPnP access.

2.2.2.1 Setting up port forwarding “Manual”

For this communication type, the host name (external IP address, DNS address, DynDNS address) must be entered manually in the “Gateway address” group.

Additional configurations in the network:

- Port forwarding
  - Set up the WAN router
  - Set up firewalls/internal routers involved
- External (public) IP address
  - Option 1: Use a static IP address
  - Option 2: Use dynamic IP address
    - Option 1: Use DynDns address (e.g. no-ip.org)

- Option 2: Set the update URL, as described below, on the router

Dynamic external IP address & update URL:

If the WAN router supports individual update URLs, then no DynDNS address or static fixed address is required. With the following update URL, the IP address for the gateway name is automatically updated by the Unified-E online service, so that smartphones can communicate with the App-Manager even after an IP address change.

Structure of the update URL for Unified-E:

https://unified-e.com/api/Gateways/UpdatePublicIp?account=<account-name>&gateway=<gateway-name>&password=<password>

Enter the update URL with the DynDNS router:

Enter your account and gateway name in the respective placeholders of the URL. This URL must then be entered with the WAN router and will be called whenever the external IP address has changed.

Delete gateway address in App-Manager:

When using the update URL, the DNS or IP address entry in the Gateway Address group must be deleted.

2.2.2.2 Set up port forwarding automatically “Automatic (UPnP)”

The following requirements must be met for this communication type:

- The gateway PC must have direct access to the WAN router, which has a public (dynamic) IP address
- The WAN router must have UPnP enabled for writing

When using this mode, no further manual network configurations are required, as port forwarding on the router is done automatically via UPnP from the App-Manager.

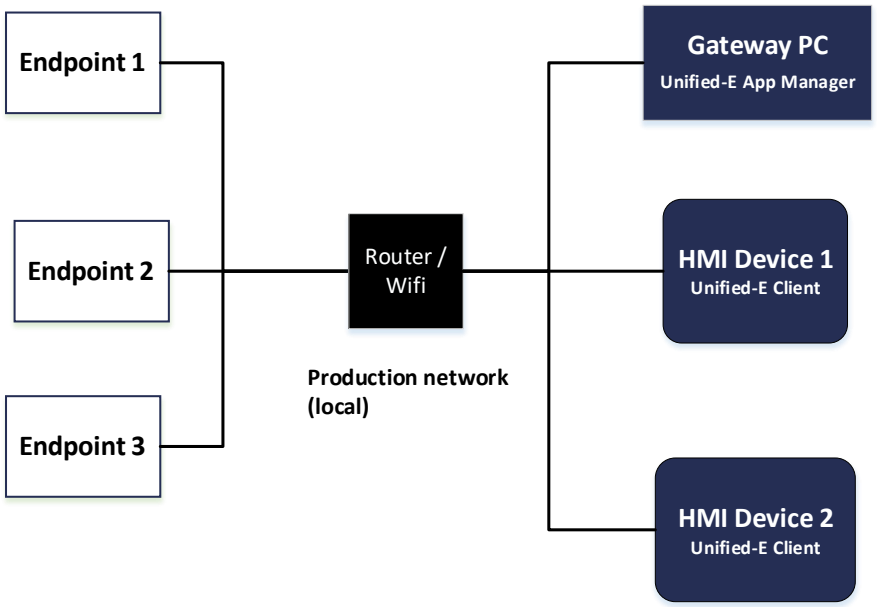
For more information about other communication settings in the App-Manager, see chapter 2.2.5.

2.2.3 Communication Type “Offline (no Internet)”

This communication type can only be used in combination with a Basic Gateway license (hardware-bound fixed-price license). The App-Manager does not require an Internet connection – except for license activation. Online services from Unified-E are not supported here – for example, push notifications cannot be sent to a smartphone via the Internet.

This communication type is suitable if all HMI operator devices are on the same network as the App-Manager. This could also be made possible via the Internet in the VPN.

Topology example:



Use case:

All operator devices are in the production network without internet. Unified-E online services such as push notifications via the Internet are not necessary.

Required license type:

The Basic Gateway license is required for this communication type.

2.2.4 Communication Type “Local network”

In this communication, the linked HMI devices and the gateway PC with the App-Manager must be on the same subnet. The App-Manager is connected via the Internet, port forwarding at the router is not configured manually or automatically.

In contrast to the “offline” communication type, the App-Manager must be connected to the Internet on a regular basis. Depending on the app configuration, push messages are sent to the smartphone via the Unified-E online service when messages arrive.

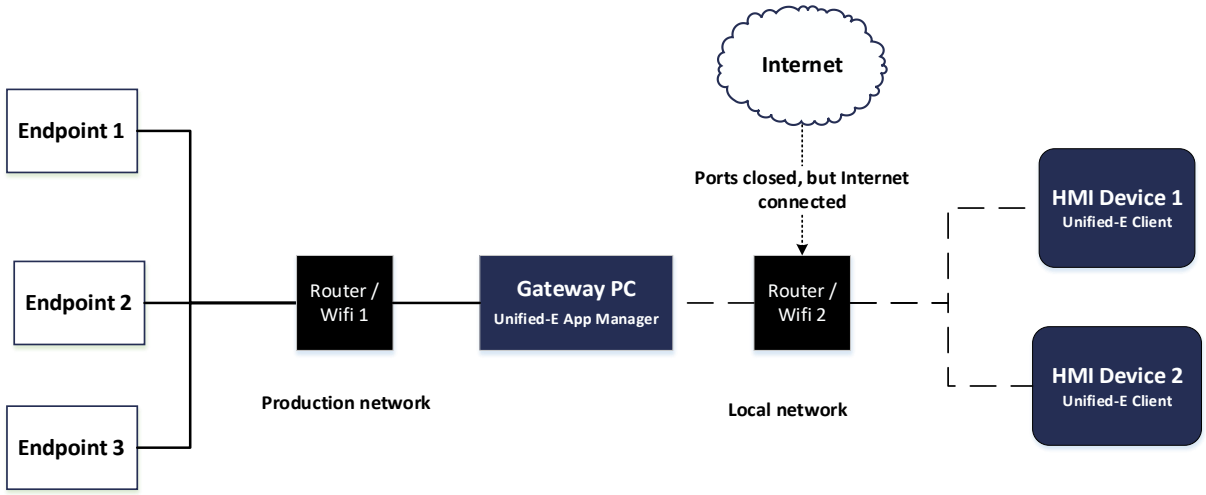
Security:

Since this communication type does not use any incoming connections via the Internet, the App-Manager can be operated in the network with a single- or multi-level firewall concept in the intranet zone without security concerns.

Additional Network Configurations:

There are no settings to be made on the WAN router, as there is no need to handle incoming requests over the Internet. There is also no need to configure external firewalls.

Topology example:



Use case:

All operator devices are in the production network and also on the Internet – no need to set up port forwarding. Unified-E online services such as push notifications via the Internet are possible.

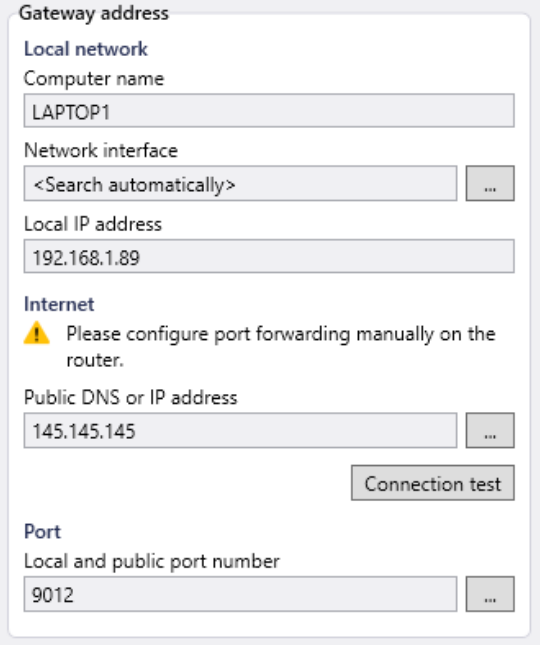
Required license type:

For this communication type, the Standard license is required.

