

SIEMENS

SIMATIC HMI

Unified Comfort Panels Industrial Edge Device - Operation

Operating Manual

<u>Preface</u>	1
<u>Security</u>	2
<u>Notes on use</u>	3
<u>Overview</u>	4
<u>Initializing Edge Mangement</u>	5
<u>Central Edge Management via IEM</u>	6
<u>Local Edge Management</u>	7
<u>Application examples</u>	A

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Preface	4
2	Security	5
2.1	Industrial security	5
2.2	Data protection.....	7
3	Notes on use	9
3.1	Notes on central Edge Management.....	9
3.2	Notes on creating apps for Unified Comfort Panels	10
4	Overview	12
5	Initializing Edge Mangement	15
6	Central Edge Management via IEM	18
6.1	Overview	18
6.2	Notes on operation	20
6.3	Additional Settings.....	21
6.3.1	Configuration	21
6.3.2	System	22
7	Local Edge Management	23
7.1	Overview	23
7.2	Apps.....	25
7.3	Management	29
7.4	Statistics.....	30
7.5	Settings	31
7.5.1	Configuration	31
7.5.2	Connectivity	32
7.5.3	System	37
7.5.4	Developer mode	40
A	Application examples	42

Preface

Purpose of this document

This documentation provides the basic information you need to manage and operate a Unified Comfort Panel as an Industrial Edge Device.

This documentation is aimed at operators who, for example, commission and operate Edge Devices or install and run Edge Apps, as well as service and maintenance technicians who perform error analysis.

Basic knowledge required

- Solid knowledge of personal computers is required.
- Solid knowledge of Linux-based operating systems is required.
- Solid knowledge of IP-based networks is required.
- General knowledge in the field of IT is required.
- Solid knowledge of Docker is required.
- General knowledge in the field of automation technology is recommended.

Scope of this document

This operating manual is valid for Unified Comfort Panels in conjunction with HMI device image version 17.0.0.2 or higher.

Conventions

The terms "Edge Device" and "HMI device" apply to a Unified Comfort Panel.

The term "app" is also used instead of the "Industrial Edge App" designation.

The term "IEM" is also used instead of "Industrial Edge Management".

Documentation

In addition to the information in this document, observe the following manuals:

- Unified Comfort Panels operating instructions
(<https://support.industry.siemens.com/cs/ww/en/view/109773257>)

When using Local Edge Management:

- Industrial Edge App Publisher - Operation
(<https://support.industry.siemens.com/cs/ww/en/view/109804060>)

For Central Edge Management:

- Industrial Edge Security manual
(<https://support.industry.siemens.com/cs/us/en/view/109781002>)
- Industrial Edge Management - Getting Started
(<https://support.industry.siemens.com/cs/ww/en/view/109804065>)

Security

2.1 Industrial security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (<http://www.siemens.com/industrialsecurity>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at (<https://support.industry.siemens.com/cs/start?lc=en-WW>).

Certificates

In Industrial Edge, trusted certificates are used for accessing Edge Management. For security reasons, import and use your own trusted certificates for Edge Management.

Sensitive resources and secrets in apps

In Industrial Edge, customers can develop their own apps and install the apps on Edge Devices.

Do not store secrets and do not use sensitive system resources in mounted volumes of the host system in custom-developed and installed apps.

Encrypted communication for apps

Customers are responsible for implementing encrypted and secure communication (e.g. https) for their apps used on the Edge Devices.

Encrypted communication between Industrial Edge Management System and Edge Devices

Customers are responsible for implementing encrypted and secure communication (e.g. https) between the Industrial Edge Management System and their Edge Devices.

Encrypted communication between the multiple Edge Devices

Customers are responsible for implementing encrypted and secure communication (e.g. https) between their Edge Devices.

Protection of the development PC and own development apps

In Industrial Edge, customers can develop their own apps and install the apps on Edge Devices.

Customers are responsible for protecting their own development PCs and preventing unauthorized access to their development PCs. In addition, customers are also responsible for protecting their own apps with regard to security and preventing unauthorized access to their own apps.

Ethernet communication

With Ethernet-based communication, end users are responsible for the security of their data network because proper functioning cannot be guaranteed under all circumstances, for example, in the event of targeted attacks that result in an overload of the device.

Notes on protecting administrator accounts

A user with administrator rights has extensive access and manipulation options available to the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

Protection of Industrial Edge Management System and Edge Devices

In Industrial Edge, Docker containers are used to use the Industrial Edge Management System.

Customers are responsible for protecting their own Industrial Edge Management System and their own devices and for preventing unauthorized access to the Industrial Edge Management System and the Edge Devices. Also customers are responsible for protecting the relay servers within the Industrial Edge Management System and for preventing unauthorized access to the relay servers.

Read and write access to controllers

Industrial Edge does not in itself support read or write access to controller data. Customer apps can support read write access to controller data.

Customers are responsible for managing read and write access of apps to controller data. Customers are responsible for any damages that are caused by changing or overwriting controller data. In addition, customers are also responsible for protecting their own apps that have write access to controller data with regard to security and preventing unauthorized access to their own apps.

External storage media

Edge Devices may have interfaces for external storage media such as memory card or USB interfaces.

Customers are responsible for protecting data stored on external storage media against unauthorized access. For example, use a suitable encryption or password protection for external storage media. Store the external storage media in a safe place.

Observe the security guidelines and information on external storage media in the Operating Instructions of your Edge Devices.

In addition, observe the security statements, which are also valid for this documentation, from the "Industrial Edge - Security overview (<https://support.industry.siemens.com/cs/us/en/view/109781002>)" manual.

2.2 Data protection

Siemens adheres to the principles of data protection, in particular the principles of data minimization (Privacy by Design).

For this product, this means:

Personal data

The product edits and saves the following personal data:

- User name (e.g. Login) containing first and/or last name directly or may be associated to first or last name
- Time stamp
- Location data (time zone)
- IP addresses
- MAC addresses
- Computer name

If the user links the data mentioned above to other data (e.g. shift plans) or if the user saves personal information on the same medium (e.g. hard disk) and thus creates a personal reference, the user has to ensure that the guidelines regarding data protection are observed.

Purposes

The data mentioned above is required for the following purposes:

- Access protection and safety measures (e.g. login, IP addresses)
- Process synchronization and integrity (for example information about time zones, IP addresses)

Storage of the data is effected for a suitable purpose and is limited to what is strictly necessary, as the information is indispensable in order to identify the authorized operators.

Data configuration

The customer can configure the data collected via the product as follows:

- Displaying data in process screens
- Data display in the form of reports, for example, for printing or for displaying as an electronic file

Guidelines for the deletion of data

This product does not provide for the automatic deletion of the data mentioned above. If required, these can be deleted. Please contact the product documentation or the customer support for this purpose.

Backing up data

The data mentioned above are not stored in anonymized or pseudonymized form, because the purpose of identification of the operators can otherwise not be achieved.

Notes on use

3.1 Notes on central Edge Management

Passwords

Whenever you set a password (except for the proxy password), the password must meet the following criteria:

- At least 8 characters
- At least 1 upper case letter
- At least 1 special character
- At least 1 number

The following characters are recognized as special characters: ! @ # \$ % ^ & * . () _ +

Time synchronization of the Industrial Edge Management and Edge Devices

A flawless operation of the Industrial Edge Management and Edge Devices require time synchronization of the Industrial Edge Management and Edge Devices. To properly synchronize the time on the Industrial Edge Management and Edge Devices, an NTP server is required.

Either use the default configured Debian NTP servers which will be used once you connect the Industrial Edge Management PC to the Internet. Or, when you operate the Industrial Edge Management and Edge Devices disconnected from the Internet in your local network, provide an own NTP server that can be accessed by the Industrial Edge Management and the Edge Devices.

Usage of a proxy server

If you use a proxy server to connect to your Industrial Edge Management, you must add the IP addresses of the Industrial Edge Management and all Edge Devices to the no proxy address list in the "Settings > Connectivity > Proxy" settings in the Maintenance UI.

Network connection of the Edge Devices

We recommend that you refrain from disconnecting the network connection of connected Edge Devices when switching off or restarting due to performance problems.

3.2 Notes on creating apps for Unified Comfort Panels

Docker IP range of Edge Devices

For Edge Devices, the IP range 172.17.0.0/16 is reserved for Docker by default. If you want to onboard an Edge Device whose IP range is 172.17.0.0/16, change the Docker IP range of the Edge Device when you create the Edge Device configuration file before you onboard the Edge Device. Otherwise, issues may occur in onboarding the Edge Device or installing apps on the Edge Device.

Hard reset

It is not recommended to power-off the device during the hard reset process.

Stopped NTP services

Whenever the NTP services have stopped running, an alert is generated indicating that the NTP services have stopped and you need to adjust the NTP settings. In that case, navigate to the NTP settings, edit any setting and save the changes. By that, the NTP services are getting restarted.

3.2 Notes on creating apps for Unified Comfort Panels

Observe the following information when creating apps for Unified Comfort Panels from standard Docker images.

Creating Docker images

Observe the following information when creating apps for Unified Comfort Panels

Docker network driver

The Docker internal network for Industrial Edge on Unified Comfort Panels is working in the "bridged" mode. Use the "bridge" Docker driver.

