SIEMENS

Industrial Edge Management - Getting Started

Getting Started

Preface

Industrial security 1

Overview of Industrial Edge 2

Industrial Edge Hub 3

Setting up the IEM 4

Installing system apps 5

Working with the IEM 6

Example of use - Monitoring bottle filling process 7

List of abbreviations/ acronyms 8

V1.2.0
A5E50177870-AC

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

A5E50177870-AC
Ⓟ 04/2021 Subject to change

Copyright © Siemens AG 2021.
All rights reserved

Preface

This documentation contains all the information you need to get started with Industrial Edge (IE) and is intended for operators who commission the Industrial Edge Management (IEM).

The complete operating manual for operators who, for example, commission and operate Edge Devices, as well as service and maintenance technicians who perform error analysis, is included in the "Industrial Edge Management - Operation (https://support.industry.siemens.com/cs/us/en/view/109780393)" manual.

The documentation for programmers who develop respectively package their own Edge Apps and load these Edge Apps to the IEM through the Industrial Edge App Publisher is included in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

New features, known issues and notes on use regarding new published versions of the Industrial Edge Management are included in the "Industrial Edge - Release notes (https://support.industry.siemens.com/cs/us/en/view/109780394)" manual.

An overview with regard to security and requirements for Industrial Edge and its components are included in the "Industrial Edge - Security overview and requirements (https://support.industry.siemens.com/cs/us/en/view/109781002)" manual.

Information regarding Edge Devices and their operations are included in the "Industrial Edge Devices - Operation (https://support.industry.siemens.com/cs/us/en/view/109783785)" manual.

Purpose of this document

The objectives of this documentation include the following:

- You are provided with a functional overview of Industrial Edge.
- You find all the information on how to set up the Industrial Edge Management (IEM) On-Premises.
- You learn how to connect an Edge Device to your IEM and install Edge Apps onto Edge Devices.

Basic knowledge required

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

Scope of this document

This Getting Started is valid for Industrial Edge.

Convention

The term "Edge Device" is used in this documentation to designate hardware with a configured Industrial Edge Device OS.

Instead of the product designation "Industrial Edge Apps", the short forms "Edge Apps" and "Apps" are also used.

Instead of the product designation "Industrial Edge System Apps", the short form "System Apps" is also used.

Instead of the product designation "Industrial Edge Device", the short form "Edge Device" is also used.

Instead of the product designations "Industrial Edge Databus" and "Industrial Edge Databus Configurator", the short forms "Databus" and "Databus Configurator" are also used respectively.

Instead of the product designations "Industrial Edge Cloud Connector" and "Industrial Edge Cloud Connector Configurator", the short forms "Cloud Connector" and "Cloud Connector Configurator" are also used respectively.

Figures

Picture components are marked with black position numbers on a white background: ①, ②, ③, etc.

Table of contents

Preface ... **3**

1 Industrial security ... **7**

2 Overview of Industrial Edge ... **9**

3 Industrial Edge Hub ... **13**

3.1 Sign up ... 13

3.2 Log in ... 16

3.3 Home ... 17

3.4 Market ... 19
3.4.1 Purchasing an Edge App license ... 19

3.5 Library ... 20
3.5.1 Copying the app to the IEM catalog ... 20
3.5.2 Opening app documentation ... 21

3.6 Licenses ... 21

3.7 IEM Instances ... 22
3.7.1 Managing IEM instances ... 23

3.8 Download Software ... 24

3.9 Documents ... 24

3.10 User Management ... 25
3.10.1 Overview ... 25
3.10.2 Inviting a new user ... 26

3.11 Cancelling an IE Hub subscription ... 26

4 Setting up the IEM ... **29**

4.1 Setup steps ... 29

4.2 Downloading the Industrial Edge Management OS ... 30

4.3 Creating an IEM instance and downloading the configuration file ... 31

4.4 VMware Workstation ... 32
4.4.1 Creating the VM ... 32
4.4.2 Configuring the VM ... 37
4.4.3 Installing the Industrial Edge Management OS ... 45

4.5 Oracle VirtualBox ... 46
4.5.1 Creating the VM ... 46
4.5.2 Configuring the VM ... 50
4.5.3 Installing the Industrial Edge Management OS ... 59

4.6 Configuring the Industrial Edge Management OS ... 63

4.7 Activating & Installing the Industrial Edge Management ... 67

4.7.1 Activating the Industrial Edge Management ... 67
4.7.2 Settings ... 73
4.7.2.1 Editing network settings ... 74
4.7.2.2 Setting up a proxy server ... 75
4.7.2.3 Configuring the Docker network ... 79
4.7.2.4 Downloading logs ... 80
4.7.2.5 Adding an NTP server ... 80
4.7.3 Installing the Industrial Edge Management ... 82
4.8 Installing system configurators ... 86
4.9 Adding a relay server ... 88
5 Installing system apps ... 93
5.1 Copying system apps to the IEM ... 93
5.2 Connecting an Edge Device ... 94
5.2.1 Layer 2 network access ... 95
5.2.2 Creating the Edge Device configuration file ... 95
5.2.3 New Edge Device - Parameters ... 101
5.2.4 Connecting the Edge Device through an USB flash drive ... 104
5.2.5 Example logs ... 105
5.2.6 Connecting the Edge Device through a browser ... 106
5.2.7 Settings ... 108
5.2.7.1 Editing network and Layer 2 network access settings ... 108
5.2.7.2 Setting up a proxy server ... 112
5.2.7.3 Configuring the Docker network ... 116
5.2.7.4 Downloading logs ... 117
5.2.7.5 Adding an NTP server ... 117
5.2.8 Certificate management for connected Edge Devices ... 119
5.3 Installing system apps on Edge Devices ... 119
5.4 Launching system apps ... 122
6 Working with the IEM ... 125
7 Example of use - Monitoring bottle filling process ... 129
7.1 Description ... 129
7.2 System setup and requirements ... 130
7.3 Building the app ... 131
7.4 Creating the project and app in the Industrial Edge Management ... 132
7.5 Creating the app version in the IE App Publisher ... 135
7.6 Installing the app ... 140
7.7 Starting the app ... 143
8 List of abbreviations/acronyms ... 149
Glossary ... 151

Industrial security

1

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 and requirements (https://support.industry.siemens.com/cs/us/en/view/109781002)" manual.

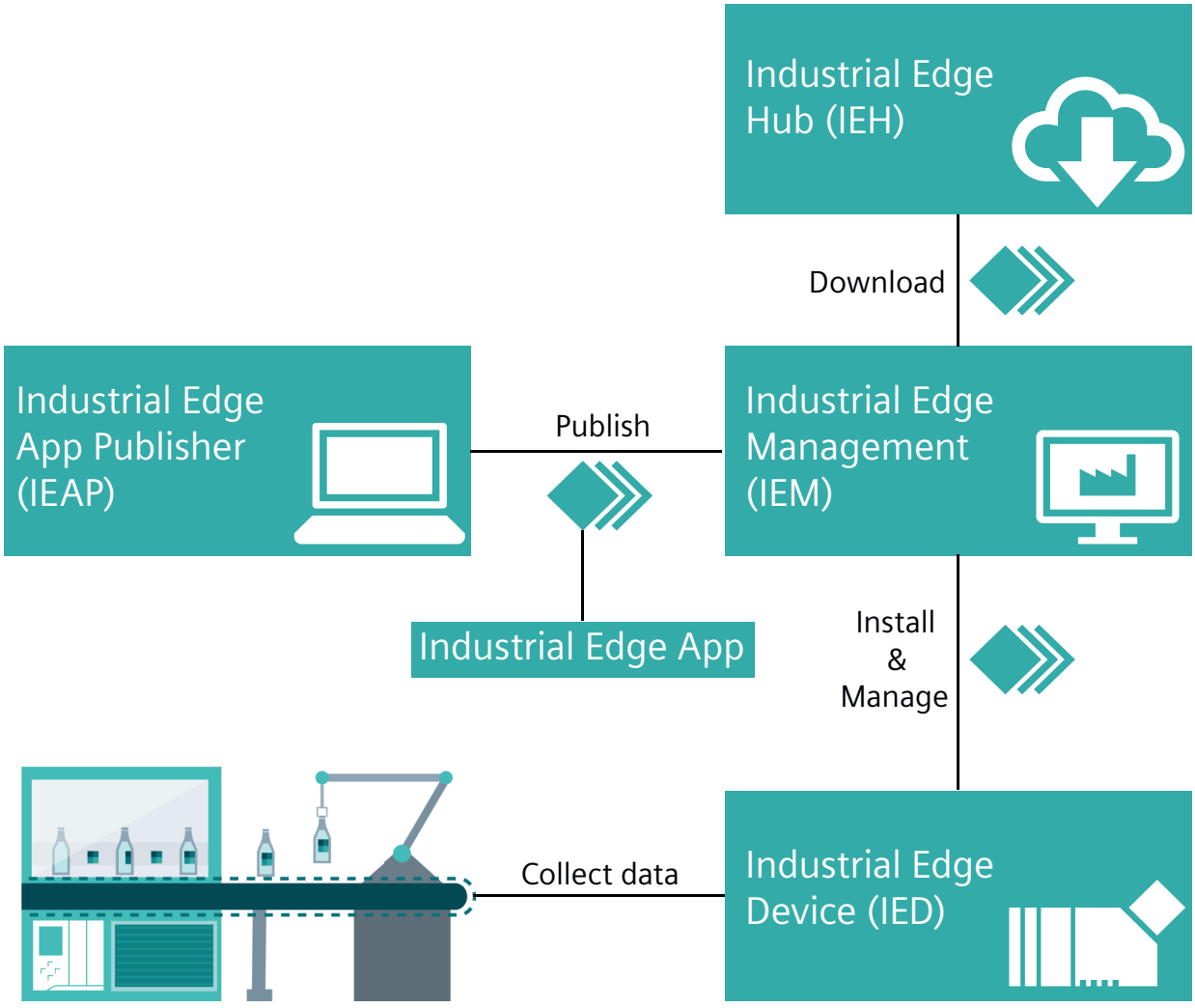
Overview of Industrial Edge

2

Industrial Edge combines local engineering with Cloud engineering.

Industrial Edge provides you with the following options:

- Install and use apps as required
- Distribution of apps to individual or grouped Edge Devices
- Availability of local data and, if desired, global data
- Regular software update cycles for Edge Devices and Edge Apps
- Pre-processing of data with low latency times
- Regular maintenance and updates of your system
- Management of associated Edge Devices and Edge Apps
- Development of custom Edge Apps
- Connectivity to your IT system and to automation
- Transfer of data with IT and cloud systems



Industrial Edge consists of the following main components:

- Industrial Edge Hub (IEH):
  The Industrial Edge Hub (IEH) is the central starting point for downloading and configuring the Industrial Edge Management (IEM). From the IEH, you download the Industrial Edge Management OS to enable the IEM on-premises and all necessary software for running the IEM. Furthermore, the IEH provides an app catalog where you purchase available Edge Apps. All necessary documentation and information about Industrial Edge is also available in the IEH.
- Industrial Edge Management (IEM):
  The Industrial Edge Management is the central infrastructure of Industrial Edge. The Industrial Edge Management is available as local IEM On-Premises. The Industrial Edge Management allows you to manage both connected Edge Devices and Edge Apps that you install individually on each Edge Device. The Industrial Edge Management also provide tools for managing Edge Devices and tracking analytics. Developers also have the possibility to create new projects using collaboration features and role-based access for co-developers.

- Industrial Edge Apps:
  Edge Apps are used for intelligent processing of automation data. Edge Apps are available from Siemens, business partners (OEMs), third-party vendors or from your own development. You use the IEM to configure, install and maintain Docker containerized Edge Apps from the Industrial Edge Hub to targeted Edge Devices.
- Industrial Edge Devices:
  You run the individual Edge Apps through Edge Devices. Edge Devices can store automation data locally and retrieve it as needed. In addition, Edge Devices can load this data to the cloud infrastructure (e.g. MindSphere) and retrieve it at any time. The Edge Device software is available for download. Once provisioned and connected, the IEM activates the Edge Device through a Edge Device configuration file.

Industrial Edge Hub

3

3.1 Sign up

Requirement

- You have purchased access to the Industrial Edge Hub.

  Note

  Purchasing access to the Industrial Edge Hub

  You purchase access to the Industrial Edge Hub in the Siemens Industry Mall. The purchasing process requires an email address and the allocated location.

- You have received a welcome email containing the URL of the Industrial Edge Hub.

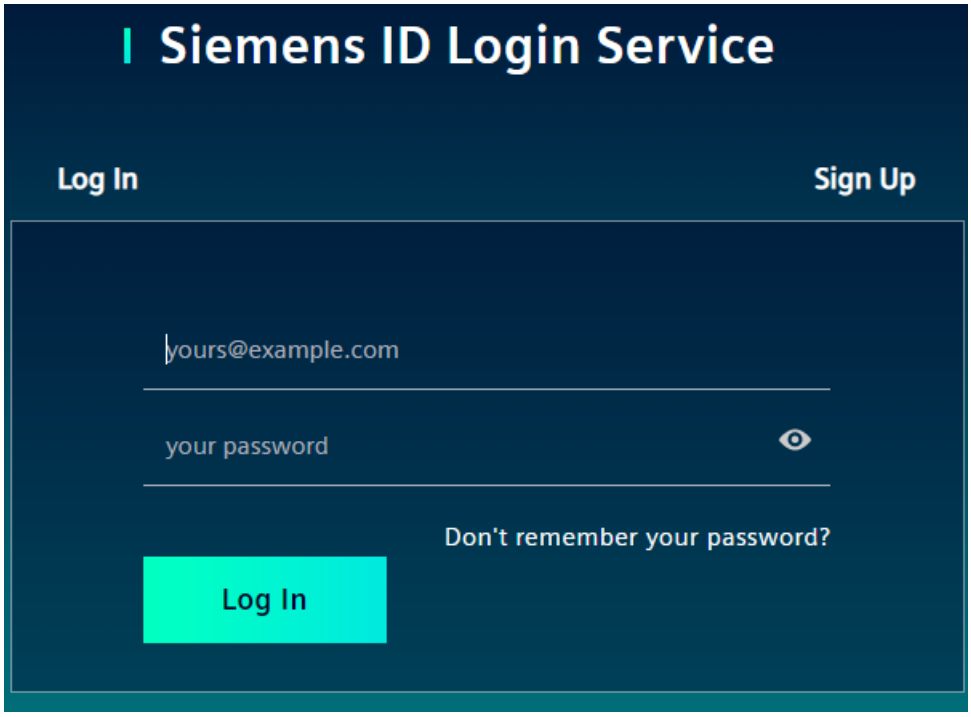
  Note

  Receiving the welcome email

  You receive the welcome email after you have purchased access to the Industrial Edge Hub. It takes some time between the purchase process and the receipt of the welcome email.

