SIEMENS

SIMATIC IPC Industrial Edge Device - Release Notes V1.3

Readme

09/2021

A5E51396292-AA

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.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E51396292-AA
Ⓟ 09/2021 Subject to change

Table of contents

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?).

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/109799476)" manual.

General notes 2

Notes for installation and use

The information in this document takes precedence over statements made in other documents.

Please read the notes carefully because they contain important information for the installation and operation of the software.

Industrial Edge Management - Download

You find the download file of the Industrial Edge Management in the Industrial Edge Hub.

Industrial Edge Management - Installation

You find installation instructions for Industrial Edge Management in the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109799508)" manual.

Industrial Edge Management - Operation

You find operation instructions for Industrial Edge Management in the "Industrial Edge Management - Operation (https://support.industry.siemens.com/cs/us/en/view/109799510)" manual.

Industrial Edge - Security overview

You find an overall security overview of Industrial Edge in the "Industrial Edge - Security overview (https://support.industry.siemens.com/cs/us/en/view/109799476)" manual.

Industrial Edge App Publisher - Operation

You find operation instructions for the Industrial Edge App Publisher in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109795386)" manual.

Industrial Edge Device - Operation

You find operation instructions for Industrial Edge Devices in the "Industrial Edge Device - Operation (https://support.industry.siemens.com/cs/us/en/view/109799507)" manual.

Industrial Edge - Update Procedures

You find update instructions regarding Industrial Edge and its components in the "Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/109795343)" manual.

Support of Edge Apps and Industrial Edge Management components

Industrial Edge only supports apps that were developed by Siemens or customers.

Supported Edge Devices

3

The supported Edge Devices inclusive their Non-functional requirements (NFRs) are:

NFRs	**SIMATIC IPC227E** **Celeron N2930** **8 GB RAM** **240 GB SSD**
Max. count installed apps	20
Max. count running apps	8
System reserved RAM	2048 MB
Max. usable RAM	6144 MB
MLFB	6ES7647-8BD31-0CW1

NFRs	**SIMATIC IPC427E** **Core i5 – 6442EQ** **16 GB RAM** **240 GB SSD**
Max. count installed apps	80
Max. count running apps	24
System reserved RAM	2048 MB
Max. usable RAM	14336 MB
MLFB	6AG4141-5BC30-0FW8

Further Edge Devices will be added during upcoming releases.

What is new in IED-OS V1.3

4

The following features are inside Industrial Edge Device OS (IED-OS) V1.3:

- Supporting SIMATIC IPC427E as Edge Device
- Displaying the network interface name in the network settings
- Displaying date and time in local time and local time zone in the NTP tile in the statistics section of the Edge Device UI
- Several UI improvements
- Improvements for more robust hard reset operation

Fixed bugs

The following bugs have been fixed with IED-OS V1.3:

- Fixed a bug where a confusing error message was displayed when deploying an app which has no reverse proxy forwarding rule but which exposes minimum 1 port on the IED
- Fixed a bug where the edge-core version was displayed in the statistics section instead of the IED-OS version
- Fixed a bug

5 Scope of delivery

IED-OS V1.3 includes the following components:

Component	Version	Description
Mentor Industrial OS	2.3.1.1	
Edge-core-lite	1.2.1-4	
UI	1.2.0-8	
Edge-manager	1.2.0-9	
Edge-storage-manager	1.2.1-1	
dm-led	1.2.1	
dm-network	1.2.1	
dm-ntp	1.2.1	
dm-onboard	1.2.1	
dm-system	1.2.1	
usbdaemon	1.2.0	

Notes on use 6

The following restrictions apply with the delivery of IED-OS V1.3.

Updates of Edge Devices

Once a new Industrial Edge Device OS is published, in this case IED-OS V1.3, the admin of the Industrial Edge Management can synchronize and load the new version to the Industrial Edge Management. Then, the Industrial Edge Device OS can be updated manually for each connected Edge Device in the Industrial Edge Management.

You find the procedure and additional information on how to update Edge Devices in the "Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/109795343)" manual.

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 PC, on which the Industrial Edge Management is running, with 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 to which the Industrial Edge Management and Edge Devices must be able to connect to.

IPv4 DNS server address

The IEM-OS and IED-OS are only configurable with IPv4 addresses. Thus, properly working and valid IPv4 DNS server addresses, to set up the IEM-OS and IED-OS, are required. It might happen that on customer's network configurations a DHCP server provides an IPv6 address for an IPv4 network. In that case, the DNS name resolution does not work anymore.

Ensure that the DNS server always provides an IPv4 address for a properly DNS name resolution.

Client access to IEM

The Industrial Edge Management cannot be called through the Internet. Clients that want to access the Industrial Edge Management or Edge Devices must be located in the plant network.

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.

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.

Hard reset and reboot of SIMATIC IPC227E

When you perform a hard reset or a reboot of the SIMATIC IPC227E, it may happen that the event fails and an error occurs on the SIMATIC IPC227E with 3 LEDs lighting up red on it.

In that case, you must open the BIOS menu of the SIMATIC IPC227E and set the "xHCI Mode" to "disabled" in the "SCU > Advanced > USB configuration" BIOS settings. After you updated the BIOS settings, you can again perform a hard reset or a reboot of the SIMATIC IPC227E.

Note

Opening the BIOS menu

You open the BIOS menu by pressing and holding <Esc> after you switch on the SIMATIC IPC227E.

Connecting an Edge Device with IED-OS version 1.0.0

When you connect an Edge Device with IED-OS version 1.0.0 through an USB flash drive to the IEM, ensure, before you save the Edge Device configuration file on the USB flash drive, that the USB flash drive is formatted to a NTFS format and inserted into the USB 3.0 port of the Edge Device. USB flash drives with exFAT formatting are not supported.

Supported keyboard layout

When you provide the needed information in input fields, the IED-OS only support characters from an English keyboard layout. For example when you add a topic and enter the topic name in the IE Cloud Connector Configurator. Special characters like "ö", "ä" or "ü" are not supported and result in error messages.

UEFI Secure Boot

UEFI Secure Boot is supported by the released Industrial Edge Device OS versions.

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.

Running the IEM and IE Devices with self-signed certificates

If you are running the IEM and Industrial Edge Devices with self-signed certificates, consider the information from this FAQ (https://support.industry.siemens.com/cs/ww/en/view/109795516).

Known issues 7

The following are the known issues:

Issue	Troubleshooting
Connecting an Edge Device to the IEM fails and the "Nginx configuration test failed" error message is displayed during activating the Edge Device phase.	Check the DNS server configuration since the error message is DNS server related. The DNS server must be configured properly and reachable for the IEM.
In case user data of edge device is corrupted due to unexpected power-outage or forcibly shutdown of edge device. IED-OS filesystem recovery process is going to take place. The process might take 2-3 hours depending on hardware specification of the running device.	-