2.2.5 HTTPS Server Settings for Incoming Connections

2.2.5.1 Configure the Gateway Address

For all types of communication - except “Internet (firewall-friendly)” - the gateway address must be configured in the “Gateway address” group.



Select Network Interface:

The selected network interface determines which IP addresses for the gateway (gateway name) are published.

Change your public DNS or IP address:

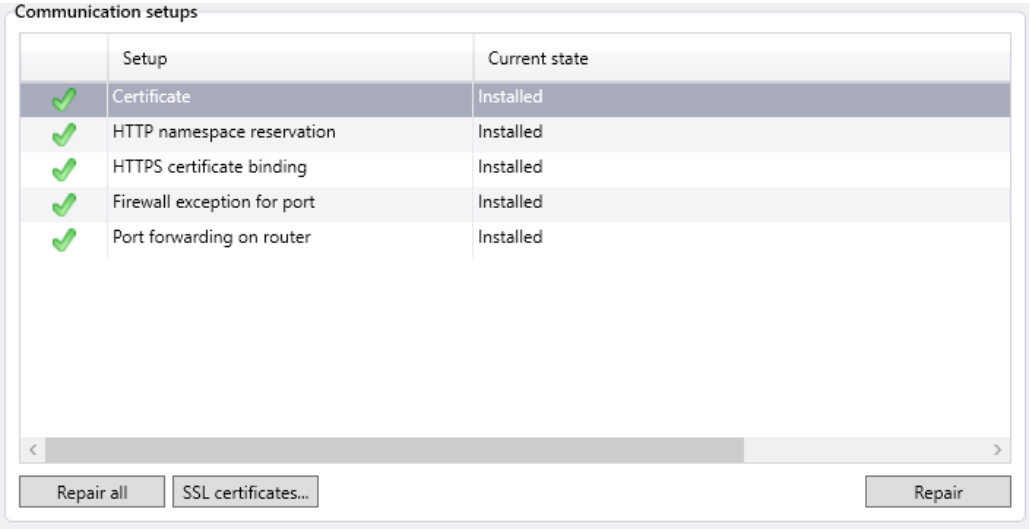
This field can only be set for “Internet (Direct)>Manual”. This sets the external IP address of the gateway manually (see also chapter 2.2.2.12.2.2.1).

Change port:

The port number that the HTTPS server listens to in the Windows service for incoming connections must be set there. The port number is used for communication on the LAN as well as over the Internet (symmetric).

2.2.5.2 Advanced communication setups

The advanced communication setups are set up automatically. The list in the “Communication setups” group is used to check whether the automatic setup was successful.



Possible status lines for the communication setups:

- Certificate: Verifies that the SSL certificate has been successfully created.
  - The smartphones check the validity of the certificate using the fingerprint, among other things
  - In the case of “offline” communication, the following applies: If the certificate is renewed, all operator devices must register again
- HTTP namespace reservation: Checks whether the Windows service “Unified-E Server” has been assigned the rights to listen on the port
- HTTPS certificate binding: Checks if the port is linked to the correct SSL certificate
- Firewall exceptions for port: Checks whether the Windows Firewall has the exception rule for inbound connections entered on the set port under “Gateway Address”
- Port forwarding on router (UPnP only): Checks that port forwarding has been successfully entered into the WAN router

All communication setups are automatically set up by the Unified-E service. These could be disrupted by installing other applications (e.g., another server application uses the same port) or by missing permissions from the Windows service.

2.2.5.3 Repairing communication components

For error conditions in the list above, a first remedy can be a “Repair” prompt, which can be started via buttons:

- “Repair all” button: An attempt is made to repair or restore the disturbed communication so that all communication requirements are met
- “Repair” button: The selected line in the list (communication setup) is automatically repaired, if possible

Possible causes of incorrect installation of communication:

- Port conflict with another application
- Special Windows firewall or only limited rights to configure the firewall
- No UPnP access to the router (in UPnP mode)

Possible actions in case of errors:

Often it is sufficient to change the port. After a few seconds, the “Current state” column will be updated.

2.2.5.4 SSL Certificates

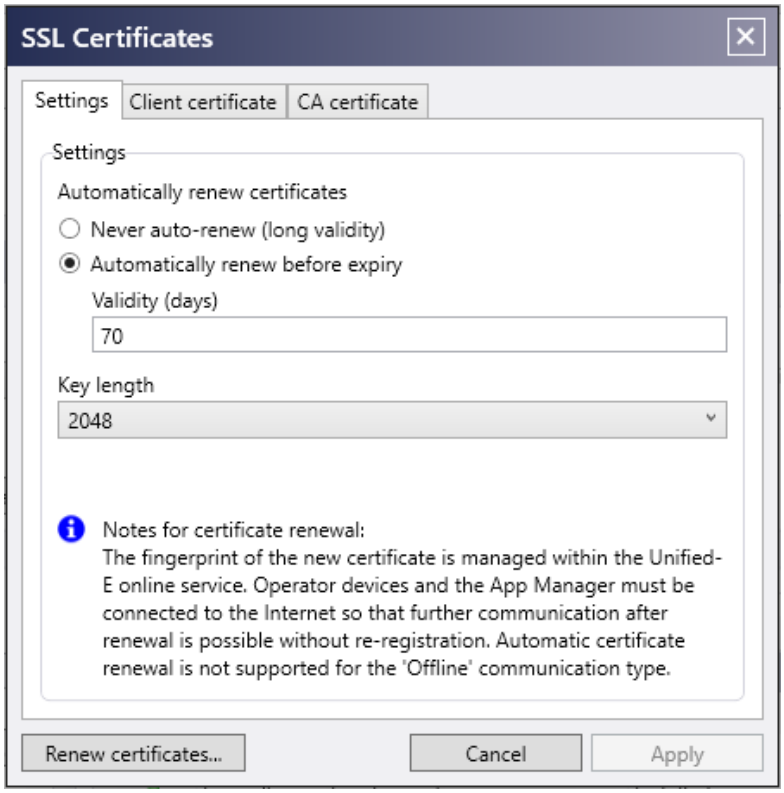
The HTTPS server embedded in the App-Manager must provide a certificate for encrypted communication. This applies to all types of communication, except for firewall-friendly communication.

Secure, self-signed certificates:

The App-Manager creates the certificates itself and stores the certificate thumbprint for the gateway name of the App-Manager in the Unified-E online service. When connecting, , the Unified-E client checks via fingerprint whether the communication is connected to the correct server and can thus communicate securely and encrypted.

Configure SSL certificate renewal:

In the “Communication setups” group, the “SSL certificates” button can be used to open the dialog for configuring certificate renewal.



In this dialog, you configure settings for the management and renewal of SSL certificates that are used for encrypted communication with the Unified-E App Manager.