Procedure

1. After you have received the welcome email containing the URL of the Industrial Edge Hub, open the Industrial Edge Hub by clicking the link in the welcome email.
   The login screen for Industrial Edge Hub is displayed.



2. Click the "Sign up" tab.
3. Enter the following parameters in the according input fields:
   - Email address: Email address that has been specified for the Industrial Edge Hub access
   - Password: Password to log in to the Industrial Edge Hub

     Note

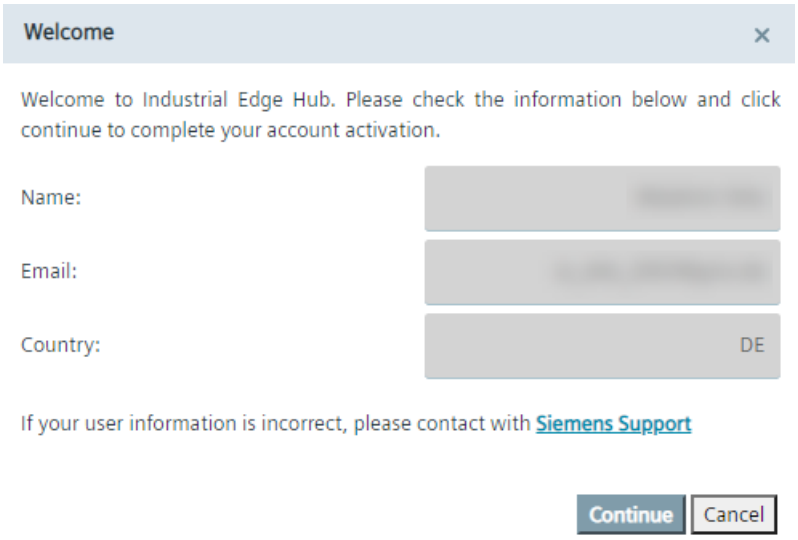
     Password requirements

     The password must meet at least 8 characters, 1 upper-case letter, 1 special character and 1 number.

   - First name: First name of the email user
   - Last name: Last name of the email user

   All input fields are mandatory.
4. Read and accept the terms of use.

5. Click "Sign Up".
   The "Welcome" screen is displayed.



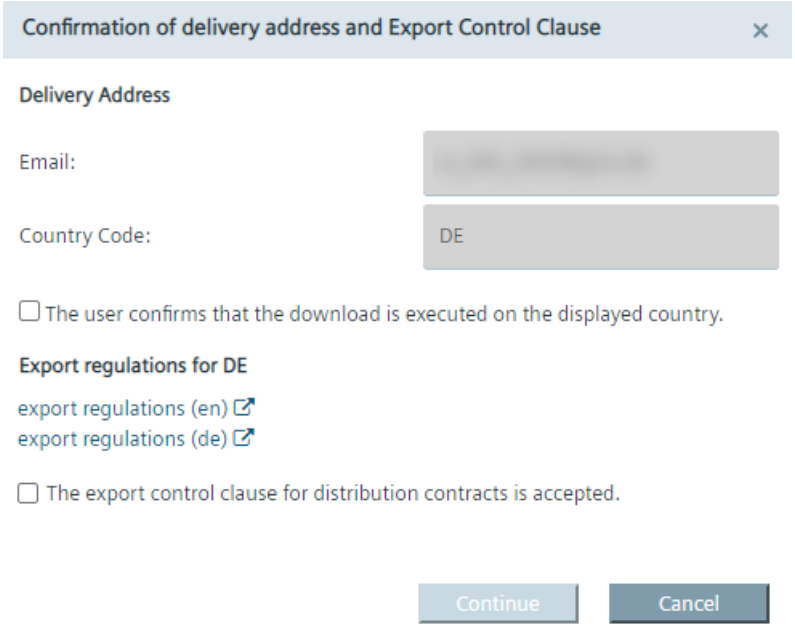
6. Check your data.
7. If everything is correct, click "Continue".

Note

Incorrect data

If the data is incorrect, click the link to contact the Siemens support.

The "Confirmation of delivery address and Export Control Clause" screen is displayed.



The displayed export regulations in the screen depend on your location, here for example Germany.

8. Before entering the Industrial Edge Hub, read the export regulations.
9. Accept the export regulations by selecting the 2 check boxes.
   The acceptance will be logged in the Industrial Edge Hub database along with the date of acceptance.
10. When both check boxes are selected, click "Continue".
    The home page of the Industrial Edge Hub is displayed.

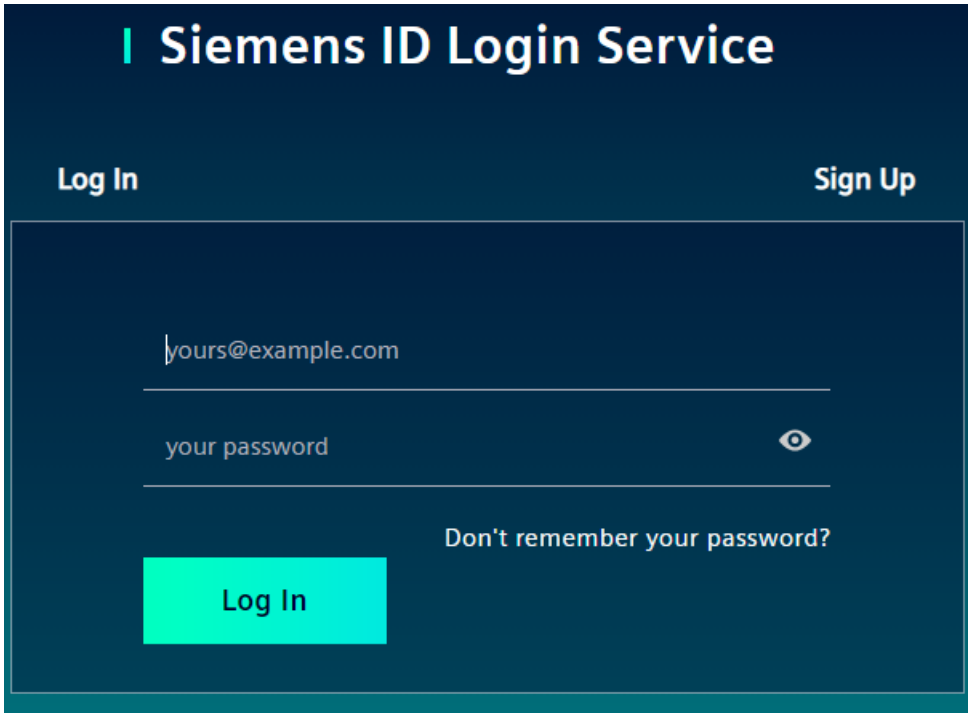
3.2 Log in

Requirement

- You have purchased access to the Industrial Edge Hub.
- You have successfully signed up to the Industrial Edge Hub.

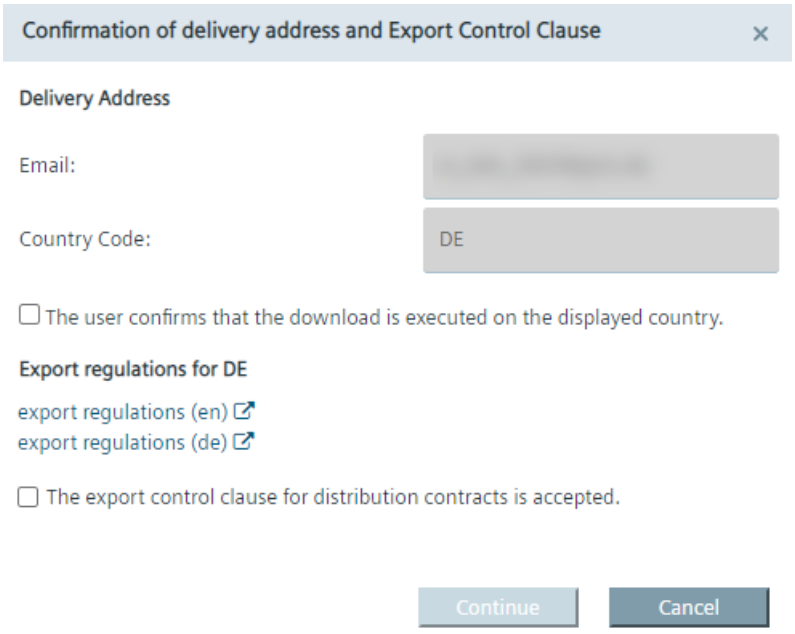
Procedure

1. Open the IE Hub by entering the URL into an Internet browser.
   The login screen for Industrial Edge Hub is displayed.



2. In the "Login" screen, enter your email address and your password in the according input fields.

3. Click "Log in".
   The "Confirmation of delivery address and Export Control Clause" screen is displayed.

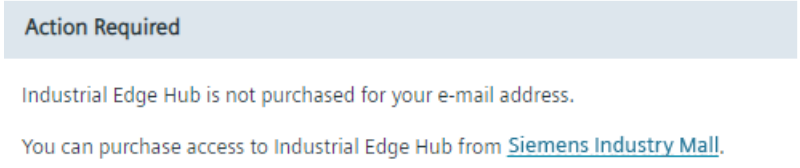


   The available export regulations in the screen depend on your location, here for example Germany.

4. Before entering the IE Hub, you must read the export regulations.
5. Accept the export regulations by selecting the 2 check boxes.
   The acceptance will be logged in the IE Hub database along with the date of acceptance.
6. When both check boxes are selected, click "Continue".
   The home page of the IE Hub is displayed.

No access to the Industrial Edge Hub

If you try to sign into the Industrial Edge Hub without having purchased access to the Industrial Edge Hub, the following screen is displayed:

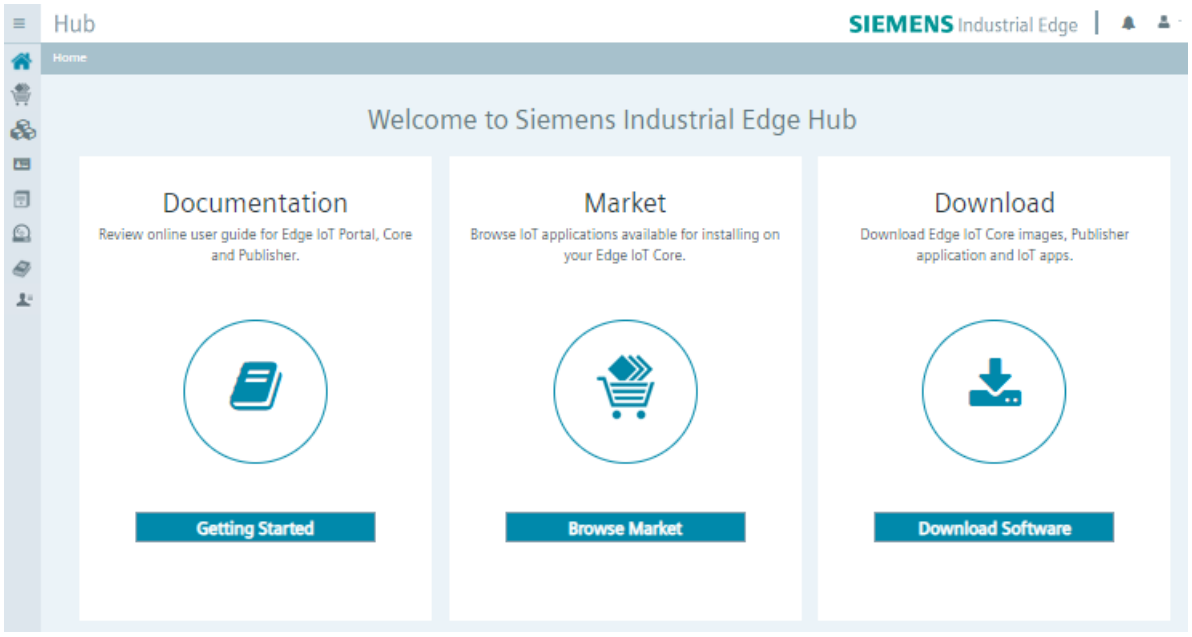


Purchase access to the Industrial Edge Hub in the Siemens Industry Mall by clicking the link.

3.3 Home

After you log in to the IE Hub, the "Home" screen of the IE Hub is displayed.

The following figure shows the IE Hub home page:



By clicking the button within the tiles, you navigate to the according menu item.

The IE Hub provides the following menu:

- Home
- Market
- Library
- Licenses
- IEM Instances
- Download Software
- Documents
- User Management

Notifications

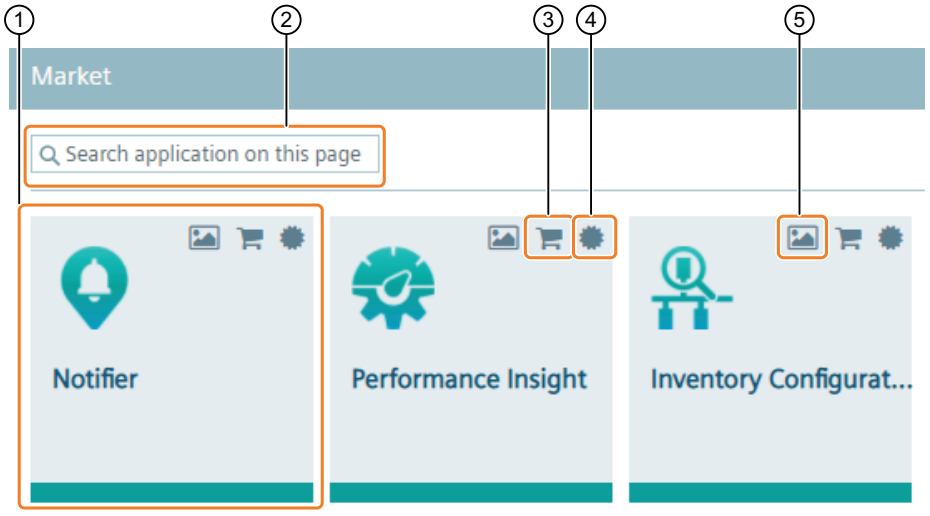
By clicking the icon, the "Notifications" screen with all notifications referring to the IE Hub is displayed. Whenever 1 of the following events occur, the according notification is displayed in the "Notifications" screen:

- Purchased Edge Device licenses
- Purchased Edge App licenses
- Releases of new Industrial Edge Management OS
- Releases of new Industrial Edge Device OS
- Releases of new Edge App versions
- Updates of Edge Apps

3.4 Market

The "Market" screen contains the global app catalog from where you purchase available and downloadable Edge Apps.