WinCC Unified communication mechanism

Use the WinCC Unified Open Pipe mechanism to communicate with the Unified Runtime software on an Edge Device.

You can find the WinCC Unified Open Pipe manual on the internet (<https://support.industry.siemens.com/cs/ww/en/view/109778823>).

Service life of the internal memory

Cyclic write access to internal memory is not permitted, because it reduces the service life of the internal memory and thus of the HMI device, for example, an app generating permanent system alarms or user-defined messages in the alarm buffer.

To prolong the service life of your HMI device, you should preferably use external memory cards to store and log data. In addition, you can activate internal flash memory monitoring in the Control Panel of the HMI device.

You can find information on supported memory cards and on flash memory monitoring in the Unified Comfort Panels Operating Instructions.

Storage locations on external storage media

It is recommended to use external storage media to store and log data. Use the following predefined storage locations.

Volume name, long term stable (LTS)	Mount point (on host)	Device interface	Storage medium
data-storage	/media/simatic/data-storage	X51	SD data memory card
data-storage-1	/media/simatic/data-storage-1	X61	USB stick
data-storage-2	/media/simatic/data-storage-2	X62	USB stick

Generating apps with Industrial Edge Publisher

Use the Industrial Edge App Publisher to prepare your app for its installation on the Edge Device.

You will find the Industrial Edge App Publisher documentation on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109804060>).

Overview

SIMATIC HMI Unified Comfort Panels offer you all the freedom and options you need to implement your innovative operating concepts.

In addition to significantly increased performance, the user benefits from the new possibilities of the panels in conjunction with the SIMATIC WinCC Unified visualization software as well as the functional expandability with apps via the built-in Industrial Edge functionality.

This document supplements the operating instructions for the Unified Comfort Panels on which it is based. You can find the basic Unified Comfort Panels operating instructions on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109773257>).

This document contains important information of how to use Industrial Edge functionality on Unified Comfort Panels. For successful setup and operation, observe the information in this document.

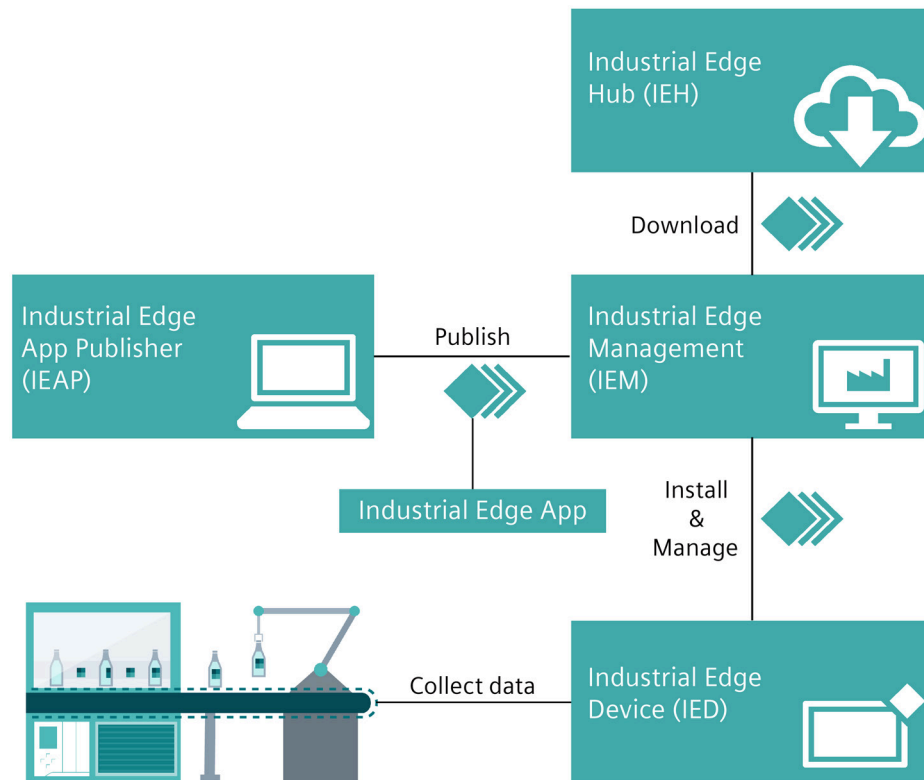
You will find a general overview and more information on Industrial Edge on the Internet (<https://new.siemens.com/global/en/products/automation/topic-areas/industrial-edge.html>).

Edge Management types

SIMATIC HMI Unified Comfort Panels support either of the following Edge Management variants.

Central Edge Management via IEM - "Backend Managed"

The following figure illustrates how a Unified Comfort Panel is used as an Industrial Edge Device within an Industrial Edge Management system (IEM).



The Unified Comfort Panel Industrial Edge Device is integrated in an Industrial Edge infrastructure and connected to a central Industrial Edge Management instance.

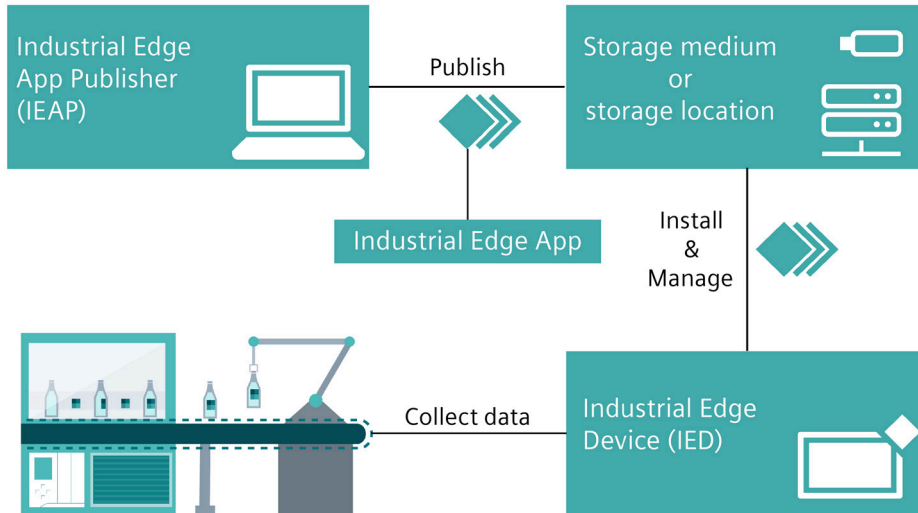
Central Industrial Edge Management includes, for example:

- Onboarding and offboarding of Edge devices
- Diagnostic information management of all Edge Devices at a central location
- Downloading apps from an Industrial Edge Hub
- Version management of Edge apps
- Importing apps from the Industrial Edge Publisher
- Installing and uninstalling apps to single, multiple or individually grouped Edge Devices

You will find detailed information on Central Edge Management in the following manual on the internet: Industrial Edge Management - Getting Started (<https://support.industry.siemens.com/cs/ww/en/view/109804065>)

Local Edge Management - "Standalone"

The following figure illustrates how a Unified Comfort Panel is used as a standalone Industrial Edge Device without an Industrial Edge Management system.



The Unified Comfort Panel Industrial Edge Device operates standalone using its own Industrial Edge infrastructure, operating and managing apps locally on the device. In addition, the Unified Comfort Panel may be connected to a network to install apps from a storage location.

Local Industrial Edge Management includes, for example:

- Installing and uninstalling apps from an external storage medium or an external storage location
- Updating apps
- Starting and stopping apps
- Diagnostic information management of all running apps
- Remote Edge Device Management via a web browser

Licensing

Note that licensing for "Backend Managed" and "Standalone" Edge Management differs, please refer to the following locations:

- "Standalone": QR code under "Control Panel" > "Apps" > "SIMATIC Apps" containing the licensing link (<https://www.siemens.com/comfort-edge-activation>).
- "Backend Managed": Industrial Edge Management - Getting Started (<https://support.industry.siemens.com/cs/ww/en/view/109804065>)

Initializing Edge Management

You can use either local or central Edge Management on a Unified Comfort Panel.

The corresponding setting is performed on the device by activating Edge Management and opening Edge Management for the first time.