- Automatically renew certificates: Specifies if and when a new certificate is automatically created and installed:
    - Never auto-renew (long validity): The certificate remains active for the entire validity period. There is no automatic renewal
    - Auto-renew before expiration: App-Manager automatically renews the SSL certificate when it falls below the remaining validity period
- Validity (days): Number of days before the expiration of the current certificate, from when the renewal is triggered
- Key Length: Select the desired key length for the certificate. The standard length is 2048 bits. Longer key lengths increase security, but can slightly affect performance

Note on certificate renewal:

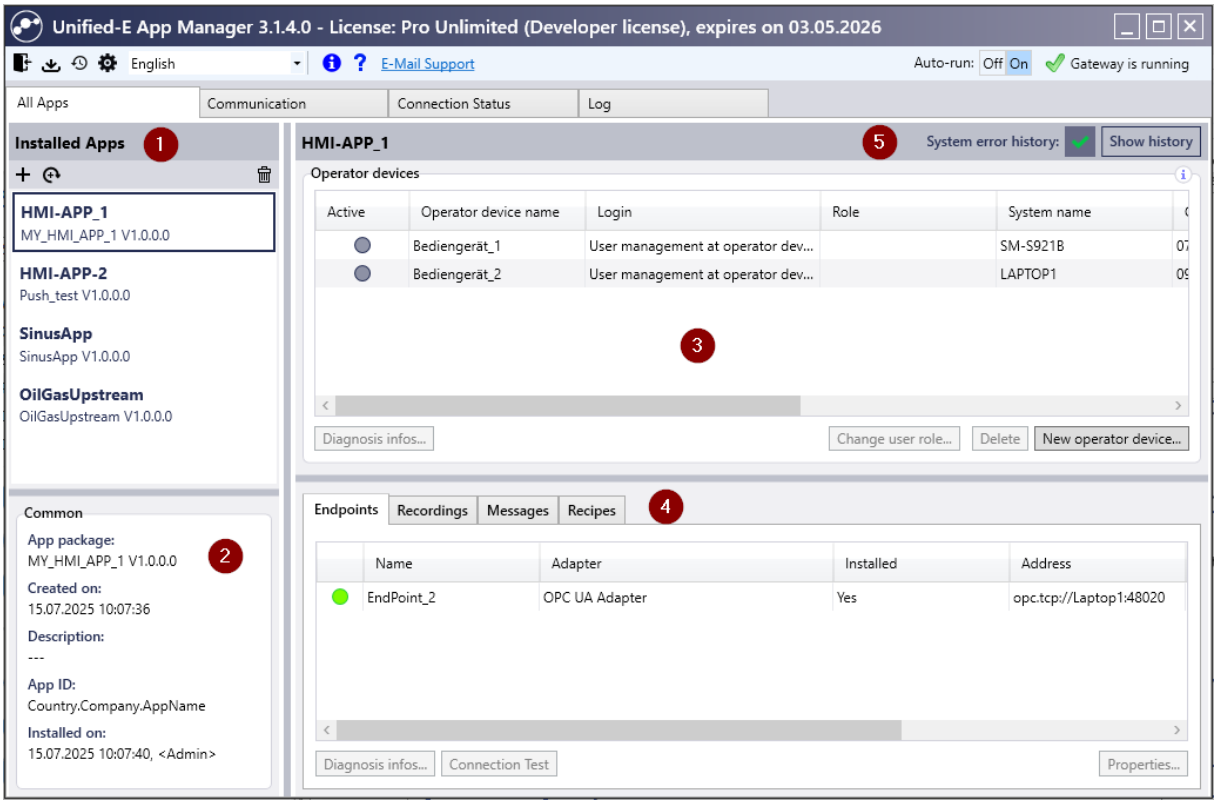
The renewal and registration of new certificates requires a working Internet connection to the Unified-E online services.

When using the “Offline” communication type, the automatic renewal of certificates does not make sense, as the online service is not available here. After a renewal, all operator devices must register again.

3 Manage HMI Apps

3.1 Overview

Hosted apps are managed in the “All Apps” tab. Multiple apps can be operated at the same time, e.g. a specific app per plant or machine within a production hall.



Areas (numbering as shown in the figure):

1. Installed Apps:
   This is where apps can be installed or deleted. When you select an app, you'll see more features for the selected app at the bottom and right.
2. Common:
   Shows general app properties.
3. Operator devices:
   This is where new operator devices are registered or linked to the App-Manager. To register, the Unified-E Client application (or “Unified-E” app for Android and iOS devices) must be installed on the operator device. After the one-time registration, the app can be started or executed as often as desired on the operator device.
4. Other Functions:
   Here you can see more functions of the selected app, which are described in detail in the following subchapters.

3.1.1 Add HMI App

Adding an app is done in the “All Apps” section. The addition can be started via the context menu or with the “+” symbol in the local toolbar.

Add app:

1. Click on the “+” toolbar button.
2. Select the app package file of the desired app in the Open dialog for which a new app instance is to be created (the app package file is generated in the App-Designer during the “Publish” process).
3. Choose an app name. This must be unique within the App-Manager.
4. Set the endpoint parameters, if necessary (chapter 3.1.3).
5. Register new operator devices. (Chapter 3.1.2.1)

Delete the app:

The selected app can be deleted via the context menu. Registered operator devices will then no longer be able to access this app afterwords.

Update the app:

An app update can be started via the context menu using the entry “Update selected app”.

When updating an app (e.g. changes in the views), the new app package file must be selected. Operator devices will automatically receive the updates when connecting—no re-registration of the devices is required.

3.1.2 Manage Operator Devices

In the “Operator devices” group, you can manage all linked operator devices of the selected app. You can add new operator devices or delete existing ones. The number of operator devices granted is based on the upper limit specified in the license. What matters is the total number of all registered operator devices across all apps.

Operator devices table:

The table shows all registered operator devices and has the following columns:

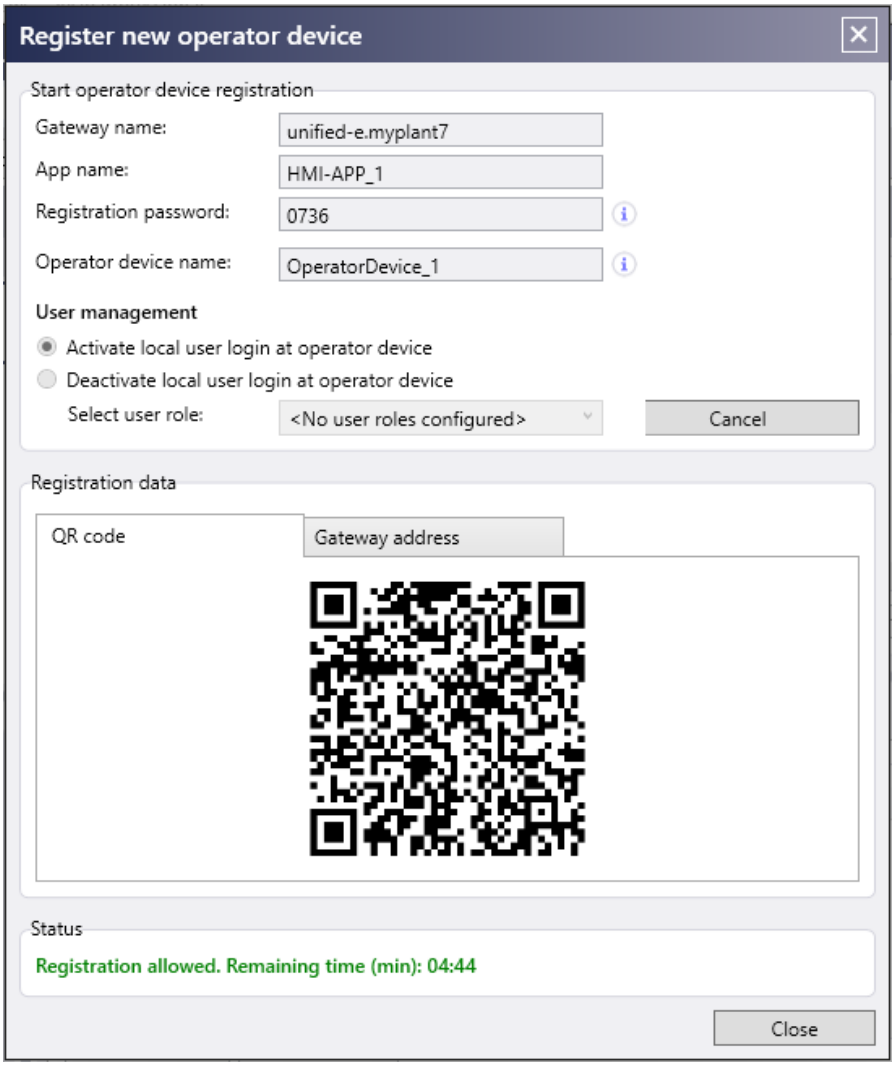
- Active: Indicates whether the operator device is currently connected. In the tooltip of the icon, status details can be viewed or the Diagnosis Info dialog can be opened to display various statistics for diagnostic purposes
- Operator device name: Name of the operator device assigned during registration
- Login: Indicates whether local user management is active on the operator
- Role: Shows the user role that applies to all users on the operator device (if local user management is disabled and user roles have been defined)

- System name: Operator device Type Name
- Created on: Date when the operator device was added
- Last access: Last connection of the operator device to the App-Manager
- Notification: …
- Language: Currently set language of the app at startup on the operator device

3.1.2.1 Add operator device

Step 1: Prepare operator device registration in App-Manager:

The “Register new operator device” dialog box is opened with the “New operator device...” button.