The following figure shows the "Market" screen as an example:



① Purchasable Edge App
② Filter the app catalog based on the app name
③ Purchase the Edge App
④ Licensing status:
- Gray: Edge App is not licensed
- Green: Edge App is licensed

⑤ If screenshots are available for the Edge App, display screenshots

3.4.1 Purchasing an Edge App license

To purchase an Edge App license, click the icon of the Edge App. You will be redirected to the corresponding Siemens Industry Mall web page. There you purchase a license for the Edge App. After you purchase a license, it takes some time for the licensing process of the Edge App. After the Edge App has been licensed for you by Siemens, you receive an email that the license has been approved for your account. Then, the color of the licensing status switches to green. Once the color of the licensing status switches to green, you are able to download the app.

Note

Purchasing an Edge Device license

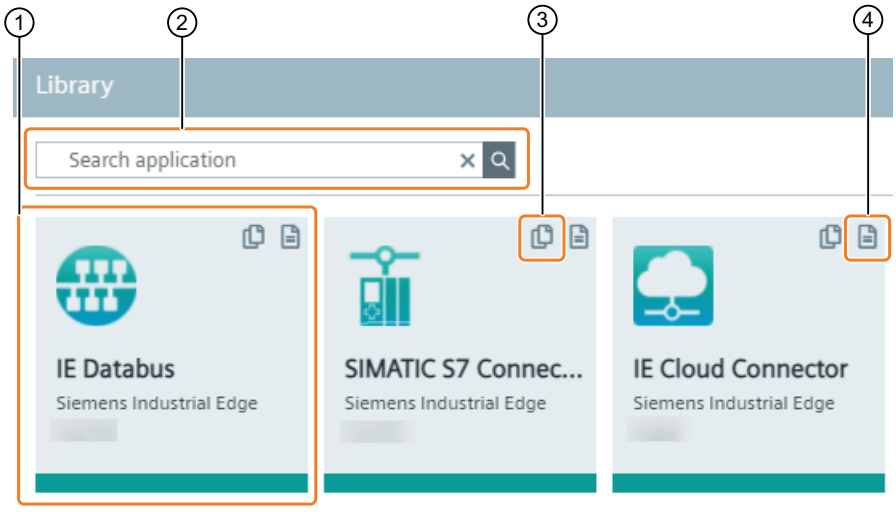
To use and connect Edge Devices in the IEM, you need according Edge Device licenses too. To purchase Edge Device licenses, you obtain a link from Siemens through which you purchase the according Edge Device licenses.

3.5 Library

The "Library" screen lists all apps for which you purchased a license and which you can transfer to your IEM instance.

The system apps are included in the purchase of the Industrial Edge Management, so you do not have to purchase a license for the system apps. You can directly copy the system apps to the catalog of an IEM instance.

The following figure shows an example of the "Library" screen:



① Licensed app including version of the app
② Search for an app
③ Copy app to IEM catalog
④ Open app documentation

3.5.1 Copying the app to the IEM catalog

Procedure

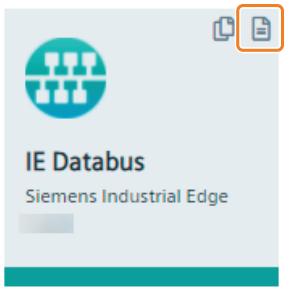
Copying an app to the IEM catalog requires an IEM instance and an Internet connection. With the functionality, you send the app directly to the catalog of 1 of your IEM instances.

To copy an app to the IEM catalog, proceed as follows:

1. By clicking the icon, the "Copy Application to IEM catalog" screen is displayed.
   The layout of the screen depends on whether or not the app includes links for open source software (OSS) sources and for the readme. By clicking 1 of the links, the respective file is being downloaded. When the app does not support the above-mentioned links, the screen is displayed without the links.
2. From the drop-down list, choose the IEM instance to which you want to send the app to.
3. Click "Copy".
   An according job is created. You can check the status of the job in the job status screen of the specific IEM instance.

3.5.2 Opening app documentation

If the app provides a documentation, the app tile contains the documentation icon.

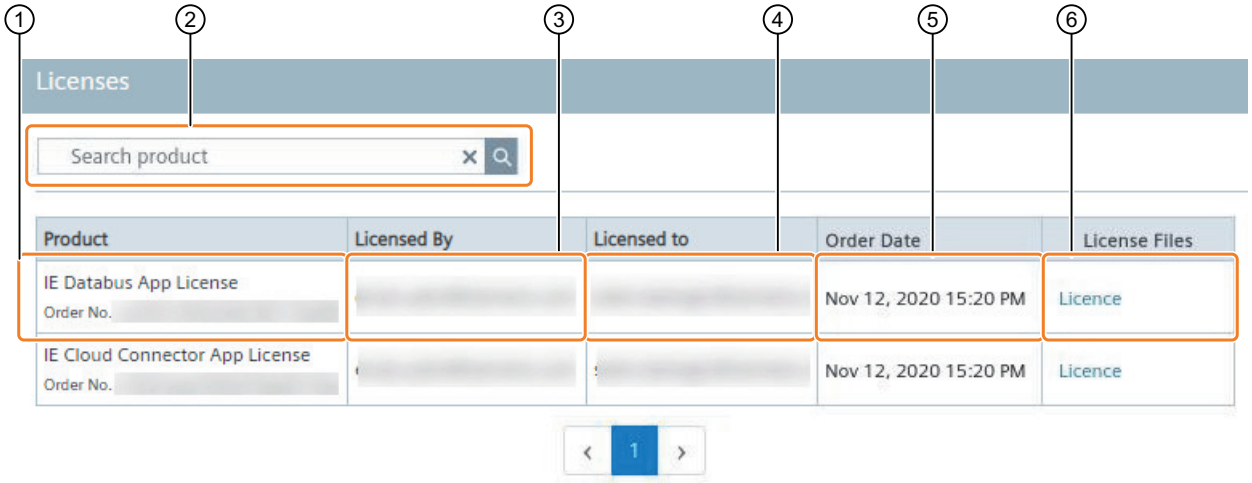


By clicking the icon, you will be redirected to the documentation page.

3.6 Licenses

The "Licenses" screen lists all licenses that are activated for your products.

The following figure shows the "Licenses" screen as an example:



① Product name and order number (MLFB)
② Filter the products by entering either the order number or the product name
③ Purchaser email address
④ Customer email address
⑤ Date of order
⑥ Download license file

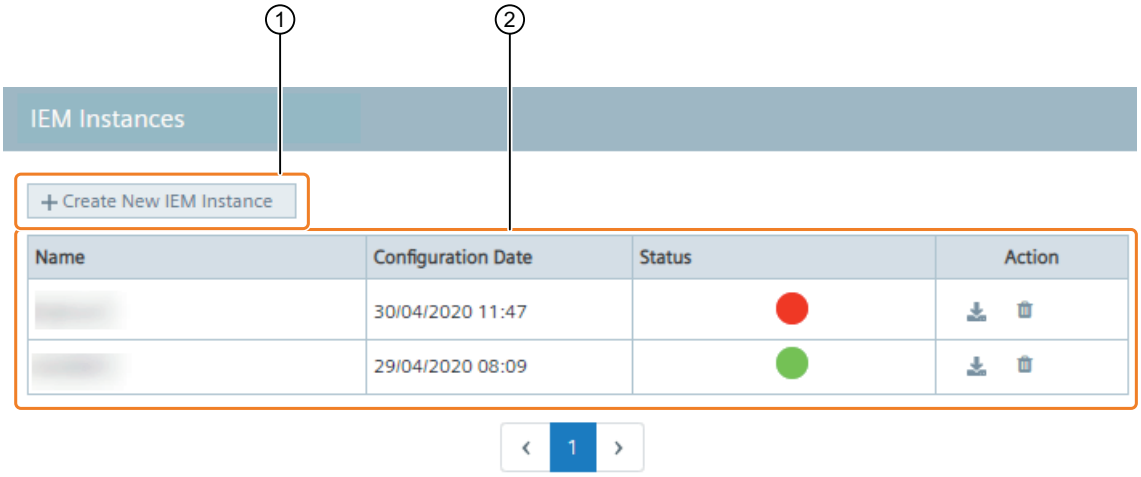
3.7 IEM Instances

The "IEM Instances" screen lists all existing IEM instances and provides the following functions:

- Creation of new IEM instances
- Management of IEM instances

When you create a new IEM instance, the IEM instance is added to the table and a configuration file is created. This configuration file contains the configuration for the IEM that you need to set up the IEM.

The following figure shows the "IEM Instances" screen as an example:



① Create New IEM Instance

② IEM instances table

Listed IEM instances inclusive following information:

- Name: Name of the instance
- Configuration Date: Creation date of the instance
- Status: Status of the instance
  - Green: Online
  - Red: Offline
- Action: Download configuration file and delete IEM instances

3.7.1 Managing IEM instances

Creating an IEM instance

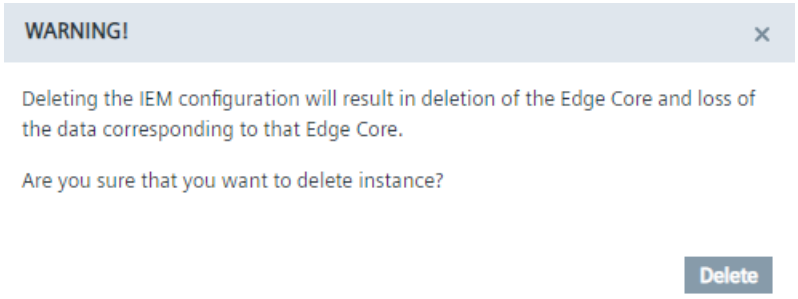
When you click on "Create New IEM Instance", you create a configuration file which you need for setting up your IEM. You find the detailed procedure to create an IEM instance in the "Creating IEM instance and downloading the configuration file (Page 31)" subsection.

Downloading an IEM configuration file

To download an IEM configuration file, click the icon of the respective instance. The configuration file is downloaded to the standard download folder of your Internet browser.

Deleting an IEM instance

1. Click the icon of the respective instance.
   A warning is displayed.



   If you delete the IEM instance, all data corresponding to this IEM instance will be deleted irrecoverable.

2. To confirm the deletion, click "Delete".
   The IEM configuration is deleted from the IEH.

3.8 Download Software

In the "Download Software" screen you download all necessary software for running the IEM.

In the "Initial Setup Tools" tab, you download the Industrial Edge Management OS which runs on a VM. From the "Update Packages" tab, you download the software update package to update the Industrial Edge Management. From the "Developer Tools" tab, you download the Windows respectively Linux version of either the UI based software or the CLI (command line interface) of the Industrial Edge App Publisher.

By clicking the "Download" button of the corresponding software, the software is downloaded to the standard download folder of your Internet browser.

The respective software also includes links for its open source software (OSS) sources and for the OSS readme. By clicking 1 of the links, the respective file is being downloaded.

3.9 Documents

In the "Documents" screen, you get the necessary documentation and additional information regarding Industrial Edge.

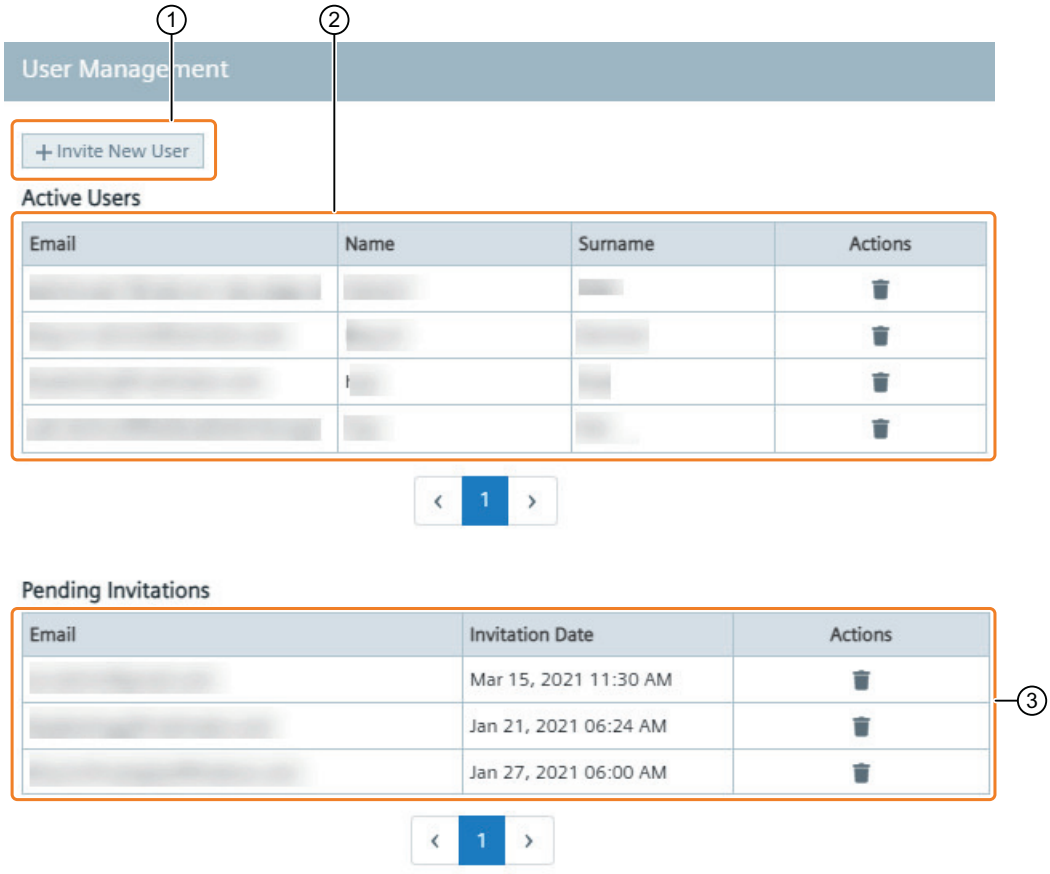
You can open all documents either as PDF or HTML file.

3.10 User Management

3.10.1 Overview

In the "User Management" section you get an overview of all registered users in your IE Hub tenant and also a list of invited users who have not yet accepted the invitation to access the IE Hub. Additionally, you can invite new users to your IE Hub tenant and again delete users from your tenant via this screen.