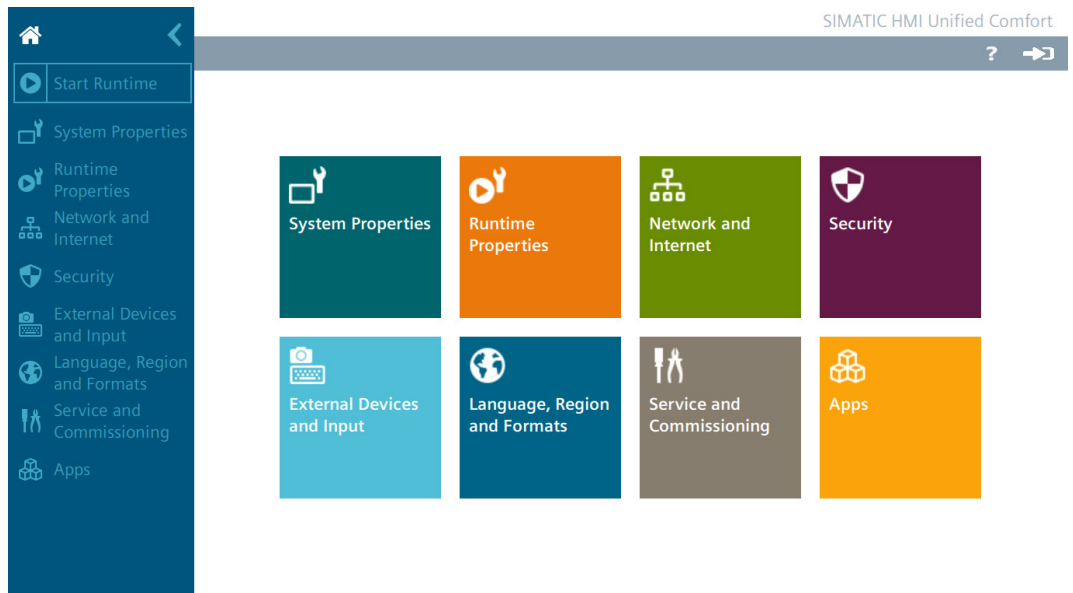
Prerequisite

- You can login to the Unified Comfort Panel as a user with the "Control Panel access" function right.

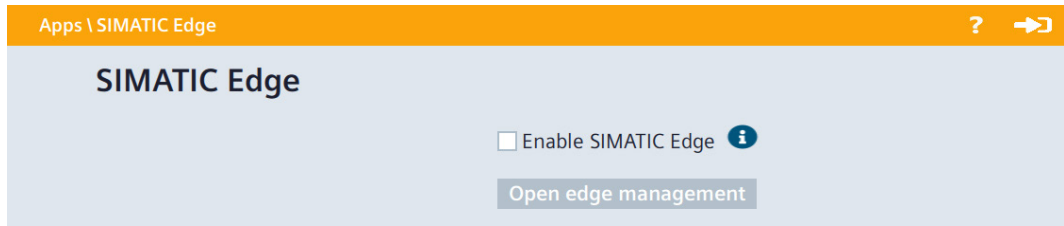
Procedure

Proceed as follows to initialize Edge Management for the first time.

1. Switch on the power supply of the Unified Comfort Panel.
2. Open the Control Panel.



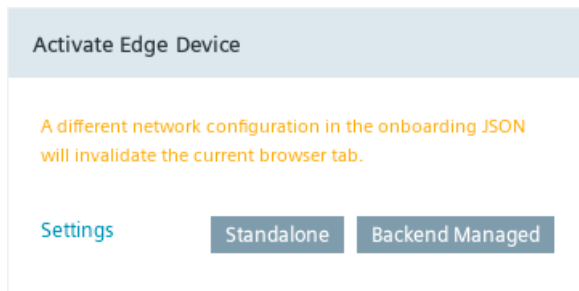
3. Select "Apps" > "SIMATIC Edge".



4. Activate the "Enable SIMATIC Edge" option and wait until the "Open edge management" button becomes active.
5. Click the "Open edge management" button.

In case you receive a security risk warning, click "Advanced" > "Accept the Risk and Continue".

The "Activate Edge Device" dialog is displayed.



Note

Edge Management type is selected once

Once "Standalone" or "Backend Managed" has been selected, the selection is stored and the "Activate Edge Device" dialog is not going to be displayed any more.

You have the following possibilities to revise your selection and display the initial "Activate Edge Device" dialog again:

- Updating the HMI device operating system by loading an HMI device image.
- Restoring a backup file.
- Performing a "Hard Reset" on the Unified Comfort Panel under "Settings > System"

-
6. You can use the "Settings" link to specify the following parameters for "Standalone" or "Backend Managed" Edge and the Unified Comfort Panel, if required:
 - "LAN": IP addresses of the X1 and X2 interfaces of the Unified Comfort Panel
 - "Proxy": IP address/port and user name/password for a proxy server
 - "Docker Network": IP address and subnet mask of the Industrial Edge Management instance
 - "System" > "Download Logs":
 - "System" > "NTP Server": Add or remove NTP servers used by the Unified Comfort Panel

- Click "Standalone" for using local Edge Management or "Backend Managed" for using the central Edge Management IEM with your Unified Comfort Panel.

Selecting "Backend Managed" will display the "Activate Edge Device" dialog.

- Specify an Edge Device configuration file that has been created via the IEM and that was copied to an external storage medium or a local drive on your device. Use the "Browse" button to open a file selection dialog.

Note

Remote access facilitates Edge Device configuration file transfer

As an alternative to direct operation on the device, you can access the Unified Comfort Panel and activate the Edge Device via remote access from a browser on the remote machine on which the configuration file has been created. In this case, clicking the "Browse" button will open the file selection dialog on the remote machine.

Settings

No further settings are required if your Edge Device configuration file contains all information including the "LAN", "Proxy", "Docker Network" and "NTP Server" settings.

Use the "Settings" link to specify missing parameters if your Edge Device configuration file does not yet contain those settings. Amongst others, you will find a description of those settings in chapter "Settings (Page 31)".

- Click "Activate" to connect to the IEM or "Skip" to cancel and log in to "Standalone" Edge Management.

You will find detailed information on connecting an Edge Device in the Industrial Edge Management Getting Started manual on the internet (<https://support.industry.siemens.com/cs/ww/en/view/109804065>).

Depending on your selection, proceed as described in the following sections.

See also

Central Edge Management via IEM (Page 18)

Local Edge Management (Page 23)

Central Edge Management via IEM

6.1 Overview

The following central Edge management functions are available with "Backend Managed" Edge through the IEM and on the Unified Comfort Panel Edge Device:

- Installing apps through the IEM.
- Managing apps through the IEM and on the Unified Comfort Panel.
- Displaying the status of hardware, installed and running apps and their memory consumption on the Unified Comfort Panel.
- Managing connectivity and system settings on the Unified Comfort Panel.

All Edge Management activities are typically performed via the IEM user interface, refer to the following manual on the internet: Industrial Edge Management - Getting Started (<https://support.industry.siemens.com/cs/ww/en/view/109804065>)

Requirement

- Edge management is enabled in the Control Panel of the Edge Device under "Apps" > "SIMATIC Edge" > "Enable SIMATIC Edge".
- The Edge Management type is set to "Backend Managed", refer to chapter "Initializing Edge Management (Page 15)".

Launching Central Edge Management

The "Sign in" dialog is automatically displayed after you successfully activated "Backend Managed" Edge for the first time.

Otherwise, proceed as follows to open Edge Management:

1. Open the Control Panel and click "Apps" > "SIMATIC Edge" > "Open edge management".

The "Sign in" dialog is displayed.

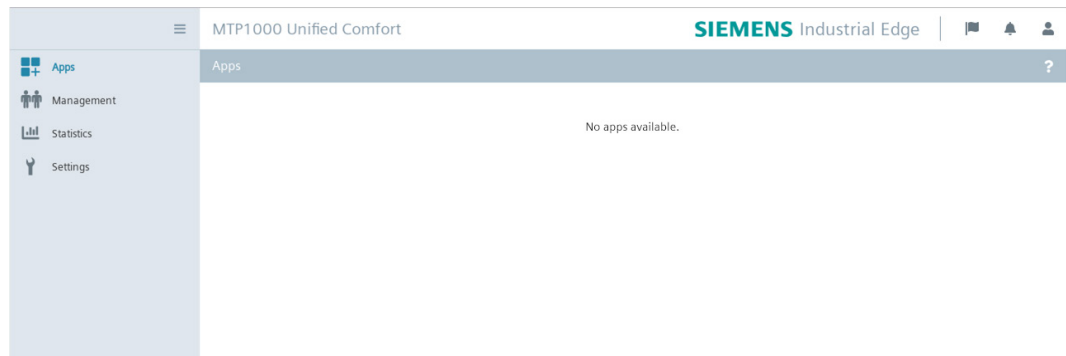
2. Specify the credentials of a user who has been assigned the "Control Panel access" function right in the configuration. For more information, refer to the Operating Instructions.

3. If required, click "Certificate" to specify a certificate for secure communication.
4. Click "Sign in".

The Edge Device user interface

After successful login, the "Apps" screen of the Edge Device user interface is displayed. The layout of the "Apps" screen varies depending on whether or not apps have already been installed.




If there are no apps installed yet, the "Apps" screen is displayed as follows:



Once an app was installed via the IEM, it will be displayed in the "Apps" screen. The following screen shows an example.



The following functions are available in the upper right header area of the Edge Management screen, independent of the entry selected in the navigation menu.

	"Tasks" icon to display the status of ongoing or finished tasks such as the installation of an app.
	"Events" icon to display the "Recent events" window. The "Recent events" window contains alerts and notifications of the following types: <ul style="list-style-type: none"> • Available app update notifications • CPU utilization alerts • Memory utilization alerts • Storage utilization alerts
	"User" icon to display the name of the current user or to log out.

The following entries are available in the navigation menu on the left of all screens:

- "Apps" to open, uninstall or display information on apps.
- "Management" to uninstall, restart, stop or display detailed information on apps.
- "Statistics" to display performance-related information of hardware and apps.
- "Settings" to view information and adjust connectivity and system parameters.