Step 2: Enter general registration parameters in dialog:

- Gateway name (read-only): Name of the gateway through which the operator device communicates. The name is specified by the license name (see chapter 2.1.1)

- App name (read-only): The name of the app that is to be registered or installed on the new operator device. This is transmitted to the device during registration and displayed there
- Registration password (read-only): Security code to log the device into the gateway. This password must be entered on the operator device during the registration process or automatically adopted by the QR code. The password is assigned when the registration process is started (after clicking “Start” button)
- Operator device name: Unique name for the operator device within the HMI app. This name appears later, for example, in the list of registered operator devices
- User management: Controls the permissions or the local user login to the operator device
    - Activate local user login at operator device: The operator device requires user authentication at startup. The users are managed locally in the operator device. Only possible if user roles exist and local user management has not been disabled in the HMI project
    - Deactivate local user login at operator device: There is no user login to the operator device. The visualization starts immediately after opening
        - Select user role: If user roles are configured, the role that will be assigned to the operator device at startup can be selected here

Step 3: Start operator device registration (pairing):

Once all the parameters listed above have been set, the registration can be started with the “Start” button. There are 5 minutes available for operator registration, which can be done on the operator device as described below via QR code or manually.

Registration via QR code:

For smartphones and tablets, operator registration via QR code is a good option. To do this, the Unified-E Client (Unified-E App) must proceed as follows:

1. Select the “+” icon or “Add new app” in the menu
2. Under “Gateway communication”, select the “Scan” button
3. Scan the QR code displayed in the App-Manager dialog
4. The HMI app is registered and can be started by clicking on it

If QR code scanning is not possible (e.g. Unified-E Client for Windows), then the registration data must be entered manually in the Unified-E Client (see also user manual of the Unified-E Client).

Registration via gateway address:

With the Basic license, registration on the operator device must be carried out with the IP address and port instead of the gateway name, as the Unified-E online service is not

available as an address directory for the gateway names with this license type. The IP address can be found in the registration dialog under the “Gateway Address” tab.

3.1.2.2 Delete the operator device

Normally, the deletion of an operator device is initiated by removing the corresponding app in the Unified-E Client – the operator device then automatically disappears from the list of registered operator devices.

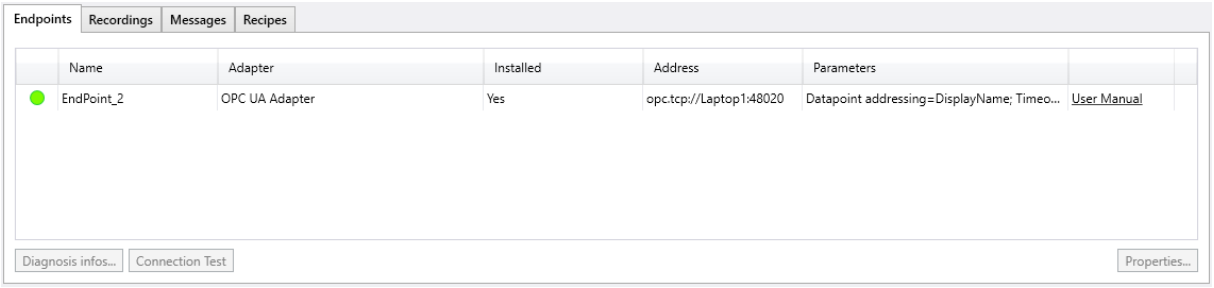
Alternatively, the operator device can be removed from the app's list of operator devices in the App-Manager by clicking on the “Delete” button.

3.1.2.3 Change user role

For an HMI app with multiple user roles, the user role can be changed via the button “Change user role...”. A re-registration of the operator device is not required for this purpose.

3.1.3 Configure Endpoints

The Endpoints table lists all the endpoints of the selected app that have been configured in the HMI project in the App-Designer.



Columns:

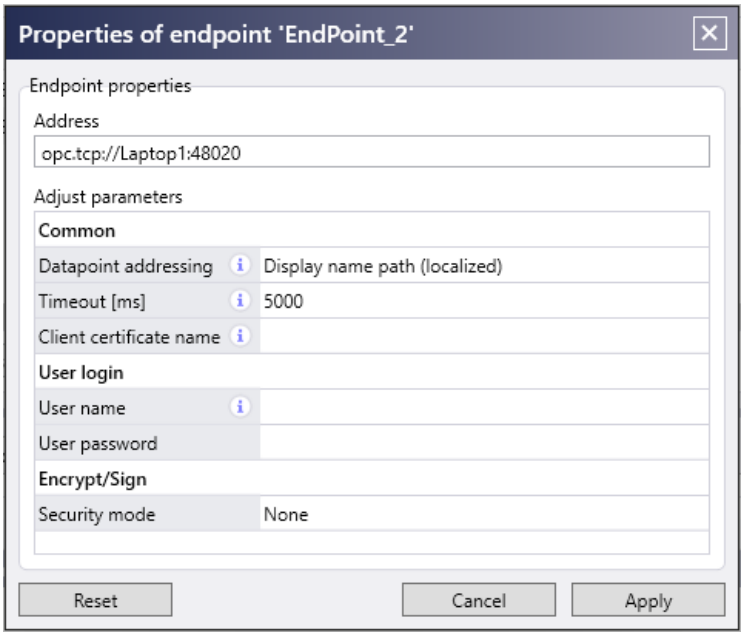
- Status: Displays the status, e.g. connected, error as a color icon. Details can be found in the tooltip
- Name: Unique object name as configured
- Adapter: Adapter name
- Installed: If “No”, then errors occurred during installation. Reinstalling the App-Manager often fixes the problem
- Address: Currently configured endpoint address
- Parameters: Displays the parameter list comma-separated
- User manual: Here you can open the PDF user manual of the adapter, which describes the address and parameterization in detail

Show diagnosis info:

With the button “Diagnosis information...” a dialog opens that shows various statistics values for reading and writing. These values can help in the search for performance problems, for example.

3.1.3.1 Adjust endpoint properties

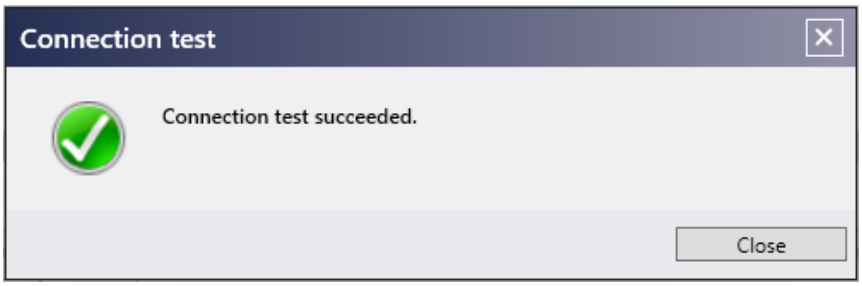
The endpoint properties in the App-Designer can be defined with the “Properties...” in the Properties dialog.



The parameters are described in the respective adapter user manual and are individual depending on the adapter. The “Reset” button can be used to reset all properties to the original values of the HMI project.