The "User Management" screen is displayed as follows for example:

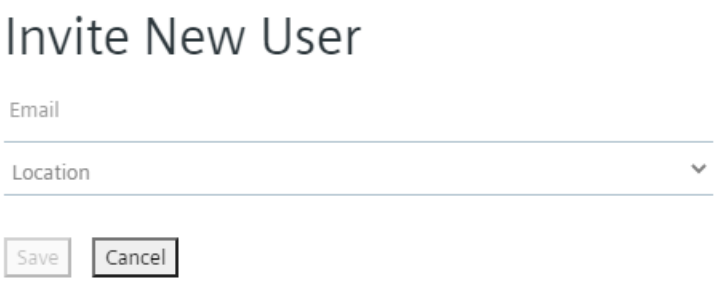


① Invite new user to your IE Hub tenant
② Registered users
③ Pending users

3.10.2 Inviting a new user

Procedure

1. Click "Invite New User".
   The "Invite New User" screen is displayed.



2. In the "Email" input field, enter the email address of the user you want to invite to your IE Hub tenant.
3. In the "Location" drop-down list, select the location of the respective user.
4. Click "Save".
   The invitee will be added to the "Pending Invitations" list and an email will be sent to the invitee. The invitee then must activate his account by signing up to the IE Hub (Page 13). After the invitee has activated his account, the invitee will move to the "Active Users" list and is able to access the IE Hub. The invitee has the same roles and permissions as the other users in the IE Hub tenant.

3.11 Cancelling an IE Hub subscription

If you do not want to extend your IE Hub subscription, you can cancel the subscription. To cancel your IE Hub subscription, contact the Industrial Edge Support. Only the IE Support can cancel your IE Hub subscription. After your cancellation has been approved by the IE Support, the expiration date will be displayed in the header of your IE Hub tenant. When the expiration date is reached, the header indicates that your account has been cancelled resulting in a limited access to the IE Hub for all users of the IE Hub tenant.

With limited access to the IE Hub, the following is no longer possible:

- Creating IEM instances
- Downloading any content (inclusive IEM configuration files)
- Purchasing apps
- Inviting new users

With limited access to the IE Hub, the following is still available:

- List of existing IEM instances
- List of purchased apps in the "Library" section

- Download already purchased app licenses
- List existing users and delete users in the "User Management" section

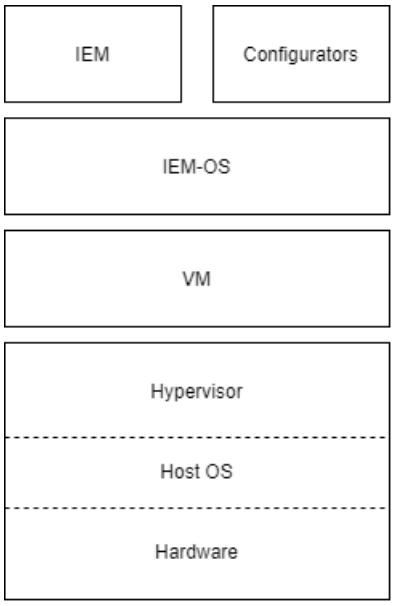
Setting up the IEM

4

4.1 Setup steps

To deploy the IEM, you need access to the Industrial Edge Hub. After accessing and downloading the Industrial Edge Management OS (IEM-OS) from the Industrial Edge Hub, you must create an IEM instance. After creating the IEM instance, you run the downloaded Industrial Edge Management OS locally in a VM. This VM, including the Industrial Edge Management OS, enables the IEM. After activating the IEM-OS, the IEM gets installed as "Edge Management" app in the IEM-OS.

The following figure illustrates how the components are based on each other:



When you successfully install the IEM, you use the IEM to manage the on-premises Industrial Edge infrastructure.

Requirements for setting up the IEM

- A software is installed on the PC to extract zip-files, for example "7-Zip".
- 1 additional network interface, for example an USB network adapter with static IP address, if you use a bridged network connection for the VM.
- UEFI Boot is enabled in the VM.
- Minimum 16 GB RAM.
- Minimum 50 GB hard disk space.
- Ensure that the time setting on the host system is correct.
- Do not enable the feature for virtualizing the clock in the VM.

- Do not install additional virtualization packages in the VM, for example VMware Tools or VMware Workstation or Oracle VirtualBox Guest Additions.
- Siemens recommends the following additional settings to raise security:
  - VM is set up encrypted
  - Trusted Platform Module (TPM) is enabled for the VM

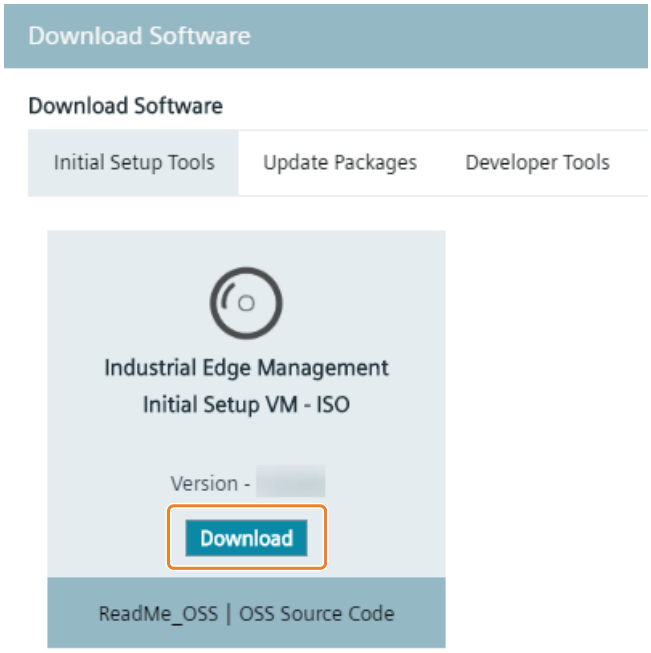
  You find information on how to enable these settings in the documentation of the virtualization environment itself from the Internet.

4.2 Downloading the Industrial Edge Management OS

You download the Industrial Edge Management OS (IEM-OS) for the VM from the IE Hub. The Industrial Edge Management OS, that is running in a VM, enables the IEM.

Procedure

1. Sign into the IE Hub.
2. In the navigation, click "Download Software".
   The "Download Software" screen is displayed.
3. In the "Initial Setup Tools" tab, click "Download" in the "Initial Setup VM - ISO" section.

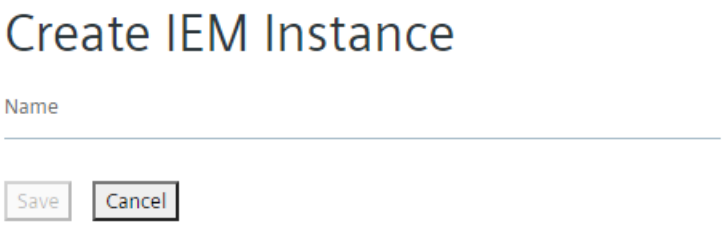


   A "*.zip" file containing the ISO image of the Industrial Edge Management is downloaded to the standard download folder of your Internet browser. The version of the IEM is also included in the file name.
4. Extract the "*.iso" file from the downloaded zip file.
   You run this ISO image later in the VM.

4.3 Creating an IEM instance and downloading the configuration file

Procedure

1. In the navigation menu in the IE Hub, click "IEM Instances".
2. Click "Create New IEM Instance".
   The "Create IEM Instance" screen is displayed.



3. In the "Name" input field, enter the name of the instance.
   The name of the instance must match the following criteria:
   - Minimum 3 characters
   - Only lowercase letters and numbers
   - Must not start with a number
   - Must be unique within your tenant in the IE Hub

Note

Recommendation for name of the instance

Siemens recommends, to use a name for the instance that corresponds to the URL of the IEM that you later configure during the setup of the IEM. Use, for example, "iem" as name of the instance and "iem.my.domain.name.com" as URL of the IEM.

4. Click "Save".
   The IEM instance is added to the IEM instance table. The configuration of the IEM instance is saved to the configuration file.

Note

Changing the name of an IEM instance

You cannot change the name of an IEM instance. Instead, you must either create a new IEM instance or delete old IEM instances and recreate a new one.

5. To download the IEM configuration file, click the icon of the respective instance.
   The configuration file is downloaded to the standard download folder of your Internet browser.

4.4 VMware Workstation

4.4.1 Creating the VM

After downloading the Industrial Edge Management OS, you import and install the IEM-OS in the virtualization environment.

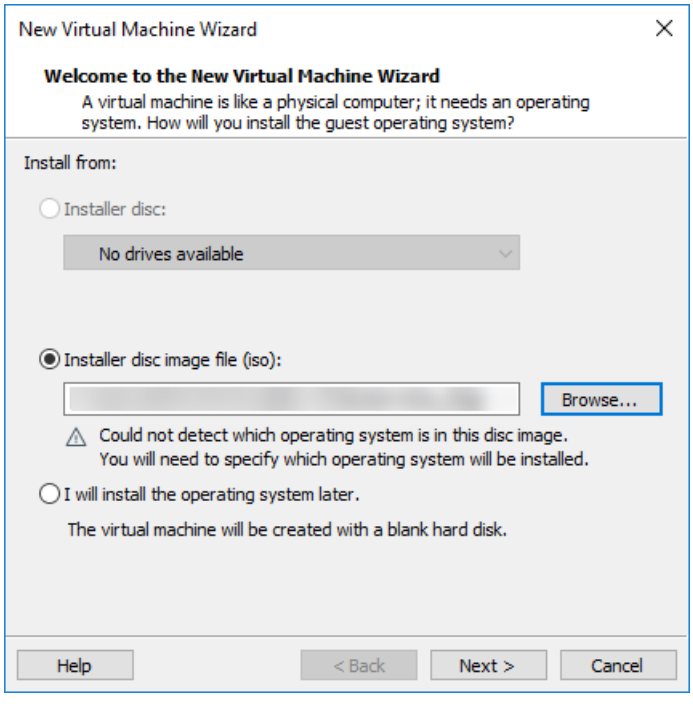
The following procedure describes the installation in the "VMware Workstation" virtualization environment.

Requirement

The ISO image of the IEM is downloaded to the PC.

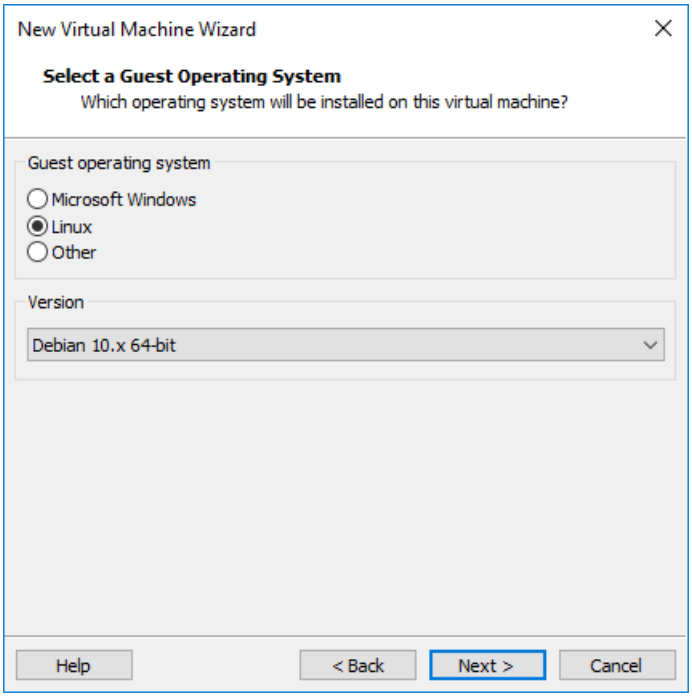
Procedure

1. Open "VMware Workstation".
2. Select the "File > New Virtual Machine" menu command.
   The "New Virtual Machine Wizard" screen is displayed.
3. Select the "Typical (recommended)" option as configuration type.
4. Click "Next".
5. Select the "Installer disc image file (iso)" option.
6. Click "Browse" and select the extracted "industrial_edge_management.iso" file.

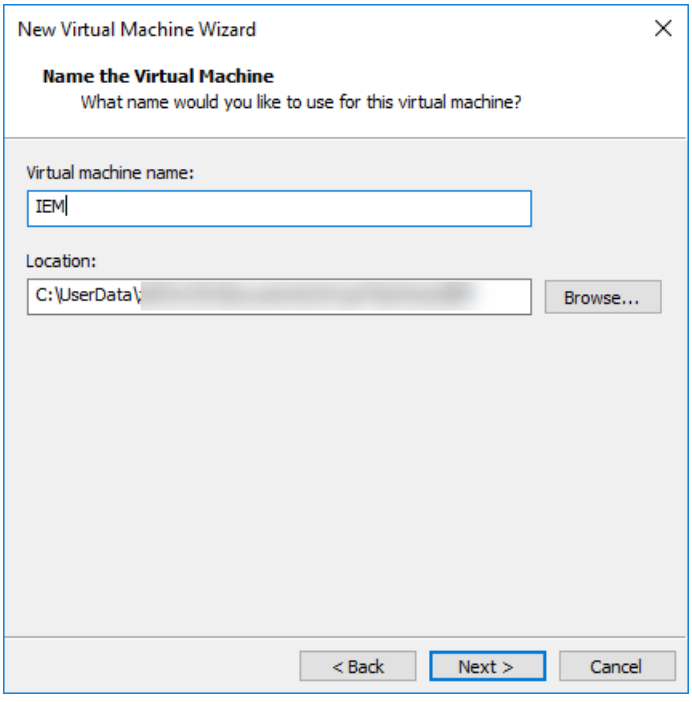


7. Click "Next".

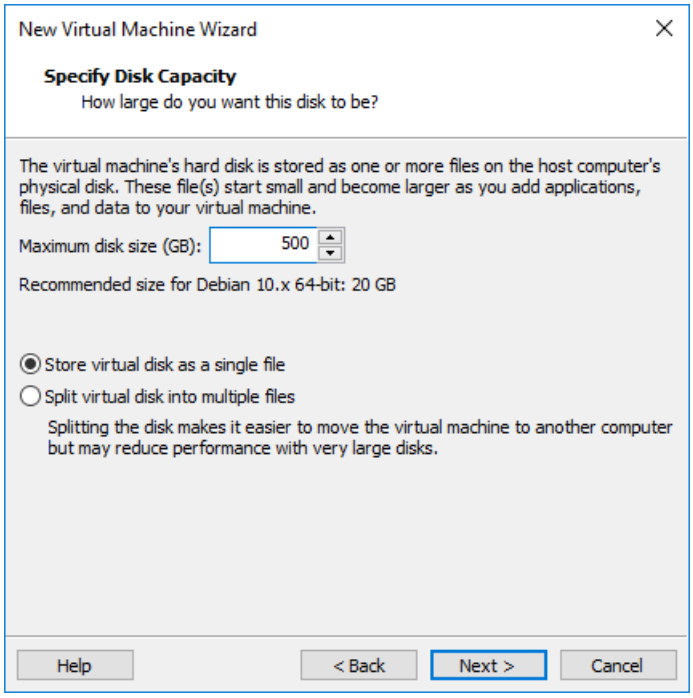
8. From the "Guest operating system" options, select "Linux".
9. From the "Version" drop-down list, choose a 64-bit version of a Linux distribution, for example "Debian 10.x 64-bit".