If viewing or changing some settings on the Edge Device is required in your Central Edge Management environment, please refer to the description of the navigation menu entries in chapter "Settings (Page 31)".

See also

Additional Settings (Page 21)

6.2 Notes on operation

Observe the following notes when using Central Edge Management with a Unified Comfort Panel:

- The user management of the Unified Comfort Panel is used.
The "Edge Device Username (Email)" and "Edge Device Password" specified in the configuration file via IEM will be ignored.
- Apps are installed via the IEM, they cannot be installed via the Edge Device user interface on the Unified Comfort Panel.
- Performing a "Reset" under "Settings > System" will delete all Edge-related data and configuration information on the device.

The device will stay onboarded in the IEM if it was onboarded before.

- Performing a "Hard Reset" under "Settings > System" will delete all Edge-related data, configuration information and initialization information on the device.

The device will be offboarded and removed from the IEM catalog.

- When you update the operating system of an already onboarded Unified Comfort Panel Edge Device, the device will stay visible in the IEM catalog but cannot be connected any more. The Unified Comfort Panel must be onboarded again as a new Edge Device. The previous device needs to be manually removed from the IEM.

In this case, we recommend to proceed as follows:

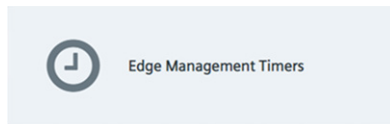
1. Perform a "Hard Reset" for the device.
2. Update the operating system of the device.
3. Initialize "Backend Managed" Edge on the device.

6.3 Additional Settings

This section describes additional IEM-related functions available under "Settings (Page 31)" in the navigation menu of your Edge Device when using Central Edge Management via IEM.

6.3.1 Configuration

The following additional tile is available in the "Configuration" tab when using Central Edge Management via IEM.



Edge Management Timers

Edge Management Timers ✕

Check Edge Management Notifications

Every

Publish IEM OS Analytics

Every

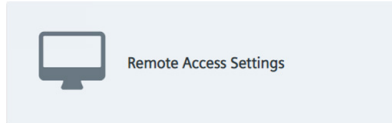
Update

In this screen, you set the time period for the following parameters:

- "Check Edge Management Notifications": Time interval for retrieving jobs from the IEM.
 - Value range: 10 seconds to 30 minutes
 - Default value: 1 minute
- "Publish IEM OS Analytics": Time interval of sending Edge Device statistics to the IEM.
 - Value range: 10 seconds to 60 minutes
 - Default value: 60 minutes.

6.3.2 System

The following additional tile is available in the "System" tab when using Central Edge Management via IEM.



Remote Access Settings

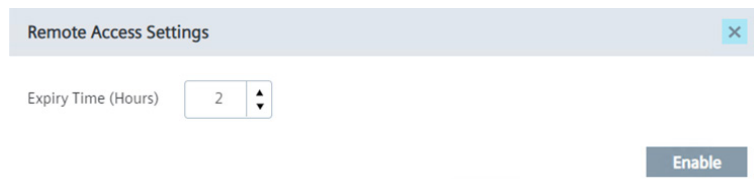
Use this tile to enable or disable remote access to your Edge Device if direct access from the control network is not possible. This function can be used for remote debugging, for example.

Requirement

A relay server has been added.

You find information on how to add a relay server in the "Adding a relay server" subsection in the following manual: Industrial Edge Management - Getting Started (<https://support.industry.siemens.com/cs/ww/en/view/109804065>)

Enabling or disabling remote access



Set the remote access timeframe for the Edge Device in the "Expiry Time" input field and click "Enable".

- Value range: 2 to 10 hours
- Default value: 2 hours

Once remote access has been enabled, the "Enable" button changes to "Disable".

Local Edge Management

7.1 Overview

The following local Edge management functions are available with "Standalone" Edge Management on a Unified Comfort Panel Edge Device:

- Installing apps.
- Managing apps.
- Displaying the status of hardware, installed and running apps and their memory consumption.
- Managing configuration, connectivity and system settings.

All Edge Management activities are performed via the Edge Device user interface.

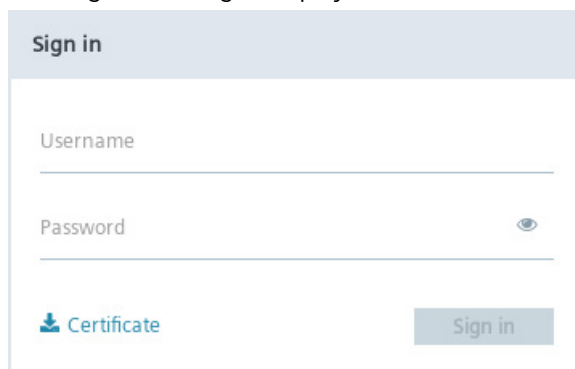
Requirement

- Edge management is enabled in the Control Panel of the Edge Device under "Apps" > "SIMATIC Edge" > "Enable SIMATIC Edge".
- The Edge Management type is set to "Standalone", refer to chapter "Initializing Edge Management (Page 15)".

Launching Edge Management

Proceed as follows to open the Edge management on a Unified Comfort Panel:

1. Open the Control Panel and click "Apps" > "SIMATIC Edge" > "Open edge management".
The local Edge Management web page is displayed in the Web Browser.
2. Log in using the "Sign in" link in the upper right corner of the Edge Management web page.
The "Sign in" dialog is displayed.



Sign in

Username

Password

[Certificate](#)

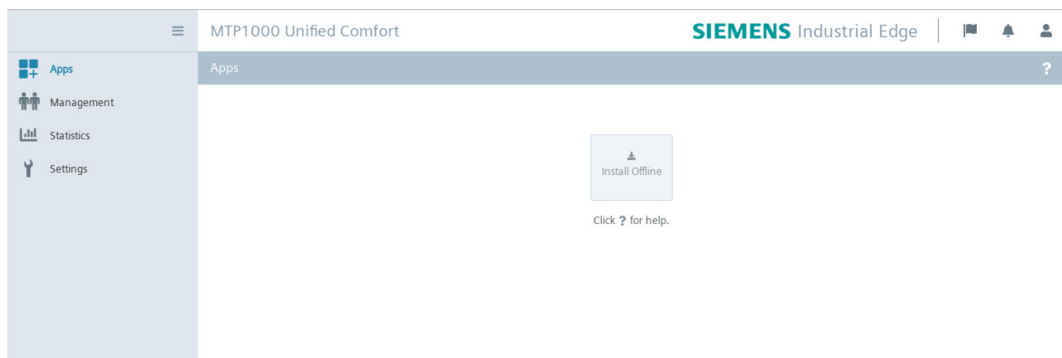
3. Specify the credentials of a user who has been assigned the "Control Panel access" function right in the configuration. For more information, refer to the Operating Instructions.

4. If required, click "Certificate" to specify a certificate for secure communication.
5. Click "Sign in".

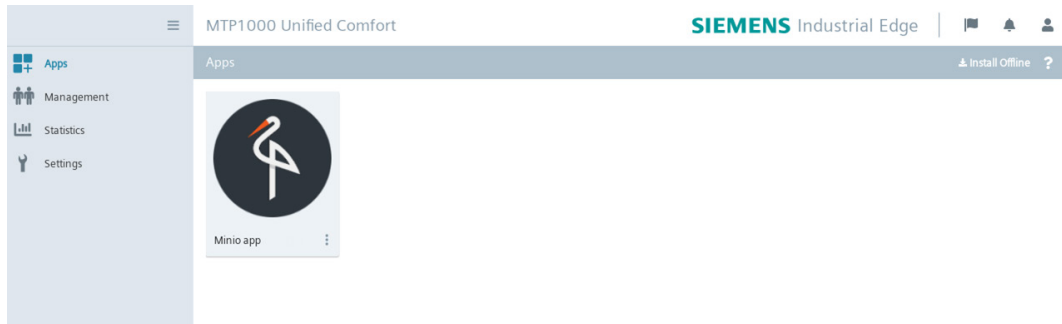
The Edge Device user interface

After successful login, the "Apps" screen of the Edge Device user interface is displayed. The layout of the "Apps" screen varies depending on whether or not apps have already been installed.




If there are no apps installed yet, the "Apps" screen is displayed as follows:



Once an app was installed, the "Install Offline" button is displayed on the right of the title bar of the "Apps" screen. The following screen shows an example.



The following functions are available in the upper right header area of the Edge Management screen, independent of the entry selected in the navigation menu.

	"Tasks" icon to display the status of ongoing or finished tasks such as the installation of an app.
	"Events" icon to display the "Recent events" window. The "Recent events" window contains alerts and notifications of the following types: <ul style="list-style-type: none"> • Available app update notifications • CPU utilization alerts • Memory utilization alerts • Storage utilization alerts
	"User" icon to display the name of the current user or to log out.