3.1.3.2 Connection

The “Connection test” button can be used to perform a connection test, for example to check adjusted endpoint parameters.



3.1.4 Manage Curve Recordings

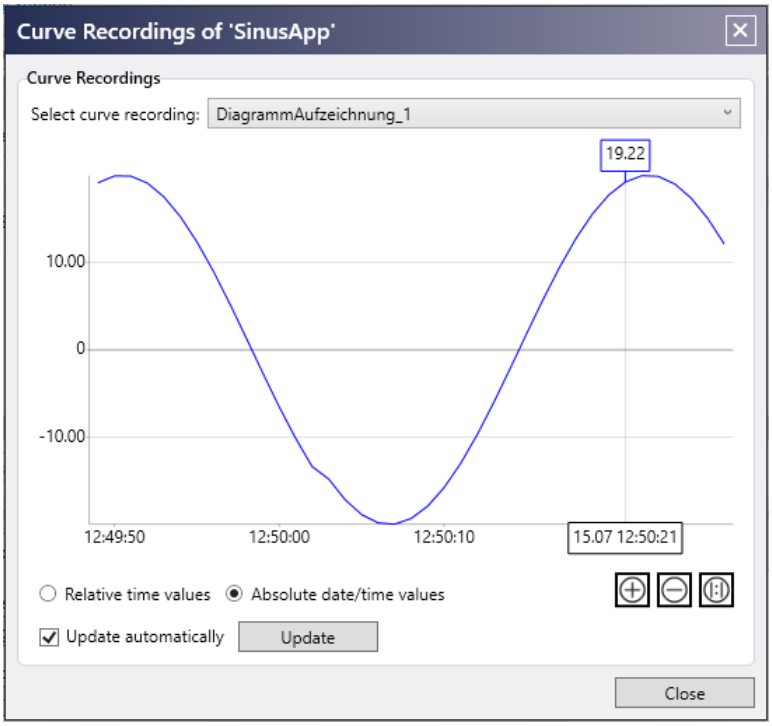
In the “Recordings” tab, you manage the centrally stored chart recordings as well as the generated CSV recording files of the selected app.

The following functions are available:

- Manage chart recordings:
  - “Chart recordings...” button: Opens the dialog to display existing chart recordings (see below)
  - “Open folder” button: Opens the folder in the file system where the chart recordings are stored. This gives you direct access to the raw data
- Managing CSV Recordings:
  - “CSV output format...” button: Opens a dialog for configuring the output format for CSV recordings.
    - “Use local culture settings” option: The Windows region settings for system accounts are used when the Unified-E Windows service is logged in to 'Local System'
    - Option “Use culture-independent settings (invariant)”: Uses the “Invariant Culture”, which is linked to the US culture (e.g. “,” for separators, “.” for decimal separators)
  - Open folder” button: opens the destination folder of the generated CSV files in Windows Explorer
- Diagnosis:
  - “Diagnosis Info...” button: Opens a separate window with detailed information to get detailed errors on recordings, e.g. when datapoints are unreachable

Chart Recordings:

The chart recordings can be accessed via the button “Chart recordings...” in the dialog and be selected for display.

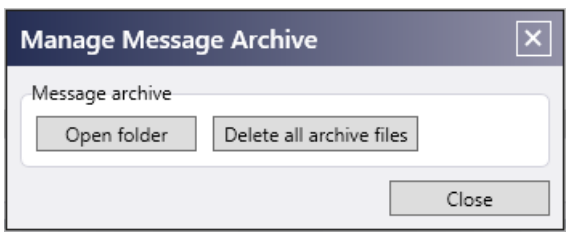


3.1.5 Manage Messages (Alarms)

The “Messages” tab allows you to manage the centrally stored message archive and the generated CSV message files of the selected app. In addition, you can define email recipients based on role assignments, which are considered when message events with email notifications are sent. Diagnostic functions are also available to help identify issues in the messaging system.

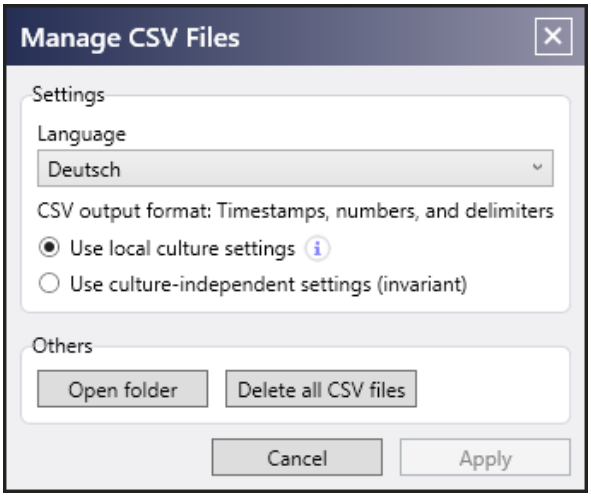
Manage message archive:

Clicking the “Message archive...” button opens a dialog where you can view the SQLite files of the message archive. You can also delete the entire archive (e.g., after creating a backup).



Manage CSV files:

Message CSV files are managed in the “Messages” tab via the CSV Files... button.



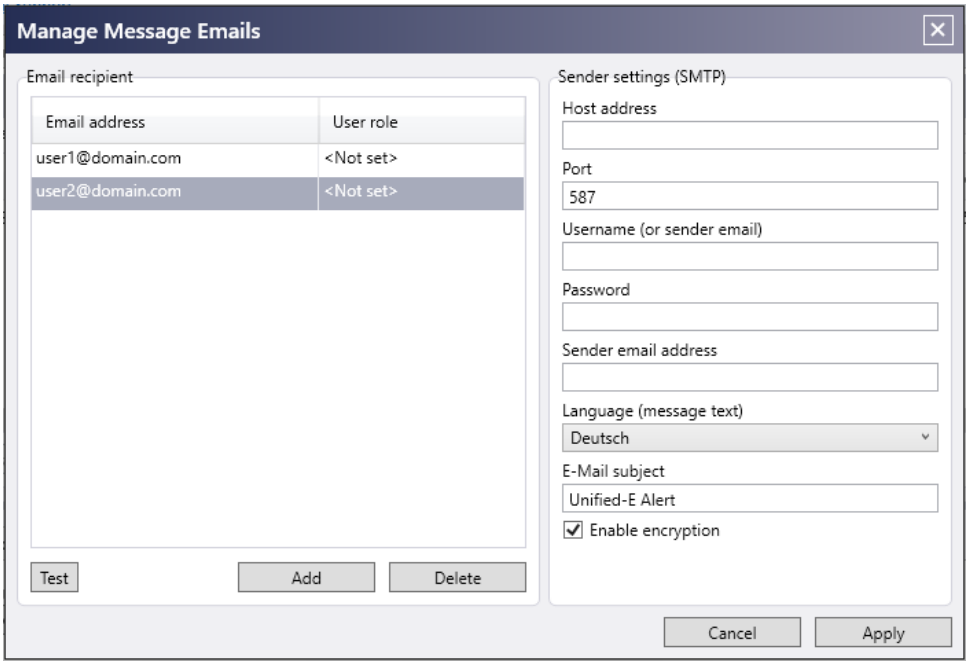
Configuration:

- Language: Selects the app language to use for CSV logging. All app languages defined in the HMI project can be selected
- CSV output format: Determines the formatting of the values, see chapter 3.1.4
- "Open folder" button: Opens the main directory of CSV message files in Windows Explorer
- "Delete all CSV files" button: Deletes all CSV message files from the main directory for CSV logging

Manage emails:

In the App-Designer, messages can be configured with the additional option "Send emails" (see user manual "Unified-E App Designer"). Both the SMTP connection data and the desired email recipients are configured exclusively in the App-Manager as follows and assigned to a user role (if available).

The "Manage Message Emails" dialog is opened in the "Messages" tab via the "Emails..." button.