10. Click "Next".
11. In the "Virtual machine name" input field, enter a name for the VM.
12. If necessary, choose a storage location for the VM on your PC by clicking "Browse".

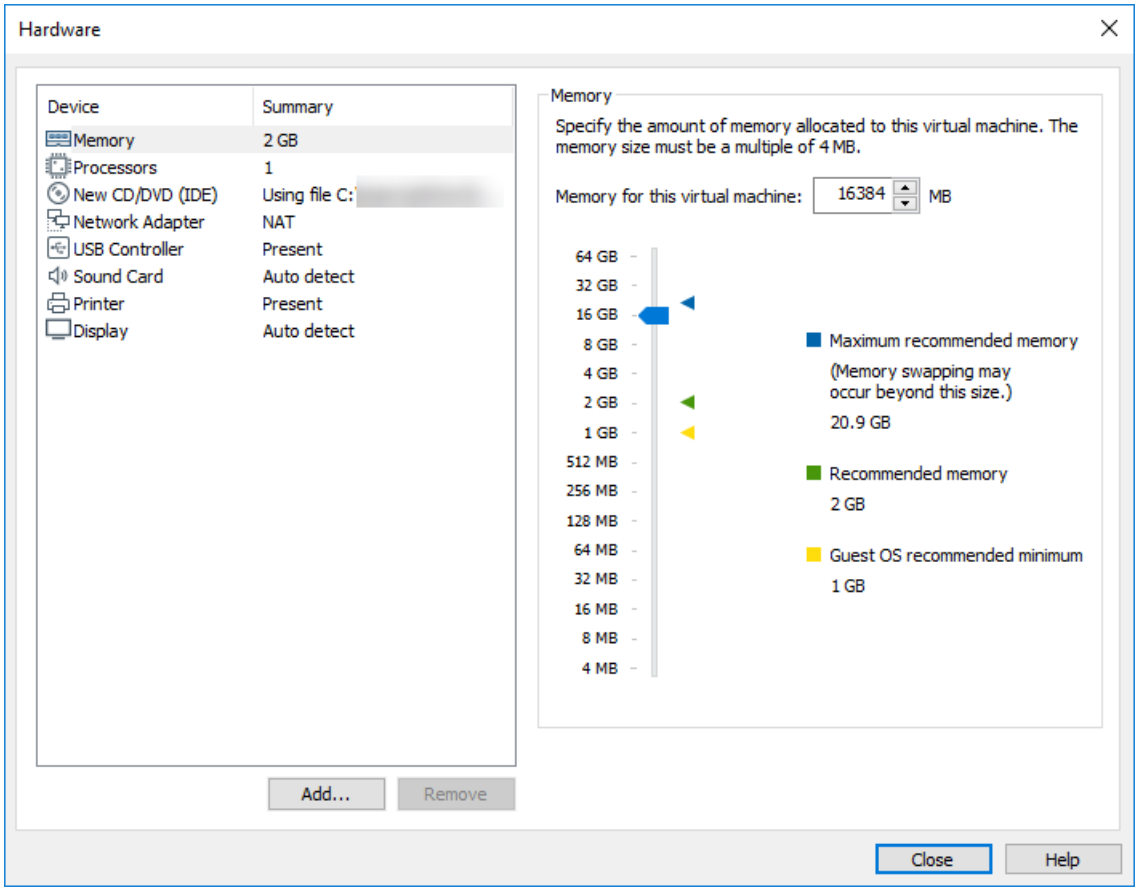


13. Click "Next".
14. In the "Maximum disk size (GB)" input field, enter a maximum disk size for the VM on the host PCs physical disk.
    The disk is mandatory for the operating system and also stores app images and containers. The size of the disk depends on the apps and the apps sizes that you want to install. Siemens recommends a maximum disk size of 500 GB. A minimum of 50 GB is mandatory.
15. Select the "Store virtual disk as a single file" option.

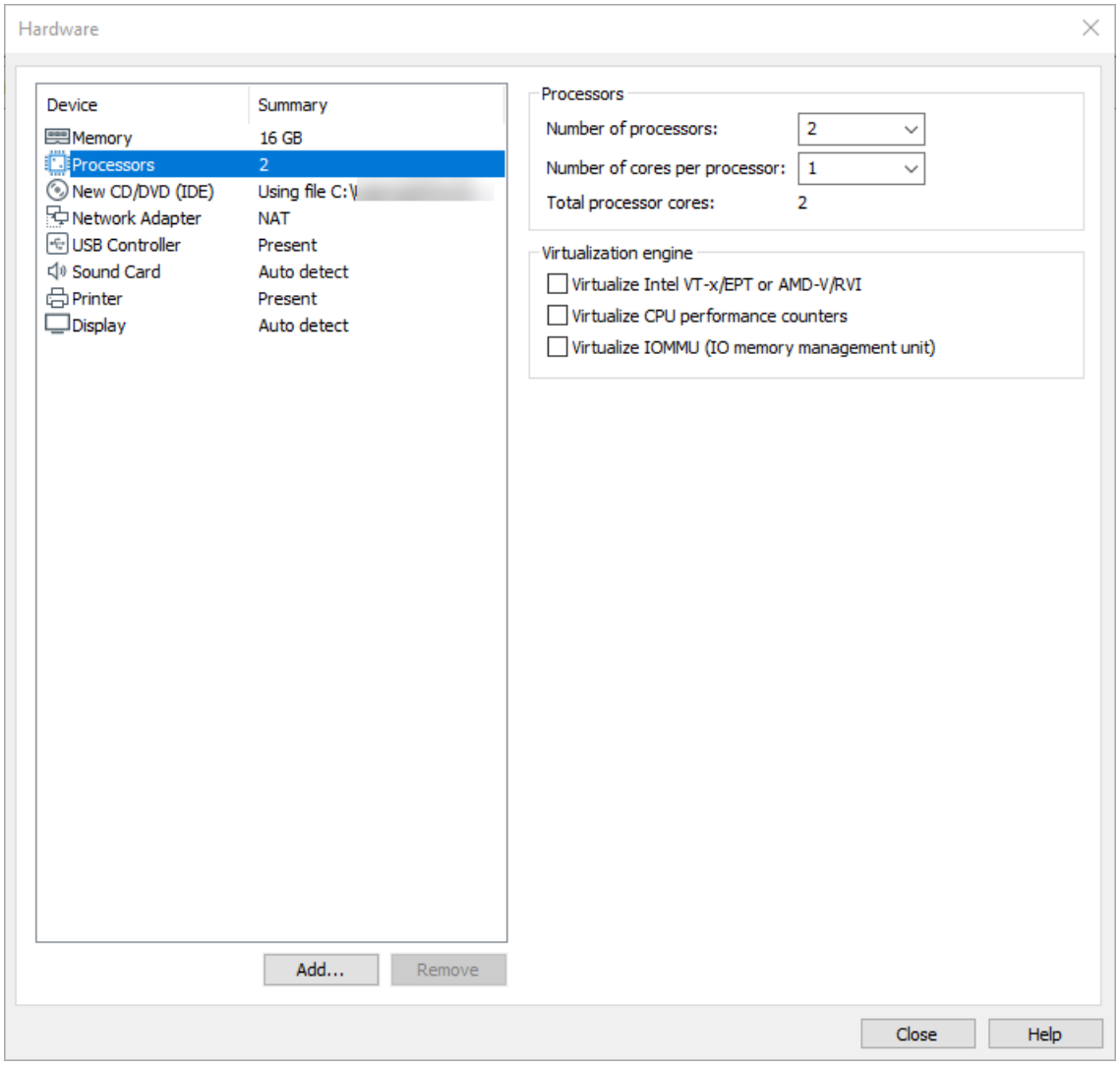


16. Click "Next".
17. Click "Customize Hardware".

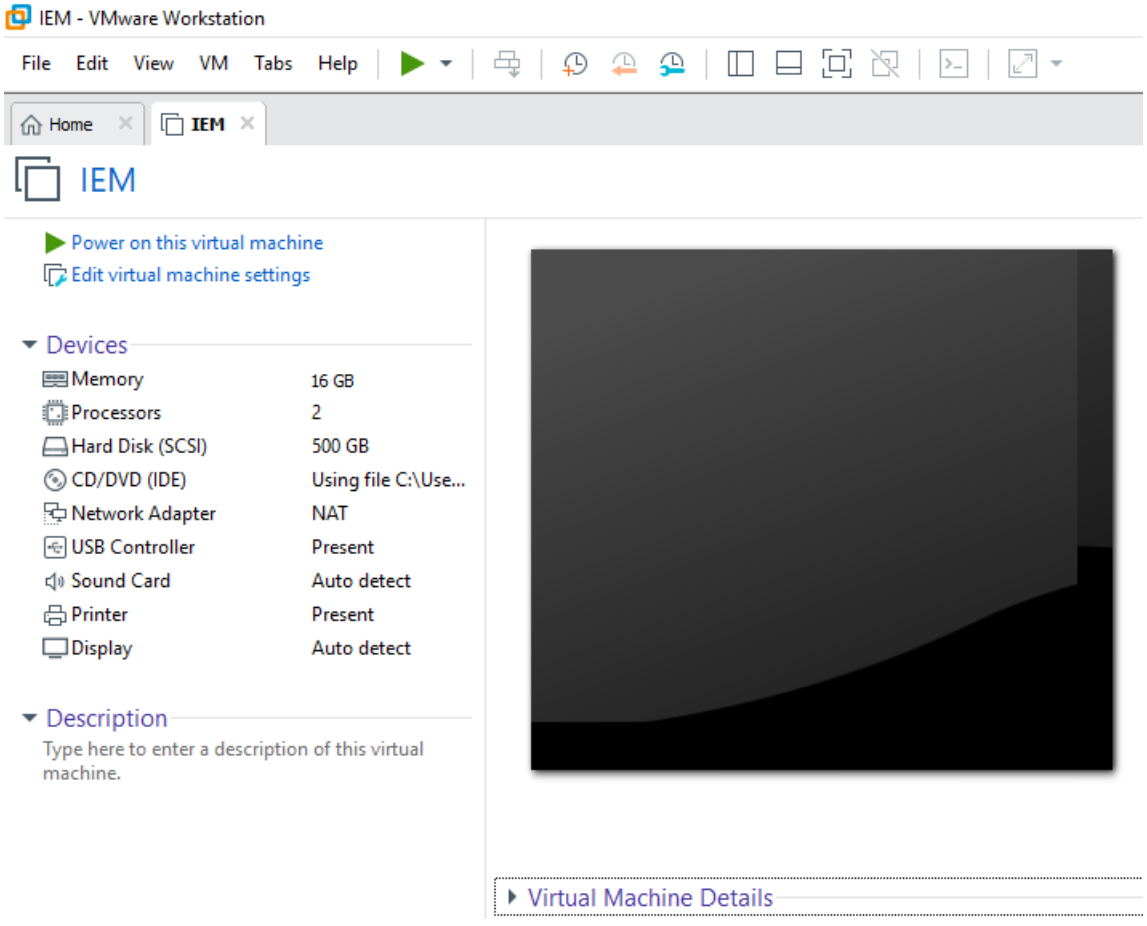
18. For the memory amount allocated to the VM, choose a minimum of 16 GB.



19. For the number of processors, choose minimum 2 processor cores for the VM.



20. Click "Close".
21. Click "Finish".
    The VM is created.



4.4.2 Configuring the VM

Requirement

If you use a "Bridged" network connection for your VM, you need 1 additional network interface.

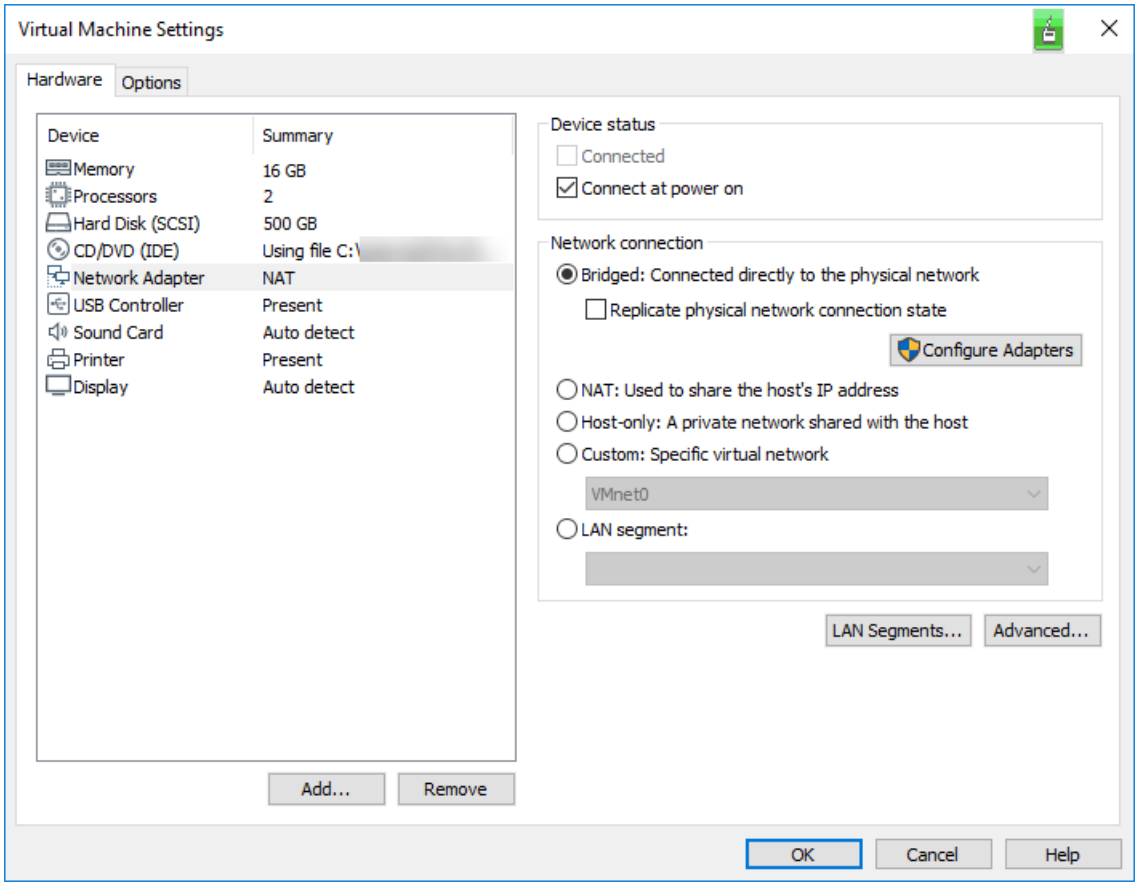
Note

USB network adapter

The following procedure describes the use of an USB network adapter as additional network interface. Proceed in the same manner for other additional network interfaces.