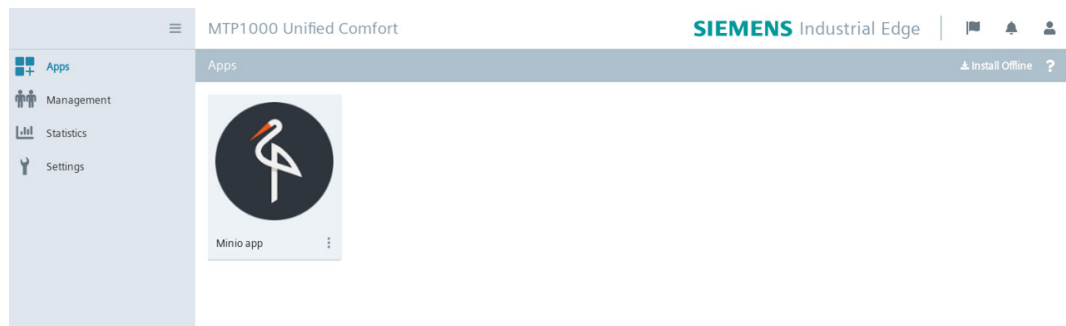
The following entries are available in the navigation menu on the left of all screens:

- "Apps" (Page 25) to install, open, uninstall or display information on apps.
- "Management" (Page 29) to uninstall, restart, stop or display detailed information on apps.
- "Statistics" (Page 30) to display performance-related information of hardware and apps.
- "Settings" (Page 31) to view information and adjust configuration, connectivity and system parameters.

7.2 Apps

The "Apps" screen provides an overview of installed apps and the following functions:

- Launching an app.
- Displaying app information.
- Uninstalling an app.
- Installing an app.



Launching an app

To launch an app, click the tile of the app. The app user interface opens in a new Web Browser tab.

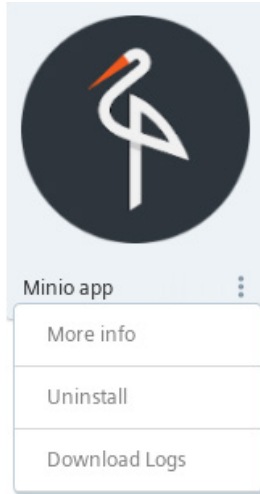
Note

User interface of the app

The user interface is only opened for apps that support a web-based user interface.

Displaying app information


1. Click "..." in the lower right corner of the app tile to open the app context menu.



2. Select "More Info" from the app context menu to display the "Apps Details" window. The information and the functions in the "Apps Details" window are identical with the information and functions for an app in the "Management" screen, refer to the "Management" section (Page 29).

Uninstalling an app

1. Select "Uninstall" from the app context menu.
2. Click "Uninstall" in the confirmation dialog.

The app will be uninstalled. Uninstall status information can be accessed through the "Tasks" icon ().

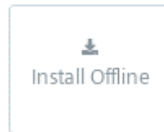
Saving app logs

Selecting "Download Logs" from the app context menu will save a log file containing available connection and communication history for the app. The "Download Logs" function is available if logging was activated under "Settings" > "System" > "Log" > "Settings" via the "Enable logs" option, refer to chapter "Configuration (Page 31)".

Installing an app

The following procedure applies to "Standalone" Edge Management only and describes how to install an app that was created with Industrial Edge Publisher and stored on an external storage medium or on a network drive that can be accessed by the Edge Device. For more information about Industrial Edge App Publisher, please refer to the operating manual on the internet (<https://support.industry.siemens.com/cs/ww/en/view/109804060>).

1. If there is no app installed yet, click "Install Offline" in the "Apps" main window.



If apps are already installed, make sure that the maximum number of apps and the maximum allocation memory value will not be exceeded by the app you want to install, refer to chapter "Statistics (Page 30)". After that, click "Install Offline" from the title bar.



The "Install Offline" dialog is displayed.

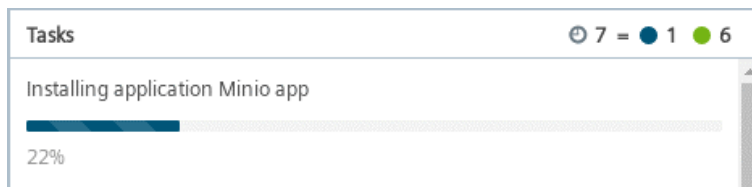
 A screenshot of the "Install Offline" dialog box. The title bar says "Install Offline" with a close button (X). Below the title bar are two tabs: "1 App Details" (selected) and "2 Configurations". Under the "App Details" tab, there are three sections:

- Storage Media**: A radio button is selected. To its right is a "Browse" button.
- Signature (Optional)**: An input field labeled "Signature File" with a "Browse" button to its right.
- Public Key (Optional)**: An input field labeled "Public Key File" with a "Browse" button to its right.

 At the bottom right of the dialog is a "Next" button.

2. Select the "Storage Media" option to install the app from a storage medium or the "Browse" option to install the app from a network drive. Click the "Browse" button to select the .app file from the specified location.
3. If necessary, browse the signature of the app that you generated during the export of the app file in the "Signature (Optional)" section.
4. If necessary, enter the public key in the "Public Key (Optional)" input field. Both signature file and public key verify the app file integrity.

5. Click "Install" to start the installation process.
6. Click the "Tasks" icon in the header area to display the installation progress.



After successful installation, the app will be displayed in the "Apps" main window.

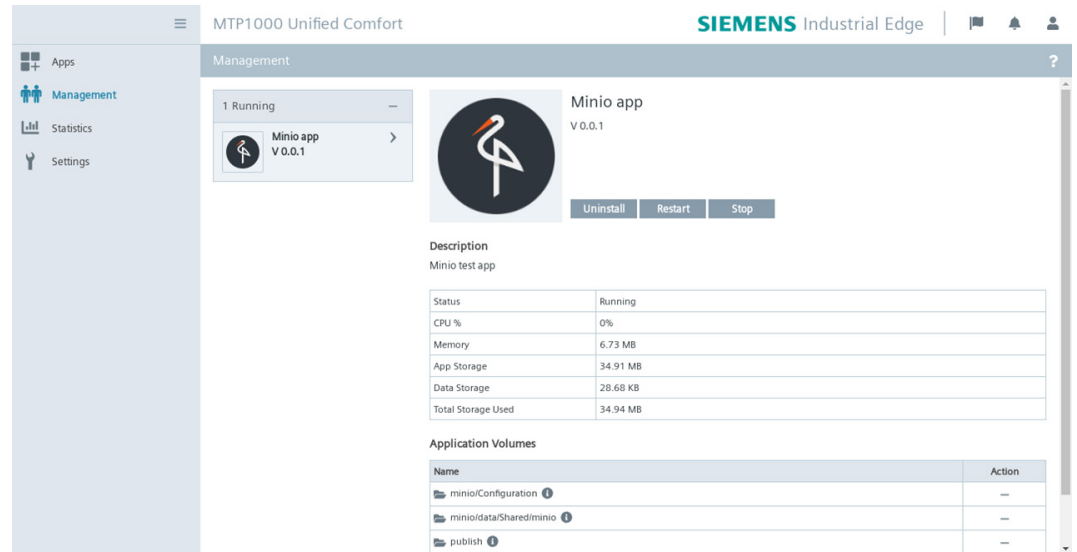


7.3 Management

Managing an app

1. Click "Management" in the navigation menu.




The management window is displayed.



2. Click the app you want to manage.
3. Depending on whether or not the app was started, the following buttons are available:
 - "Start": Run the app.
 - "Stop": Stop the app.
 - "Restart": Restart the app.
 - "Uninstall": Uninstall the app from the Edge Device.

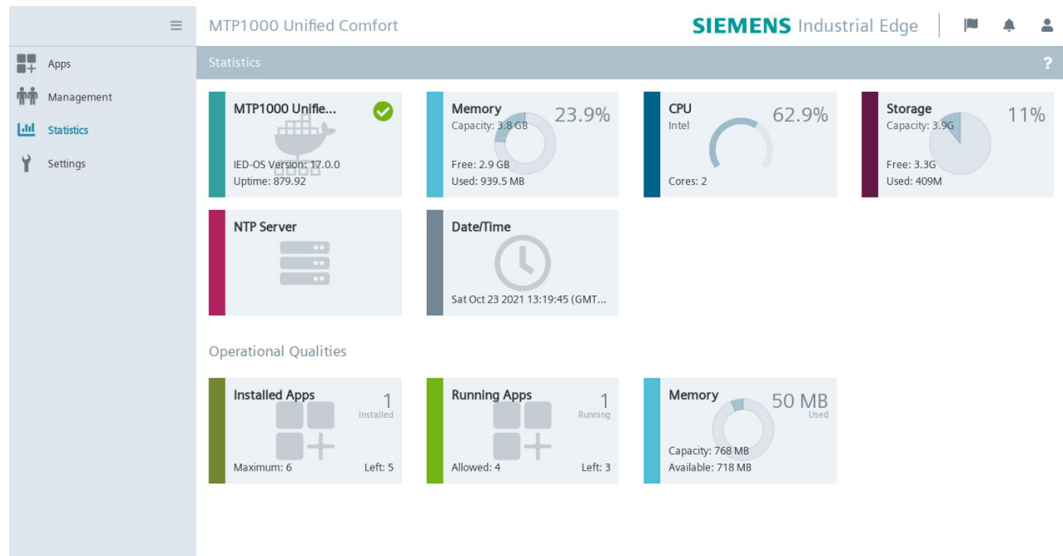
Modifying app volumes

Depending on whether or not a file was already uploaded to an app volume, the following functions are available under "Application Volumes":

	Upload a file from an app volume.
	Download a file to an app volume.
	Remove a file from an app volume.