E-mail recipient area: In the left pane, a list of all defined e-mail recipients is displayed:

- Columns of the “Email recipient” list:
  - Email address: Target address (recipient of the message e-mail)
  - User role: Optionally, a user role can be assigned
- Buttons:
  - Test: Sends a test message to the selected email address to verify SMTP settings
  - Add: Adds a new recipient row
  - Delete: Removes the currently selected recipient

Sender Settings (SMTP) area: In the right pane you define the sender settings (SMTP) and the sender information for sending e-mails:

- Host address: Address of the SMTP server (e.g. smtp.domain.com)
- Port: SMTP server port number (default: 587 for TLS)
- Username / Password: SMTP access credentials
- Sender email address: Address that appears as the sender in the email
- Language (message text): App language in which the text of the message is sent
- E-Mail subject: Subject line of the message sent
- Enable encryption: Enables transport encryption (TLS) for sending

Show diagnosis info:

The “Diagnosis info...” button opens a separate window with detailed information to analyze message processing issues, such as when email delivery fails or messages can’t be added to a CSV file.

3.1.6 Manage Recipes

Recipe datasets are stored in Unified-E as XML files. A separate file is created for each data dataset – or per version, depending on the configuration in the HMI project – and managed centrally in the App-Manager for all operator devices.

In the “Recipes” tab, you have access to the recipe datasets generated during operation. Clicking the “Open folder” button opens the main folder in Windows Explorer. Recipe files can be manually added or deleted there (import/export) or regularly backed up.

3.2 System Error History

System errors are internal error states of the Unified-E system, e.g. connection problems to endpoints or errors when writing files. They are automatically detected and logged. System errors affect the technical operation of the App-Manager itself.

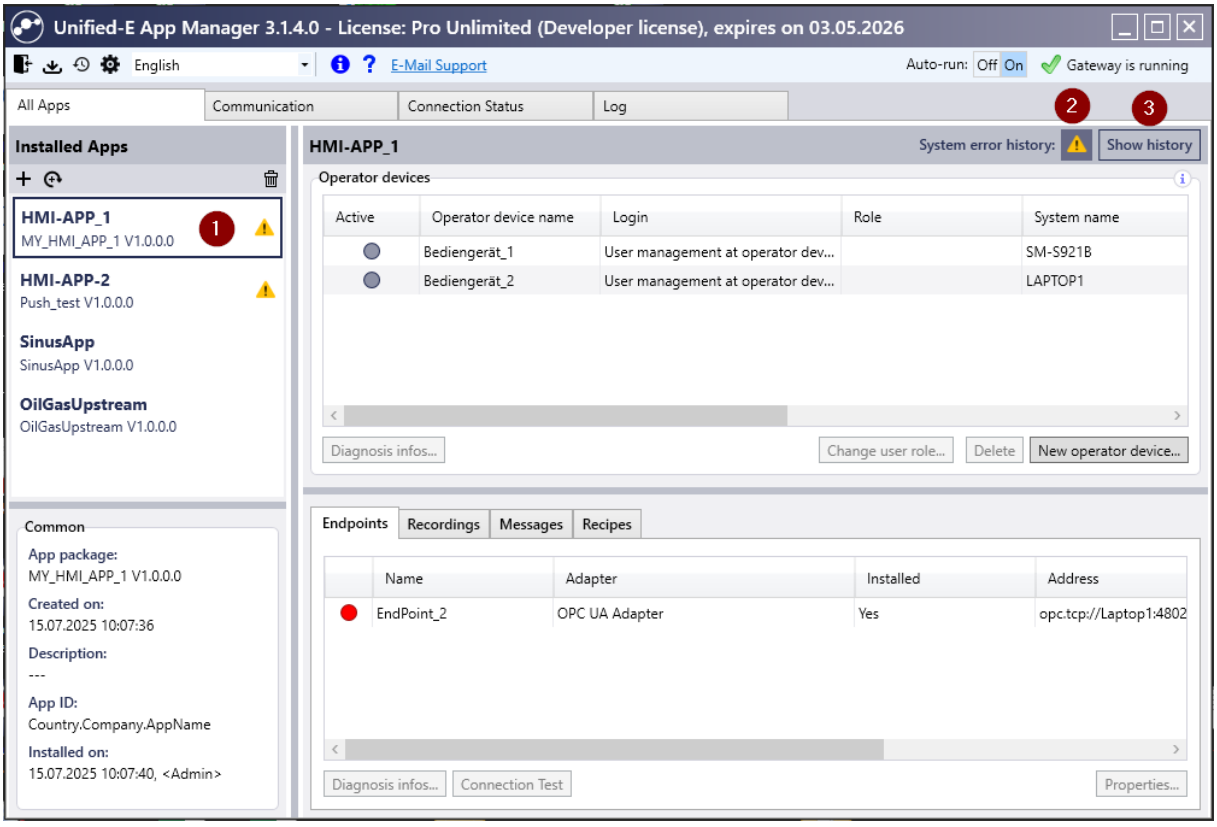
Messages, on the other hand, are user-defined events that have been specifically configured for visualization in the HMI project – such as machine states, warnings or system errors. They are used to monitor the plant.

Summarized:

- System error = technical fault in the App-Manager
- Message (alarm) = project-specific information from the machine or plant

System Error Indicator:

Upcoming system errors are indicated with a warning icon.



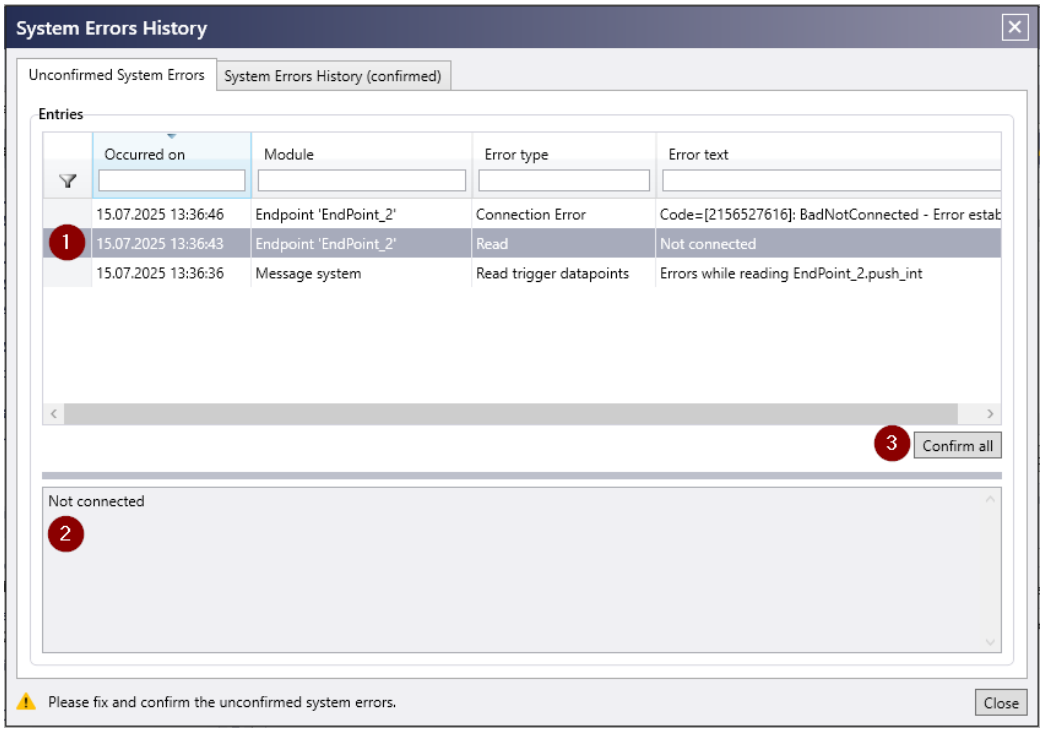
System error elements (numbering according to figure):

1. Warning icon (app selection): The warning icon appears to the right of the app name if there are unconfirmed system errors with the app
2. Warning icon (header): The warning icon appears when the selected app has unconfirmed system errors
3. “Show history” button: Opens a dialog with system errors. System errors can be confirmed here (see below)

Confirm system error and display history:

System errors can be confirmed (i.e. acknowledged or acknowledged) in both the HMI app and the App-Manager. To confirm in the App-Manager, it opens the dialog via the “View history” button.