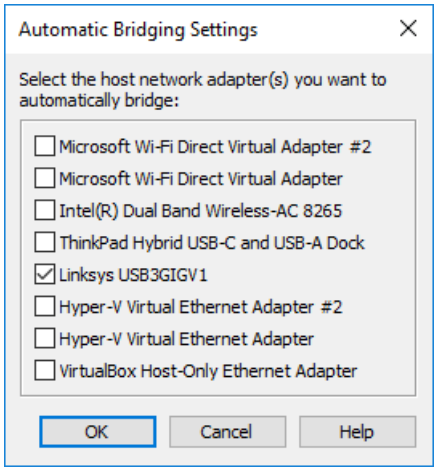
Procedure

1. Select the created VM.
2. Click "Edit virtual machine settings".
3. In the hardware list on the left side, choose "Network Adapter".
   The steps 5. to 10. describe the configuration when you use an USB network adapter for the network connection of your VM. This configuration is optional. You can also use a "NAT" network connection.
   If you use a "NAT" network connection for your VM, go to step 11.
4. On the right side under "Network connection", select "Bridged: Connected directly to the physical network".

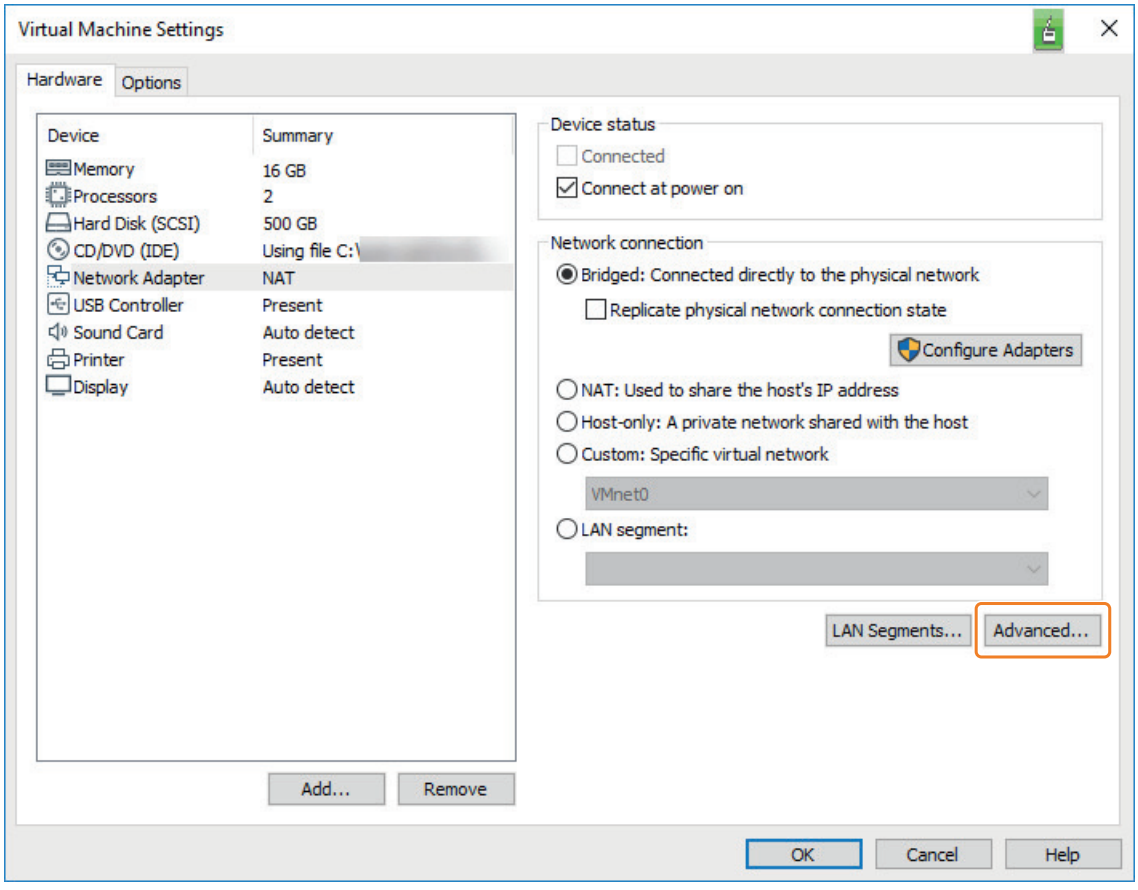


5. Click "Configure Adapters".
   The "Automatic Bridging Settings" screen is displayed.

6. Activate only your connected USB network adapter.

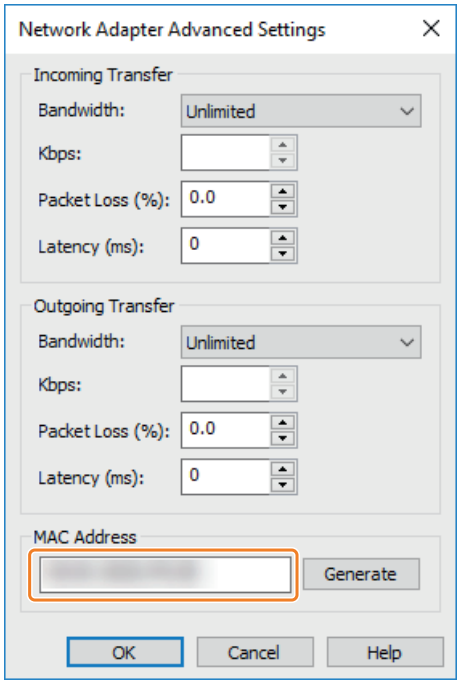


7. Click "Ok".
8. On the right side below the "Network connection" section, click "Advanced".



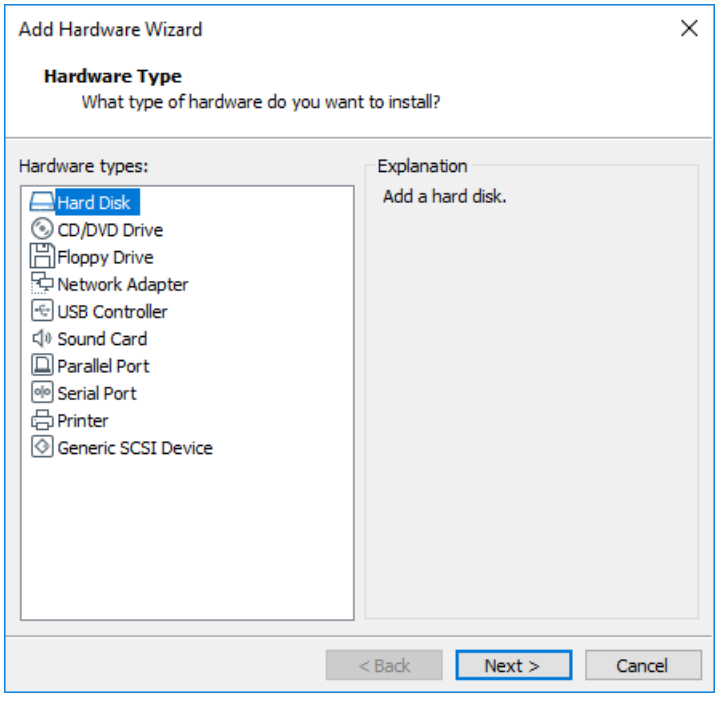
The "Network Adapter Advanced Settings" screen is displayed.

9. In the "MAC Address" input field, enter the MAC address of your USB network adapter for a bridged network connection.



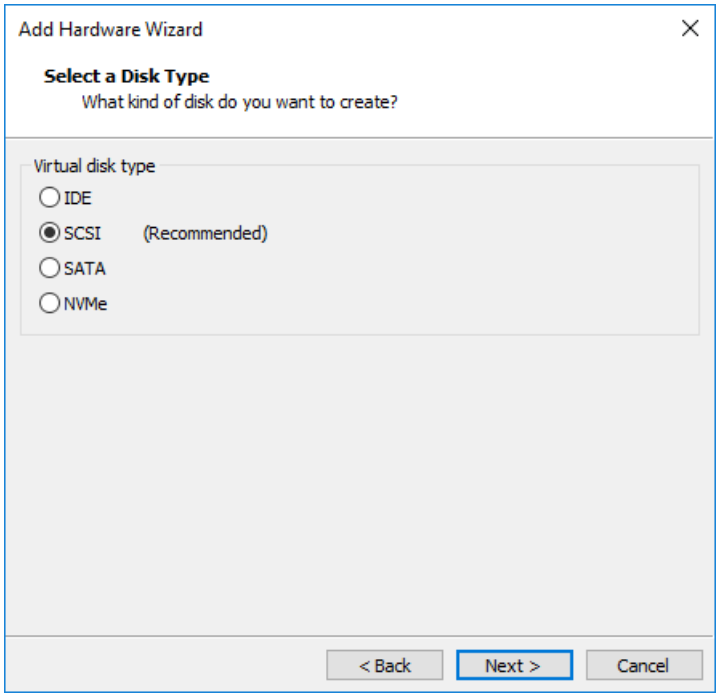
10. Click "Ok".

11. Below the left navigation, click "Add".
The "Add Hardware Wizard" screen is displayed.

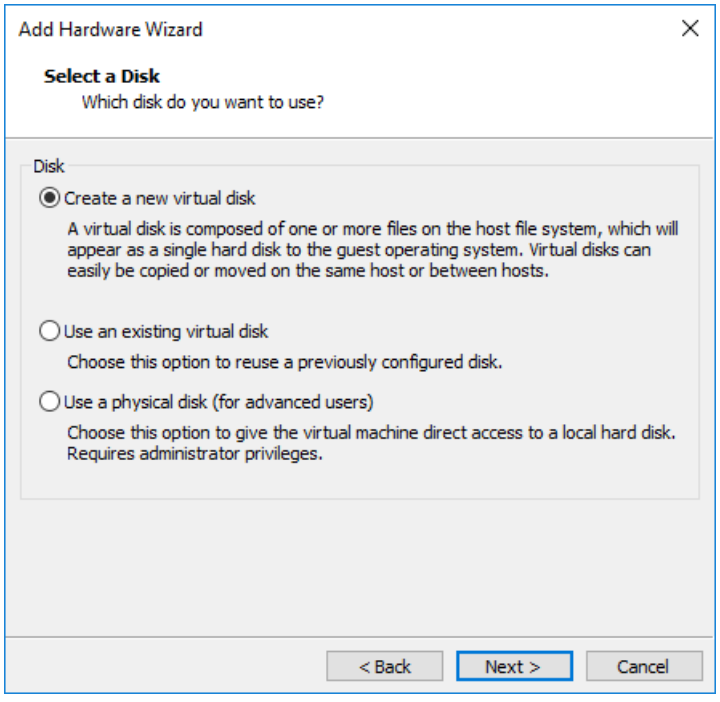


12. Select "Hard Disk" and click "Next".

13. As virtual disk type, select "SCSI" and click "Next".

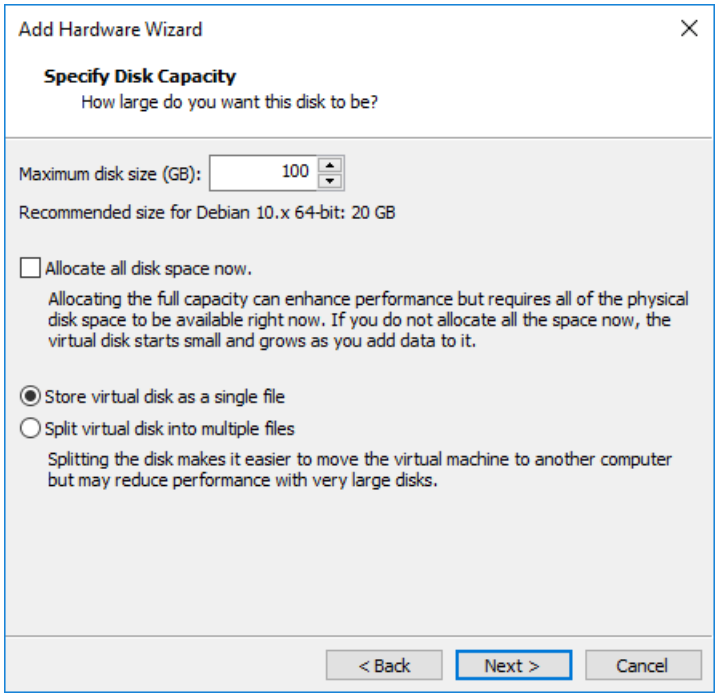


14. Select "Create a new virtual disk" and click "Next".

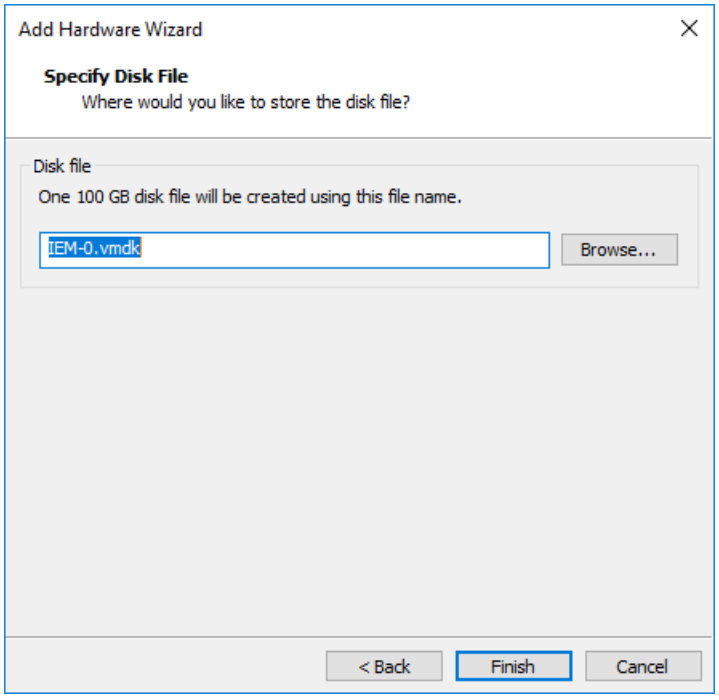


15. In the "Maximum disk size (GB)" input field, enter a maximum disk size that is lower than the disk size that you configured before.
    The second hard disk is for the apps data storage.
    Siemens recommends a maximum disk size of 100 GB for the second disk. A minimum of 50 GB is mandatory.