7.4 Statistics

The "Statistics" screen provides hardware- and app-related performance information.



Statistics

The following information is displayed in the "Statistics" section:

- "MTP1000 Unified Comfort" (example): Name, Edge core version and activity time of the Edge Device.
- "Memory": Current application data memory "live" status of the Edge Device.
- "CPU": Current CPU load on the Edge Device.
- "Storage": Current RAM memory status of the Edge Device.
- "NTP Server": Currently not used, reserved for future extension.
- "Date/Time": Current date and time of the HMI device.

Operational Qualities

The following information is displayed in the "Operational Qualities" section:

- "Installed Apps": Number of installed apps and the maximum number of apps allowed to be installed on the Edge Device.
- "Running Apps": Number of currently running apps.
- "Memory": Total amount of memory allocated by all apps installed on the Edge Device. The allocated memory for an app is defined in the Industrial Edge Publisher under "Memory Limit" on the "System" page of the app service settings. The maximum value of memory that can be allocated by all apps installed on the Edge Device is 768 MB.

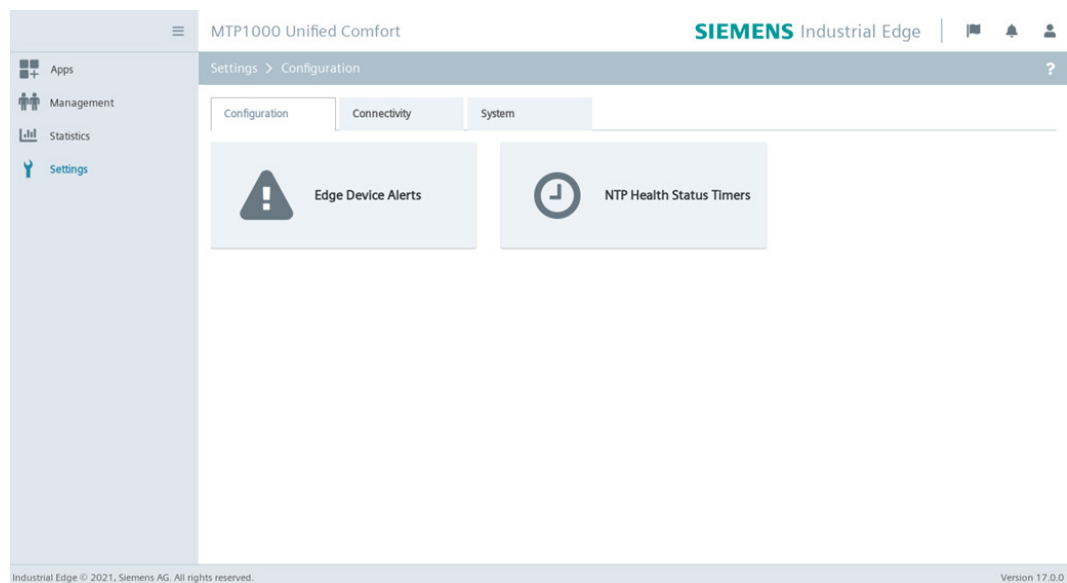
The system will refuse to install an app in the following cases:

- The maximum number of apps is reached.
- The maximum memory allocation value for all apps will be exceeded by installing the app.

7.5 Settings

7.5.1 Configuration

In the "Configuration" tab, you specify the properties for Edge Device alerts and NTP health status timers.



Edge Device Alerts

Clicking the "Edge Device Alerts" tile will display the following dialog.

The dialog box is titled 'Edge Device Alerts' and has a close button (X) in the top right corner. It contains three input fields for configuring utilization thresholds. The first field is for 'CPU (%)' with a value of '80' and a range of 'Min. 10, Max. 80'. The second field is for 'Memory (%)' with a value of '80' and a range of 'Min. 10, Max. 80'. The third field is for 'Storage (%)' with a value of '70' and a range of 'Min. 10, Max. 70'. An 'Update' button is located at the bottom right of the dialog.

In this screen, you configure alert thresholds. You configure the following utilization thresholds:

- CPU
- Memory
- Storage

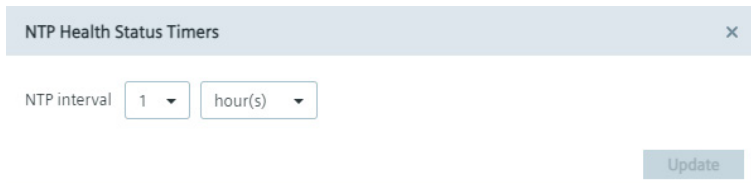
Whenever one of these resources exceeds its utilization threshold, a warning icon is displayed in the header of the Edge Management user interface its message is displayed via tooltip.



In that case, either expand the utilization threshold or decrease the utilization itself. To save the changes, click "Update".

NTP Health Status Timers

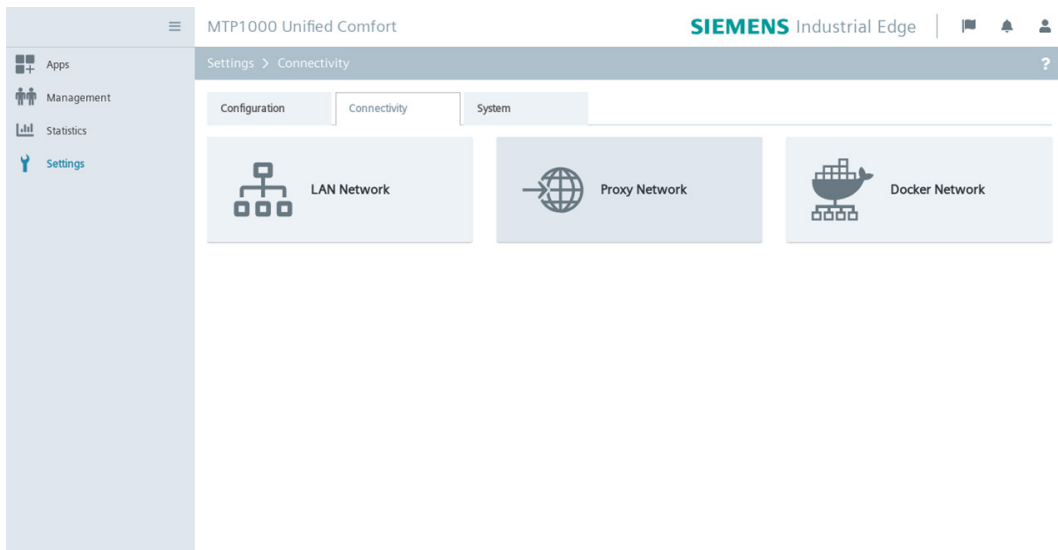
Clicking the "NTP Health Status Timers" tile will display the following dialog.



In this screen you set the monitoring interval for the NTP server status check. By default, the interval is set to 1 hour. Maximum interval is 1 day and minimum interval is 1 minute. To save the changes, click "Update".

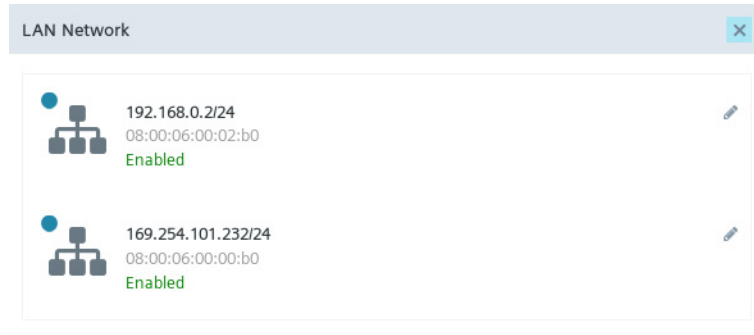
7.5.2 Connectivity

In the "Connectivity" tab, you specify the properties for LAN network, proxy network and Docker network.



LAN Network

Click the "LAN Network" tile to check the network properties of your Edge Device.



Changing network settings

1. Click the edit icon to configure the LAN network settings for one of the interfaces.



The "Edit Network Interface" screen" is displayed.

The screenshot shows a window titled "Edit Network Interface" with a close button. It contains several sections:

- DHCP:** A checkbox labeled "DHCP" is checked.
- Static:** A section with three rows of input fields for "IPv4", "Netmask", and "Gateway".
- DNS (Optional):** A section with "Primary DNS" and "Secondary DNS" (four input fields).
- Layer 2 (L2) for Apps (Optional):** A section with "Start IP Address" (four input fields: 192, 168, 80, 24), "Netmask" (four input fields: 255, 255, 255, 0), and "IP Address Range" (a dropdown menu showing 8). There is an "Advanced Settings" button.