Unconfirmed system errors can be displayed or confirmed in the dialog as follows.



Elements of the System Error History dialog (numbering according to the figure):

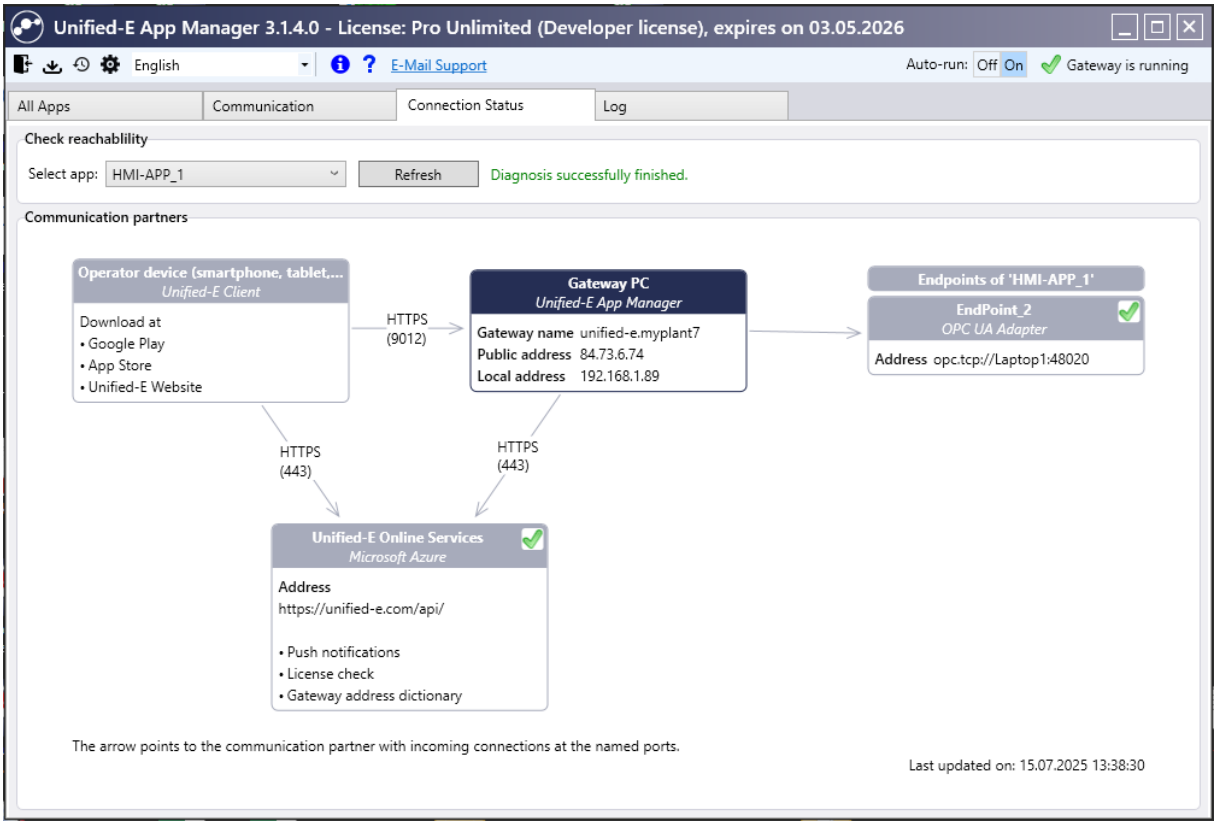
1. System Error list: Contains all pending or unconfirmed system errors
2. Details area: The error text of the selected system error is displayed here in multiple lines
3. “Confirm all” button: All system errors are confirmed, i.e. deleted from the list. If a confirmed system error occurs again, an entry in the system error list is made again

4 Connection Status & Diagnostics

In the “Connection status” tab, you can find important information about how communication takes place between the connection participants of the selected app and whether they can be reached.

The view also shows which ports are used to handle incoming and outgoing connections. To check accessibility, select the desired app above. The endpoint connections of the selected app are also checked.

Configuration:



5 Activity Log

Important activities such as operation (setpoint change) are recorded in detail in the log.

There are the following log categories:

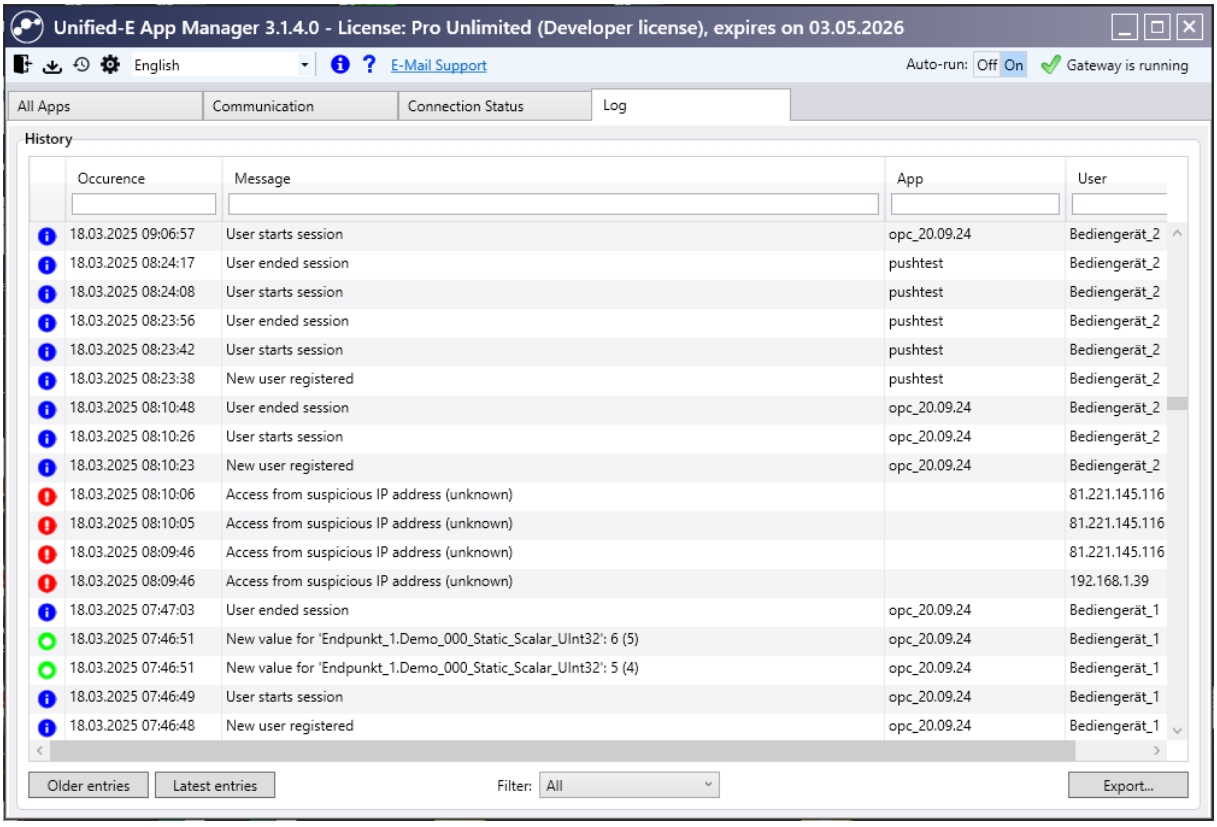
- Information (blue “i” symbol): General information, e.g. “User starts connection”
- Operation (green icon): A user has changed a value. Both the old and the new value are listed
- Important (red “!” icon): Events that require increased attention, such as when unauthorized requests have been detected

The log entries are stored in signed XML files. To keep the files manageable in size, a separate log file is used per month.