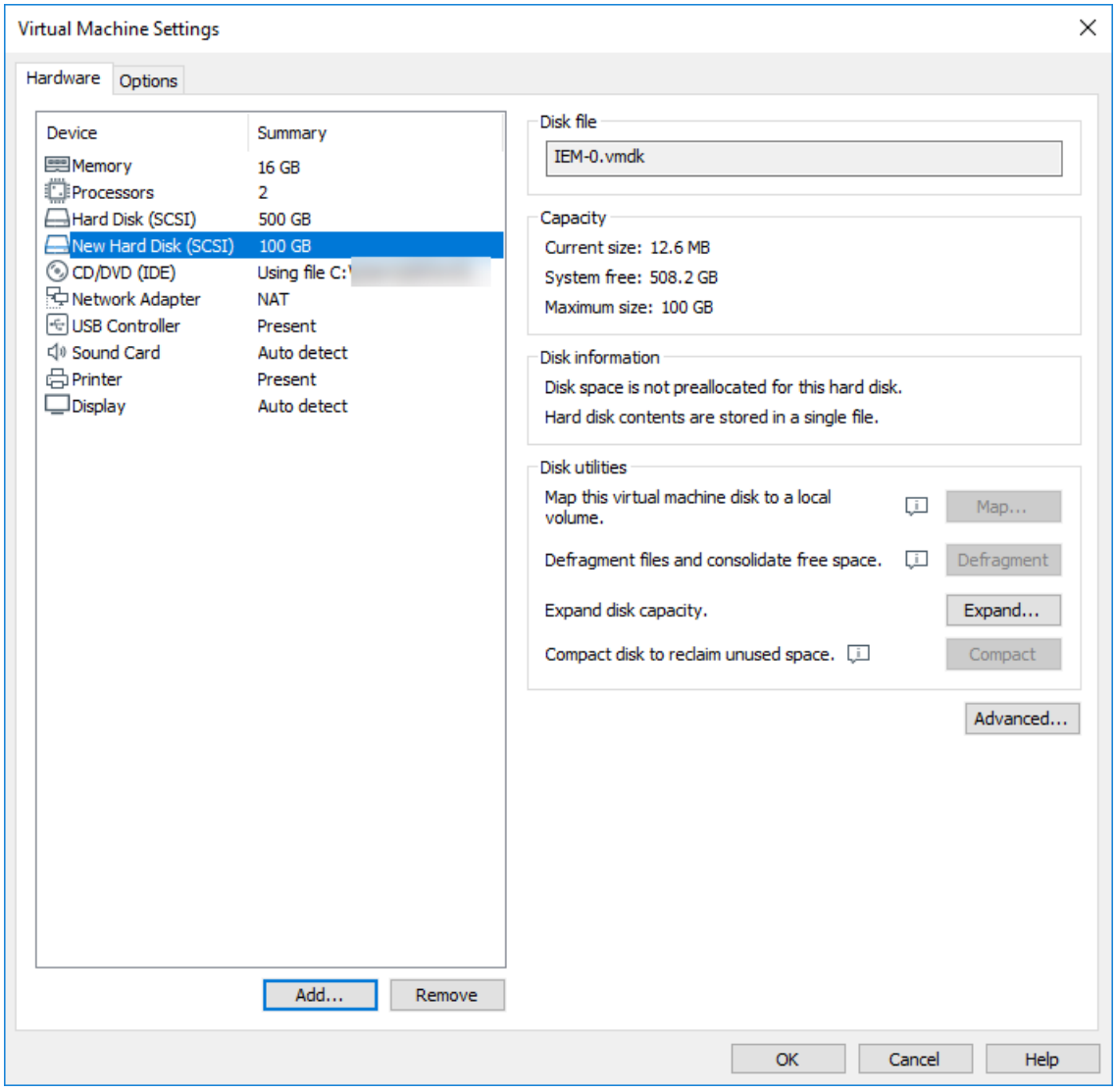
16. Select "Store virtual disk as a single file".



17. Enter a unique name for the created disk file. The disk file will be stored under the entered file name.

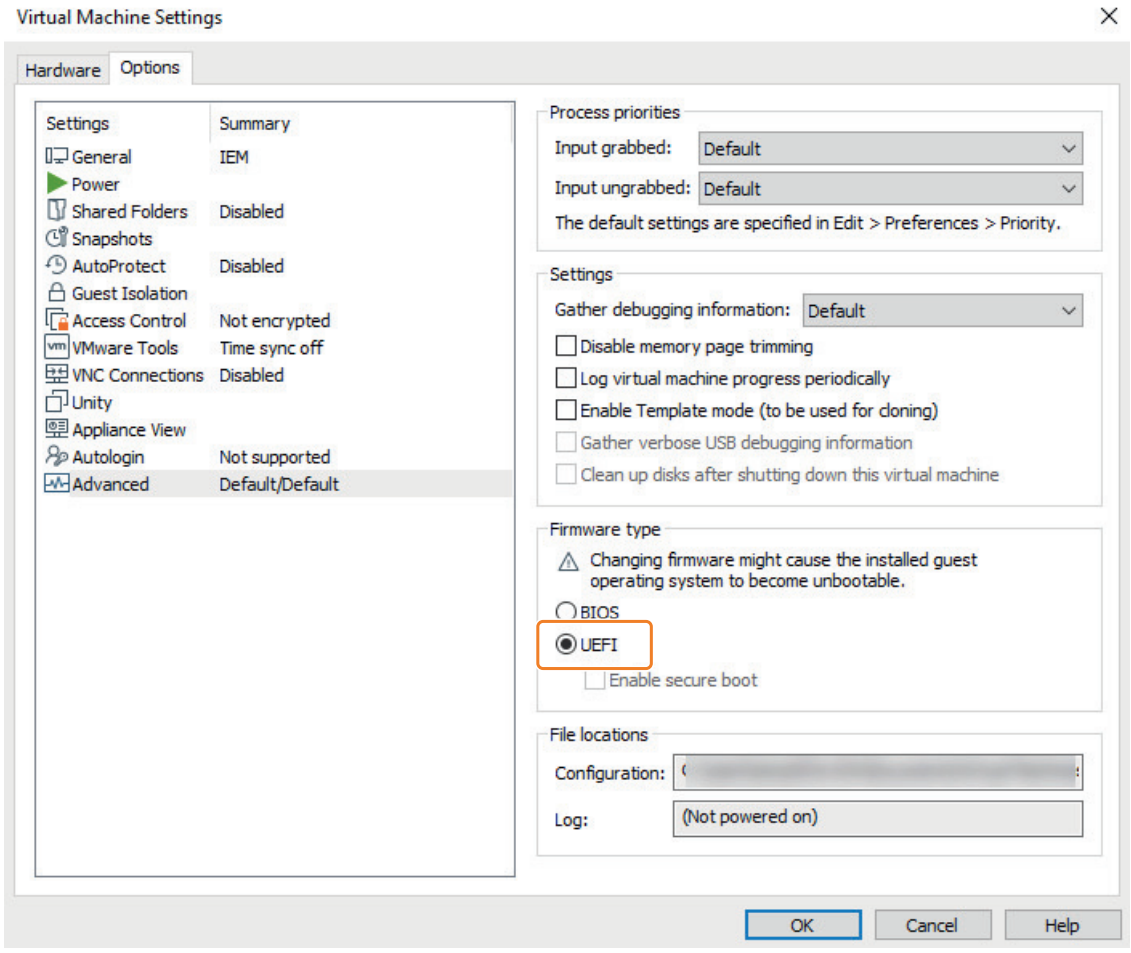


18. Click "Finish".
    The second hard disk is added to the hardware list in the left navigation.



19. Click the "Options" tab.
20. In the navigation on the left side, choose "Advanced".

21. Under the "Firmware type" section, select the "UEFI" checkbox.



22. Click "Ok".
    The VM is configured.

Note

Installed open-vm-tools

If open-vm-tools are installed, the IEM does not start after a reboot. When you want to use open-vm-tools, you must add the following configuration to the open-vm-tools config file ("tools.conf"):

```
[guestinfo]
exclude-nics=docker*,veth*
```

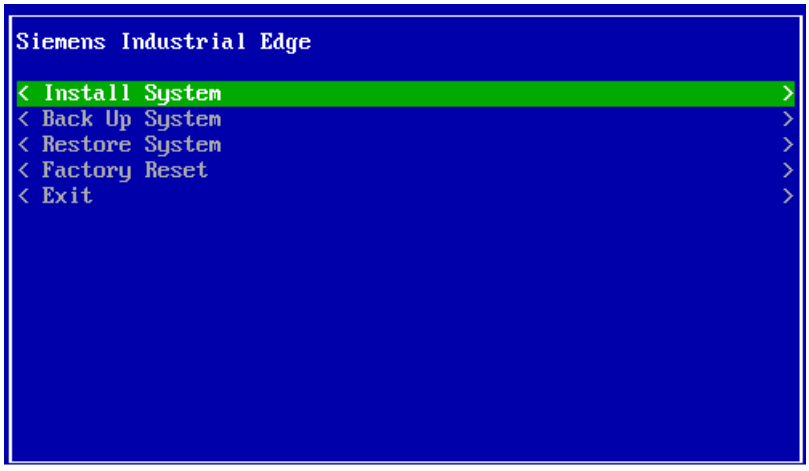
4.4.3 Installing the Industrial Edge Management OS

Requirement

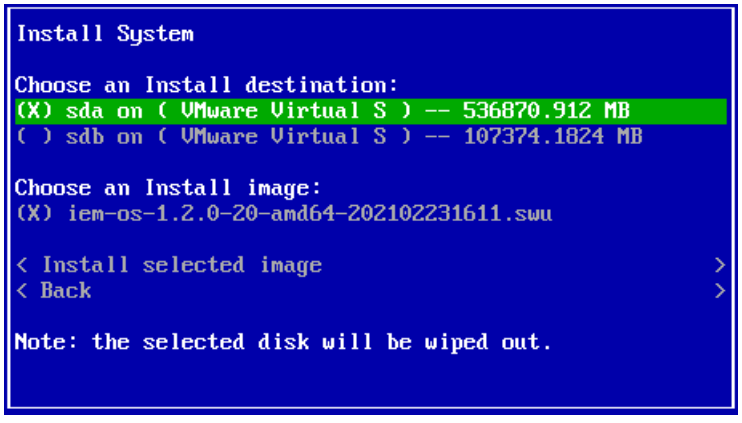
UEFI Boot is enabled in the VM settings.

Procedure

1. Start the VM.
   The "Siemens Industrial Edge" screen is displayed.



2. Select "Install System".
   The "Install System" screen is displayed.
3. Select the "sda" partition.



4. Select "Install selected image".

5. If Trusted Platform Module (TPM) is not enabled on the IEM host, select "Yes" to continue without TPM.

   Note

   No TPM enabled

   If Trusted Platform Module (TPM) is not enabled on the IEM host and you select "No", the installation of the Industrial Edge Management OS will not start.

   The installation of the Industrial Edge Management OS is starting.

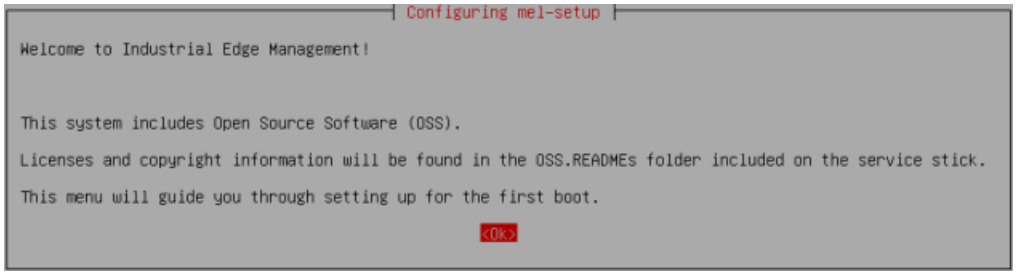
6. Wait until the installation is completed.
7. When the installation is completed, reboot the VM by selecting "Reboot".
   The VM is getting rebooted.

   Note

   Changing boot order

   When the "Siemens Industrial Edge" screen is displayed again after the reboot, you must change the boot order in the UEFI settings. Open the UEFI settings and set the disk at first place respectively the disk as boot disk in which the Industrial Edge Management OS has been installed.

   After the reboot is finished, the welcome screen is displayed through which you configure the IEM-OS.



   The "Configuring the Industrial Edge Management OS (Page 63)" subsection describes how to configure the IEM-OS.

4.5 Oracle VirtualBox

4.5.1 Creating the VM

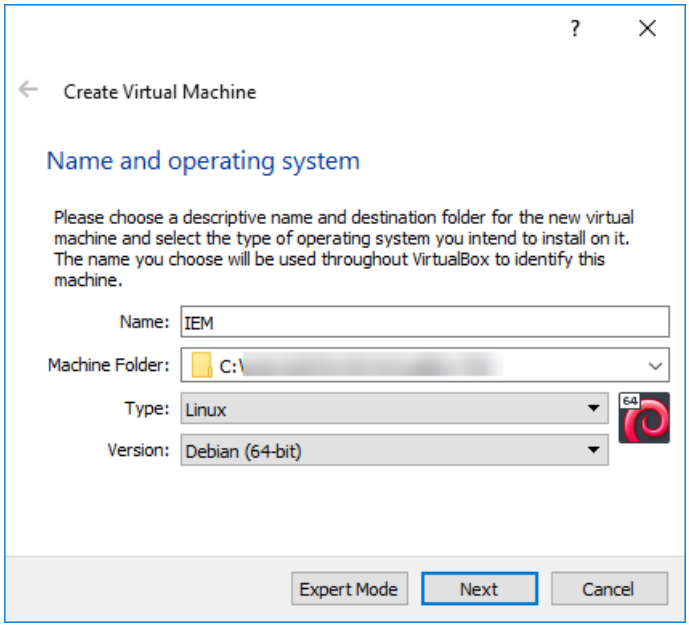
The following procedure describes the installation in the "Oracle VirtualBox" virtualization environment.

Requirement

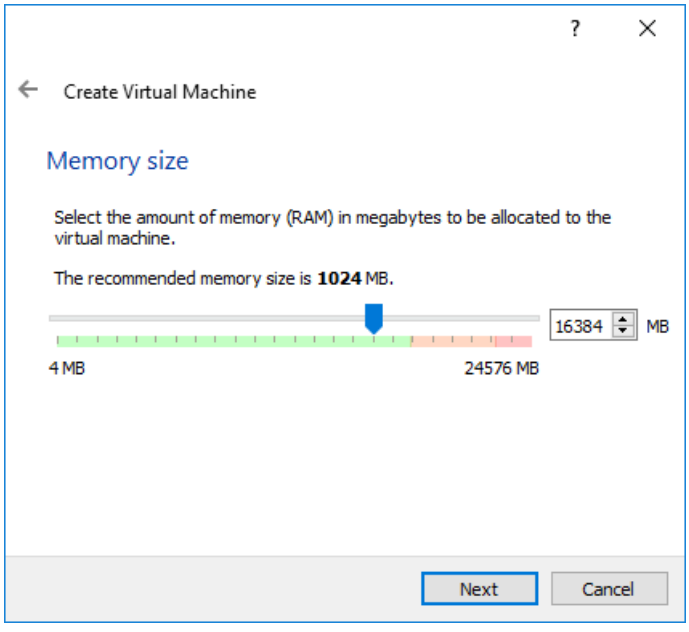
The ISO image of the IEM is downloaded to the PC.