Below the L2 section, there is a warning: "Removing the L2 network will stop the functioning of apps that use it." and another warning: "Changing the network configuration will invalidate the current browser tab." At the bottom right, there is an "Update" button.

2. Configure the IP address, either automatically through a DHCP server or through static information, and the DNS server as required.

3. Edit the configured Layer 2 network access or set up a Layer 2 network access on this Edge Device in the "Layer 2 (L2) for Apps" section, as shown in the following example.



Note

Removing Layer 2 network access

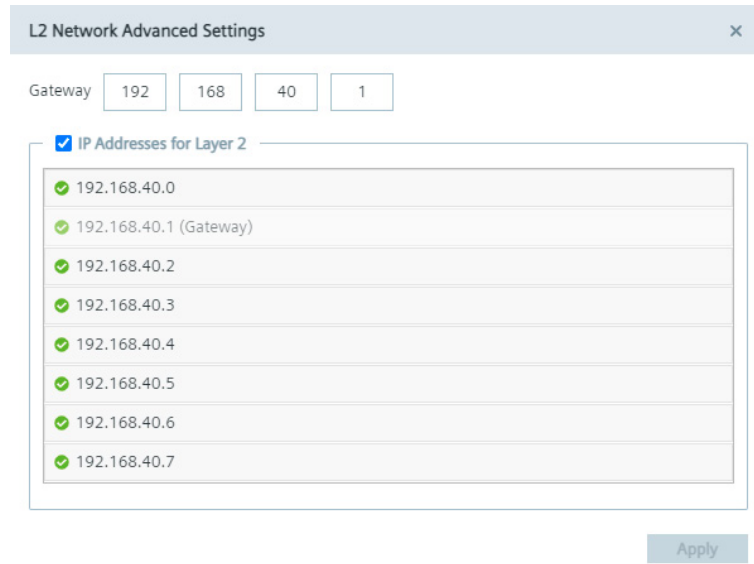
Apps using Layer 2 network access on this Edge Device will not work anymore if you remove Layer 2 network access.

You will find more information on Layer 2 network access in the following manual on the internet:

Industrial Edge Management - Getting Started
<https://support.industry.siemens.com/cs/ww/en/view/109804065>).

4. When you click "Advanced Settings", you can specify which IP addresses can be used for the Layer 2 network access for apps in the defined IP range.

After clicking "Advanced Settings", a list with several IP addresses, depending on the starting IP address and the IP range of the Layer 2 network access, are displayed, as shown in below example.



When checking an IP address, the IP address can be used for Layer 2 network access by apps. When unchecking an IP address, the IP address is blocked and will not be used. By default, the gateway is within the entered IP range. Under "Gateway", you can define an IP address for the gateway to obtain one more available IP address in the given IP range, but the IP address of the gateway must be located in the specified subnet.

L2 Network Advanced Settings

Gateway: 192 168 40 20

IP Addresses for Layer 2

- 192.168.40.0
- 192.168.40.1
- 192.168.40.2
- 192.168.40.3
- 192.168.40.4
- 192.168.40.5
- 192.168.40.6
- 192.168.40.7

Apply

5. Click "Apply" to save the Layer 2 network access changes.
6. Click "Update" to save all changes.

Proxy Network

Click the "Proxy Network" tile to open the proxy server settings.

Proxy Network

Use a proxy server

1 Proxy 2 No Proxy 3 Custom Port

IP : Port

UserName : Password

Next

Activating proxy network settings

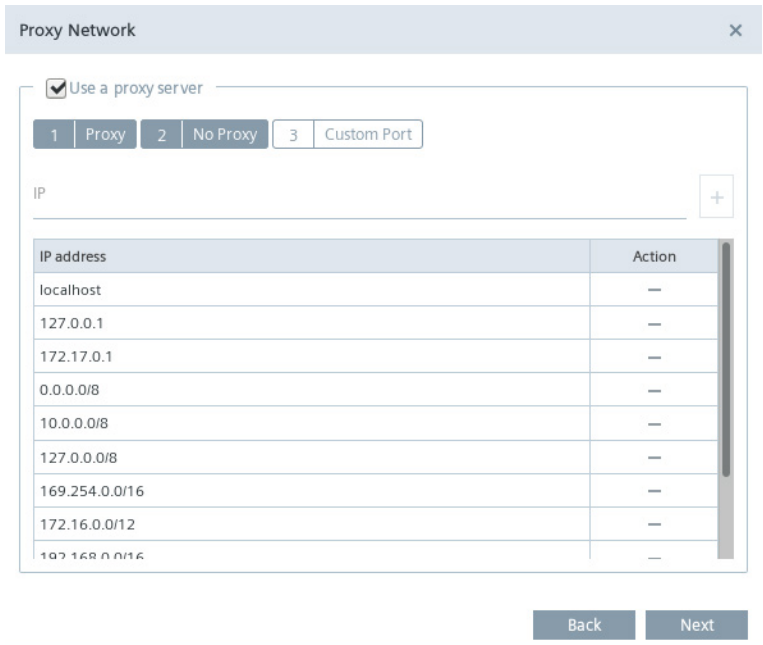
1. Check "Use a proxy server".
2. Enter IP address and port of your proxy server in the corresponding input fields.
3. Enter user name and password if the proxy server requires additional authentication.

When authentication is required, the password must match the following criteria:

- The password must start with an alphabetic character
- The password must not contain complex characters, such as \ . * "
- The password must not be longer than 21 characters

The settings apply for HTTP and HTTPS proxy servers.

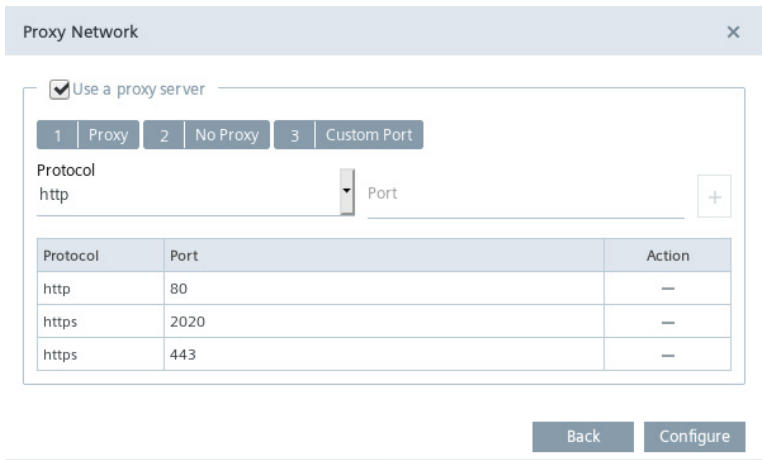
- 4. Click "Next" to open the "No Proxy" tab.



You can enter all IP addresses that shall be directly accessed without proxy.

Several "no proxy" addresses required by IEM are listed by default.

- 5. You can specify an additional IP address that shall be directly accessed by entering the IP address or its domain in the "IP" input field and clicking the "+" icon.
- 6. Click "Next" to open the "Custom Port" tab.



In the "Custom Port" tab, you configure ports for apps that use the configured ports for outgoing communication through the proxy on HTTPS or HTTP protocols. For your apps, use ports in the range of 32768...60999.

Several ports required by the IEM are listed by default.

Note

The default no proxy addresses and ports are reserved by the IEM and cannot be deleted.

7. To add additional ports, select the required protocol from the "Protocol" drop-down list, enter the corresponding port number and click the "+" icon.
8. Click "Configure" to save the proxy settings.

Docker Network

Click the "Docker Network" tile to change the default Docker network settings.

Docker Network

IP address: 172, 17, 0, 0

Netmask: 255, 255, 0, 0

Configure

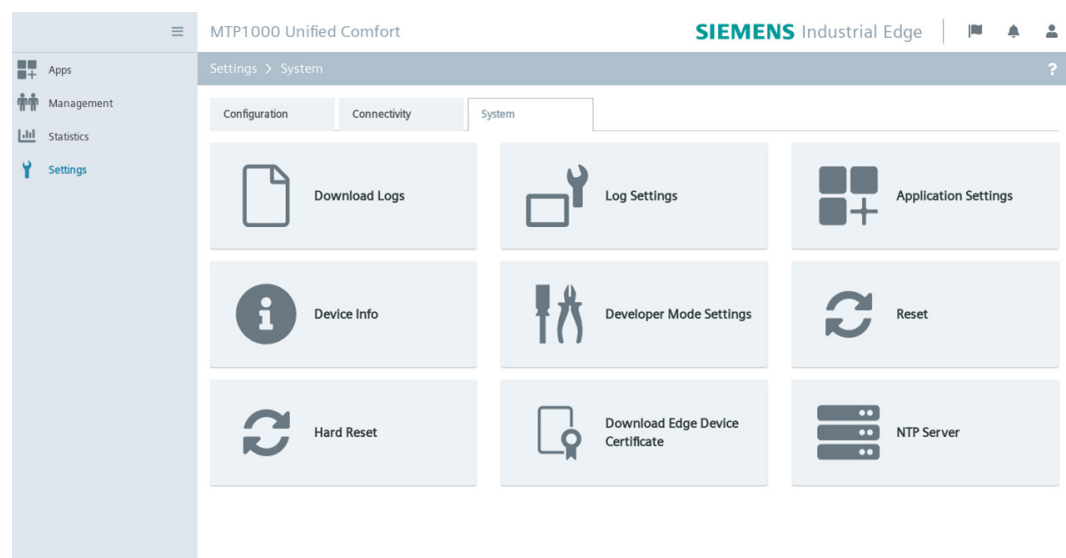
By default, the Edge Device contains two Docker networks, one for the proxy-redirect and one for the "docker0 interface" (that you create via the "IP address" input field). When you install an app that creates a new Docker network on the Edge Device, the Docker network of the installed app must not overlap the Docker networks of the Edge Device and needs free Docker network IP ranges on the Edge Device.