In the Settings dialog, you can configure whether and when older log entries or monthly files should be deleted (see chapter 6.1).

History list:

The list in the user interface always shows only the number of entries that is defined in the log settings.



Footer of the protocol list:

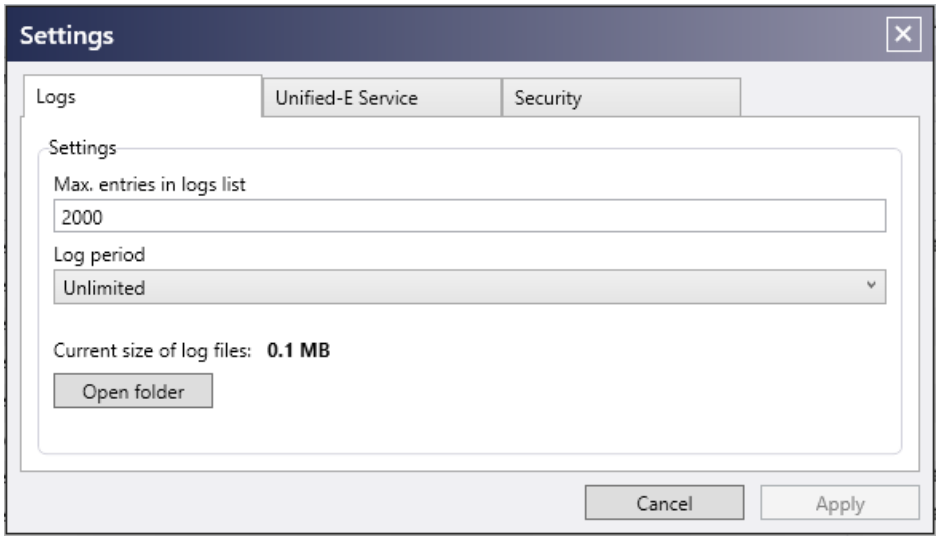
- “Older entries” button: Loads older entries starting from the current list (scrolls down)
- “Newer entries” button: Loads newer entries (scrolls to the top)
- Filter: Allows you to filter the list by category
- Export: Exports the list to the clipboard (e.g. for Excel) or as a CSV file

6 Settings Dialog

In the settings dialog, general settings can be configured. The dialog can be opened via the toolbar (gear icon). The various settings are grouped into tabs and are described in the following subchapters.

6.1 Configure Logs

In the “Log” tab of the settings dialog, you can configure how many entries are displayed in the log list and how long log files are stored.



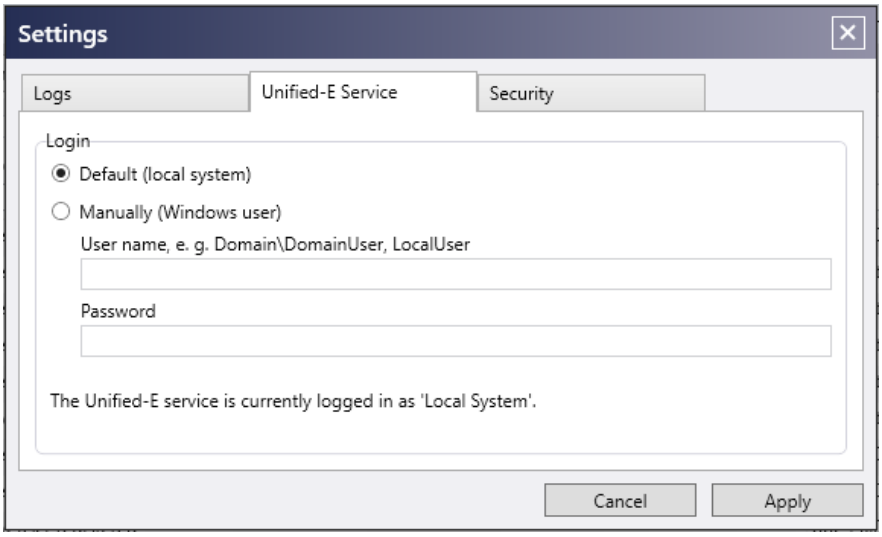
Configure log settings:

- Max entries in the log list: Specifies the maximum number of entries that are displayed in the log list (“Log” tab) at the same time. Older entries are automatically hidden if necessary, but not deleted.
- Log period: Determines how long log files are retained:
  - Unlimited: No automatic deletion
  - 6 months / 12 months / 24 months: Older monthly files are automatically deleted after the selected period has expired
- Current size of log files: Shows how much disk space the log files created so far are taking up
- “Open folder” button: Opens the location of signed XML log files in Windows Explorer

6.2 Configure Unified-E Service

In this tab, you specify which Windows credentials are used to run the Unified-E service, which handles the HMI app requests and monitors alarm message events, on the plant.

Set the login data to “Manually” if the default user “Local System” does not have enough permissions to access files (e.g. database files), for example.

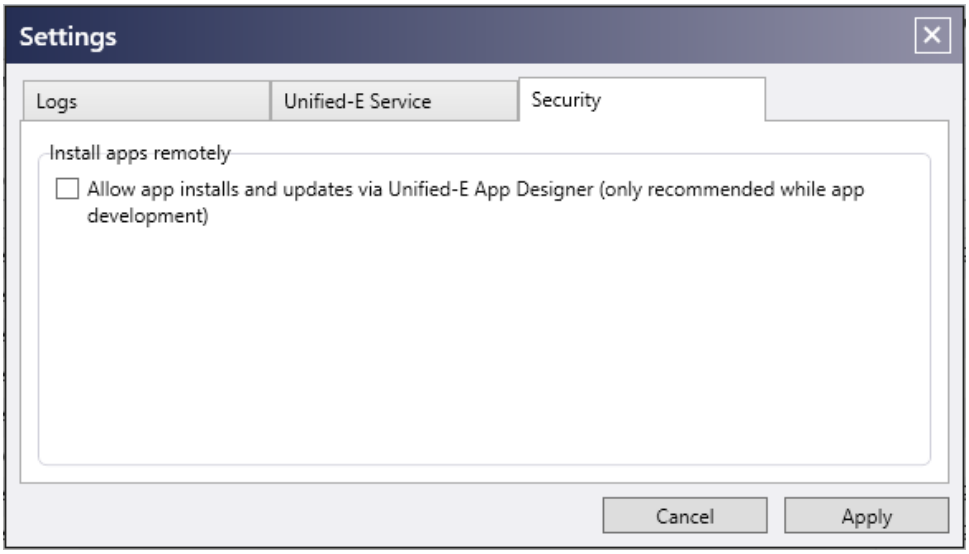


Set login details:

- Standard (Local System): The Unified-E service runs under the built-in Windows account “Local System”. This setting is active by default and is sufficient for most installations.
- Manually (Windows user): Alternatively, a custom Windows account can be used. This may be necessary, for example, if the service needs to access network resources for which the Local System user does not have permission. To do this, enter the following information:
    - User name (in the format Domain\User or LocalUser)
    - Password of the specified user

6.3 Configure Security

In this tab, you can specify whether app installations and updates are allowed remotely via the Unified-E App Designer during the “Publish” process. This option is intended for development or testing purposes only and should be disabled in production for security reasons.



7 Appendix

7.1 Support and further information

For further information on the use of the Unified-E App Manager, please visit our website at www.unified-e.com . In particular, the “First Steps” section offers a compact introduction with clear examples and frequently asked questions.

If you need technical support or have specific questions about your configuration, you can always contact our support team. To do so, please send an e-mail to:

support@unified-e.com

We will do our best to process your request as quickly as possible. Please include relevant screenshots or a short description of your project structure in your email – if available – to enable efficient editing.