The "docker0 interface" IP range starts at IP address 172.17.0.0 by default. Using a different "docker0 interface" is optional. If required, select a different IP address for the "docker0 interface" you want to use for the Edge Device in the "IP address" input field.

The "Netmask" entry is not configurable.

7.5.3 System

In the "System" tab, you perform administration and maintenance tasks for your Edge Device.



The followings functions are available through the tiles under the "System" tab.

Download Logs

Download the system logs for both administrative and debugging tasks as a ".tar.gz" file via the "Web Browser" app.

Log Settings

Use this tile to enable or disable the logging possibility for apps.

Log Settings
✕

Enable Logs
Allow Edge Apps to log into the Internal Memory.
To prolong the service life of your device, Enabling of logs is not recommended.

Update

Check "Enable Logs" to allow Edge apps to log into the internal memory. Default value: enabled.

Application Settings

Use this tile to display the maximum count and memory that can be used by apps.

Application Operational Qualities
✕

Max Installed Apps Count	6
Max Running Apps Count	4
Max CPU Load	—
Max Usable RAM Usage	768 MB
Max Usable Storage Area	512 MB

- Maximum number of apps that can be installed.
- Maximum number of apps that can run in parallel.
- Maximum CPU load
- Maximum RAM usable by apps
- Maximum usable storage area

Device Info

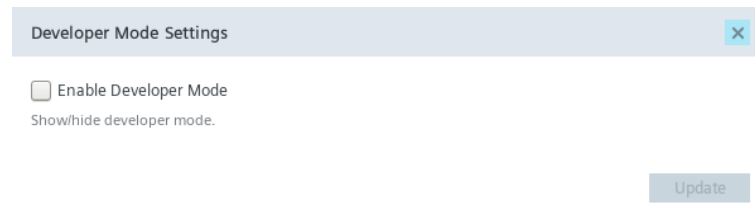
Use this tile to display hardware and firmware-related information of the Edge Device.

Device Info
✕

Device Type	MTP1500 Unified Comfort
MLFB	6AV2128-3QB06-0AX0
Serial Number	V-00000015
Image Version	V17.00.00.02_03.01.00.23

Developer Mode Settings

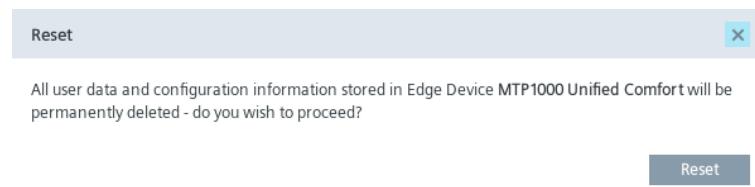
Use this tile to enable or disable the developer mode.



The developer mode allows access to debugging, diagnostics and app modification tools, refer to section "Developer mode (Page 40)".

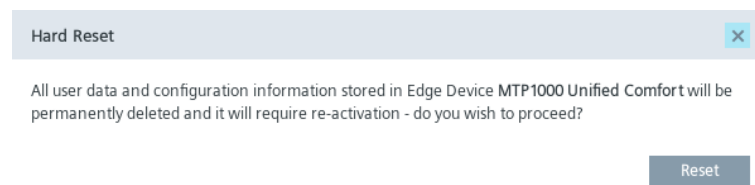
Reset

Use this tile to delete all Edge-related user data and configuration information stored in the device.



Hard Reset

Use this tile to delete all Edge-related user data, configuration and Edge initialization information stored in the device.



After a "Hard Reset", the Edge Device performs a reboot and Edge Management has to be re-initialized. After the reboot, the "Activate Edge Device" dialog is displayed.

Follow the instructions in chapter "Initializing Edge Management (Page 15)".

Download Edge Device Certificate

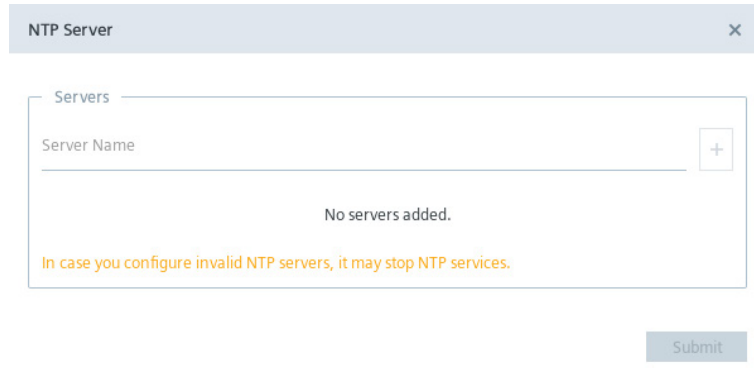
Download the Edge Device Certificate to facilitate a secure "https" connection for Edge Management via the "Web Browser" app.

NTP Server

Use this tile to add or delete NTP Servers for your Edge Device.

A maximum of four NTP servers can be specified.

The NTP server list already contains NTP servers if they were specified in the Control Panel under "Language, Region and Formats" > "Date and Time".



To add an NTP server, specify its IP address under "Server Name" and click the "+" icon.

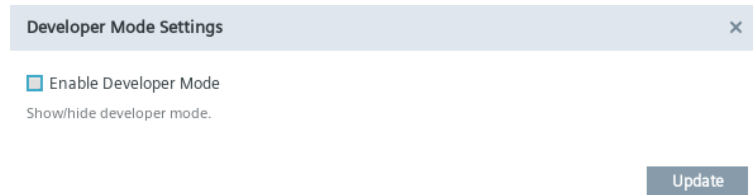
7.5.4 Developer mode

This section describes the procedure for accessing the developer mode providing detailed information on the installed apps.

Procedure

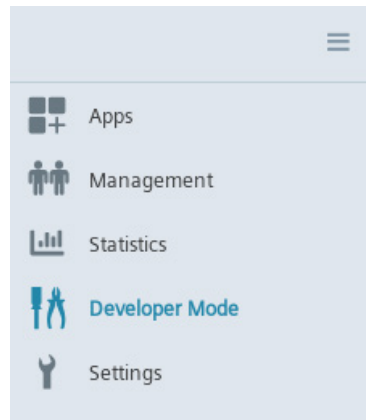
1. Select "Settings" and click the "System" tab.
2. Click the "Developer Mode Settings" tile.

The "Developer View Settings" window is displayed.



3. Check the "Enable Developer Mode" check box.
4. Click "Update".

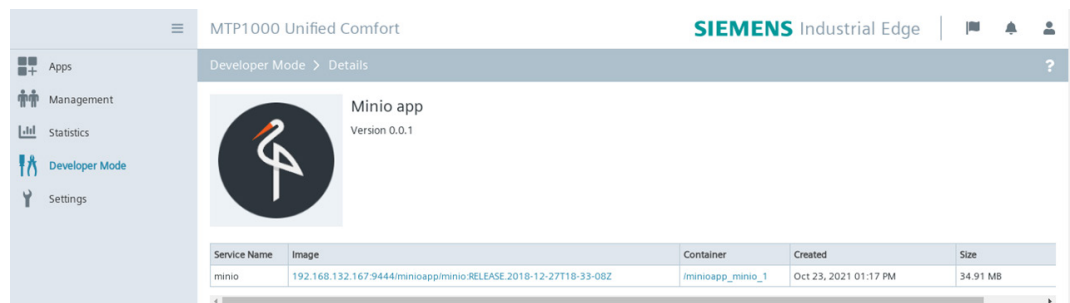
The "Developer Mode" entry is displayed in the navigation menu.



5. Click "Developer Mode".

When there are apps installed that correspond to a project for which the Edge Device owner has ownership (or has a membership within a user group and appropriate permissions), the corresponding apps are displayed as tiles.

6. Click an app tile to display the developer view and the app details.



The developer view details screen displays a list of services, images and containers. Clicking an image name displays information about the image including various parameters that you specified when you used Industrial Edge Publisher to package the individual service as part of the app.

Clicking the container name, if containers are available, will display information about the container. The "Stats" tab lists information about the resource usage and other statistical information. The "File system changes" tab provides information about changes to the file system.

Application examples

Central Edge Management

You will find application examples for Central Edge Management on the Internet (<https://support.industry.siemens.com/cs/ww/en/ps/26128/ae>).

Local Edge Management

You will find an application example illustrating the entire process of creating Docker images, generating apps with Industrial Edge Publisher and managing apps on Unified Comfort Panels on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109778780>).