Procedure

1. Open "Oracle VirtualBox".
2. Click "New".
   The "Create Virtual Machine" screen is displayed.
3. In the "Name" input field, enter the name for the VM.
4. From the "Type" drop-down list, select "Linux".
5. From the "Version" drop-down list, select "Debian(64-bit)".

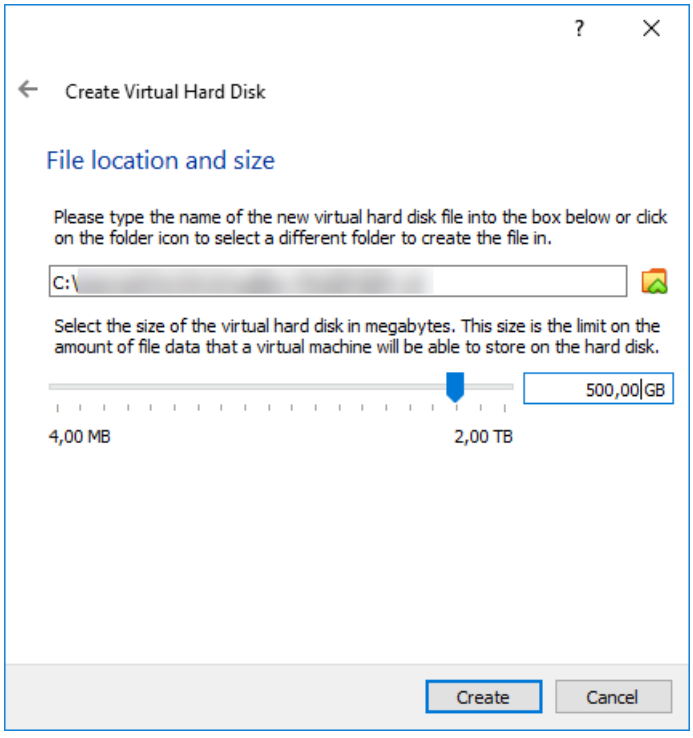


6. Click "Next".
7. For the memory amount allocated to the VM, set a minimum of 16 GB and click "Next".



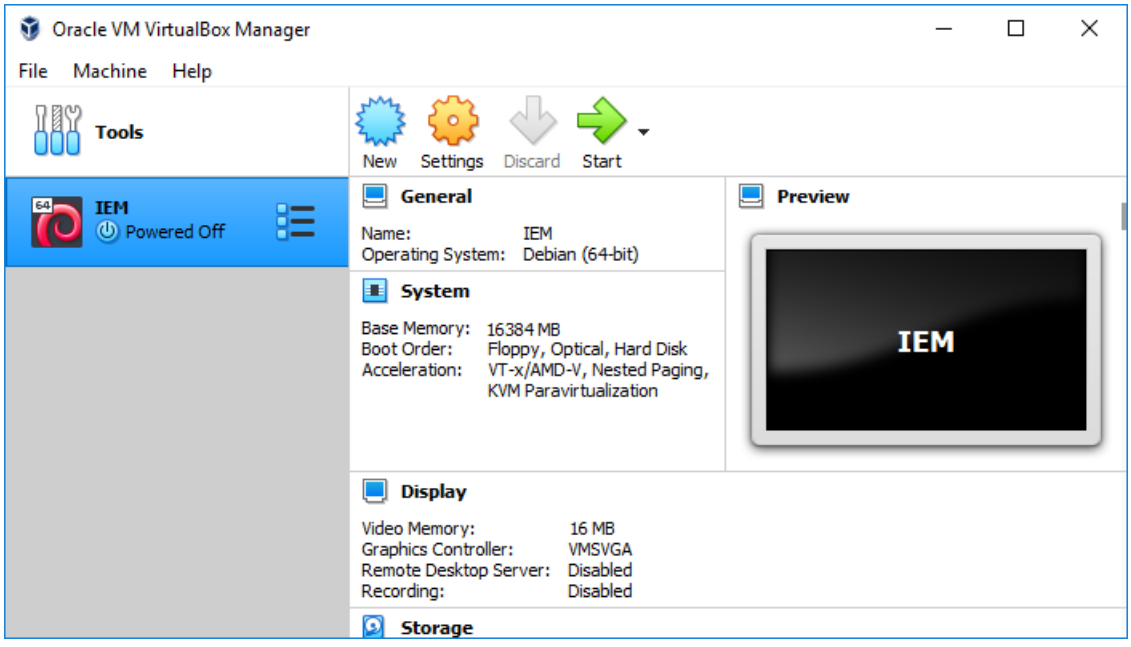
8. For the hard disk, select "Create a virtual hard disk now" and click "Create".
9. For the hard disk file type, select "VDI (VirtualBox Disk Image)" and click "Next".
10. For the storage on the physical hard disk, select "Dynamically allocated" and click "Next".
11. Choose a storage location for the hard disk file.

12. For the hard disk size, set a maximum disk size for the VM on the host PCs physical disk.



The disk is mandatory for the operating system and also stores app images and containers. The size of the disk depends on the apps and the apps sizes that you want to install. Siemens recommends a maximum disk size of 500 GB. A minimum of 50 GB is mandatory.

13. Click "Create".
The VM is created.



4.5.2 Configuring the VM

Requirement

If you use a "Bridged" network connection for your VM, you need 1 additional network interface.

Note

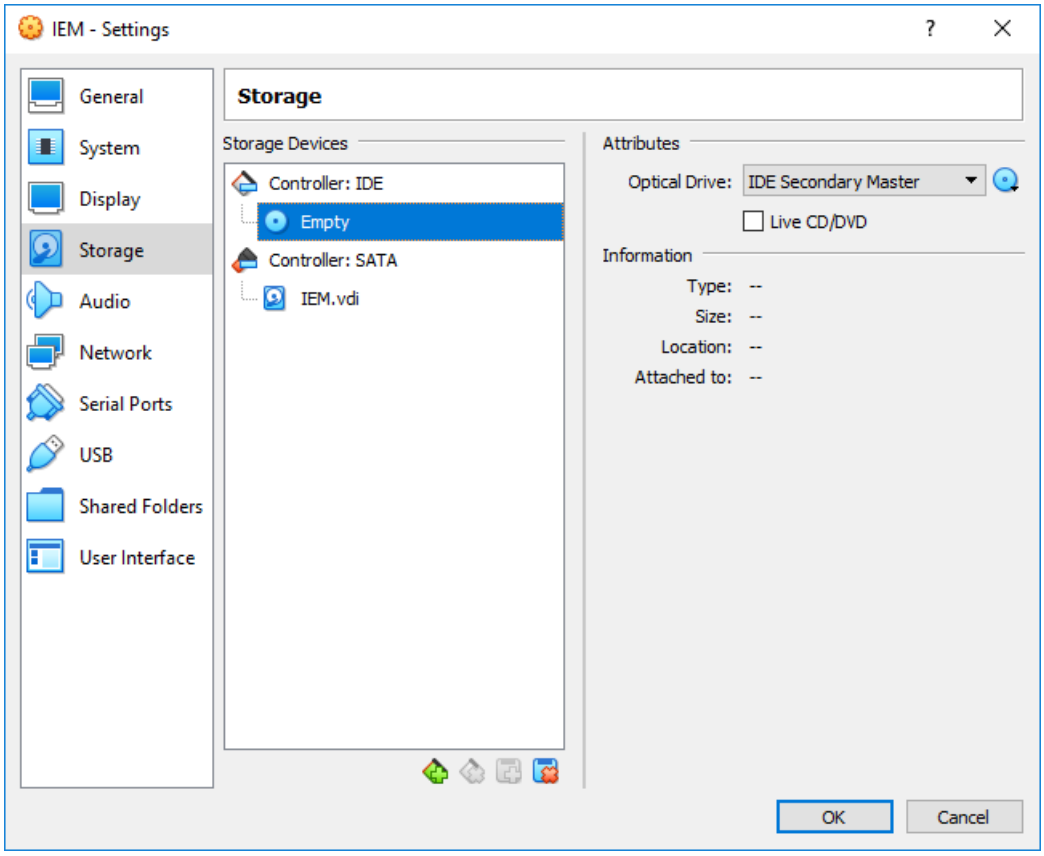
USB network adapter

The following procedure describes the use of an USB network adapter as additional network interface. Proceed in the same manner for other additional network interfaces.

Procedure

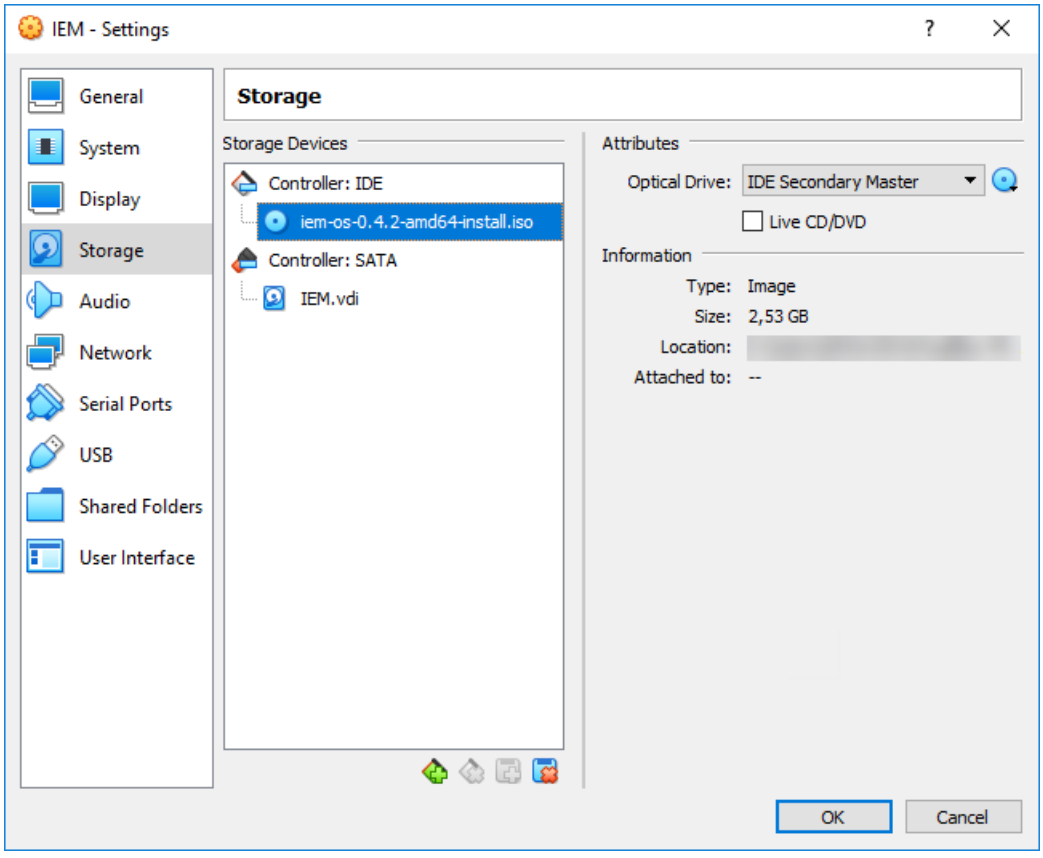
1. Select the created VM.
2. Click "Settings".
3. In the navigation on the left side, click "System".
4. Click the "Processor" tab.
5. For the number of processors, choose minimum 2 processor cores for the VM.
6. In the navigation on the left side, click "Storage".

7. Under "Controller: IDE", click "Empty".



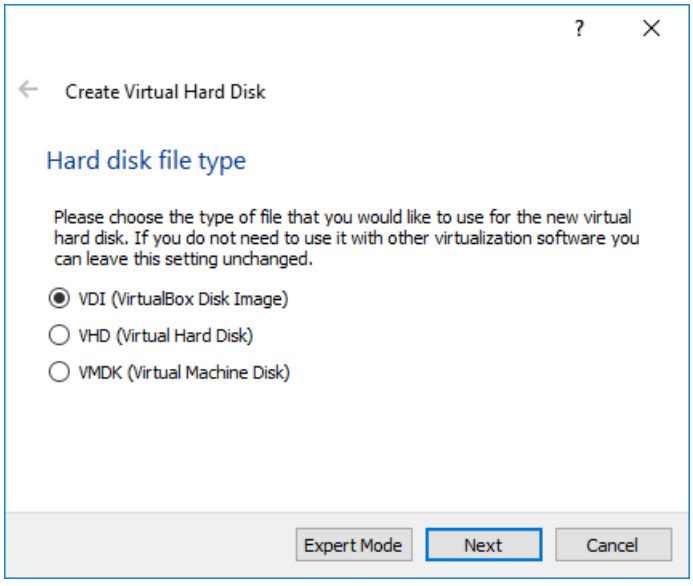
8. On the right side, click the icon.
9. Click the "Choose/Create a Virtual Optical Disk" command.
10. Click "Add" and browse the ISO image of the Industrial Edge Management.

11. Click "Choose".
    The selected ISO image is added under "Controller: IDE".

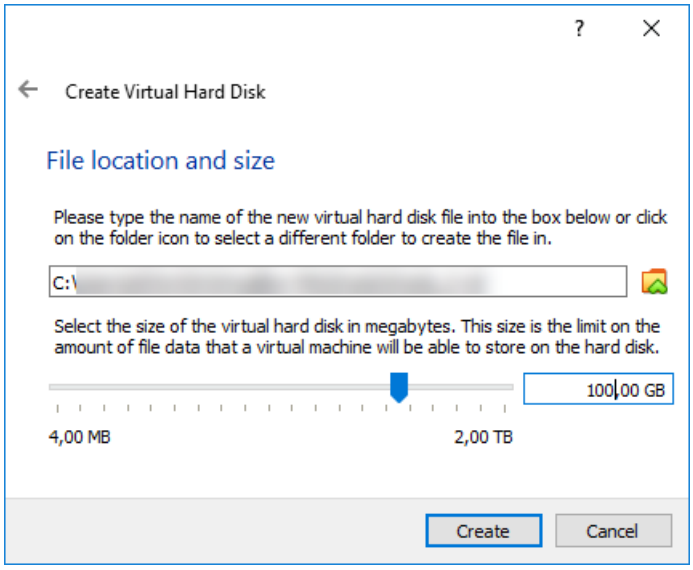


12. To add the second hard disk, select "Controller: SATA" and click the icon.
    The "Hard Disk Selector" screen is displayed.

13. Click "Create".
    The "Create Virtual Hard Disk" screen is displayed.



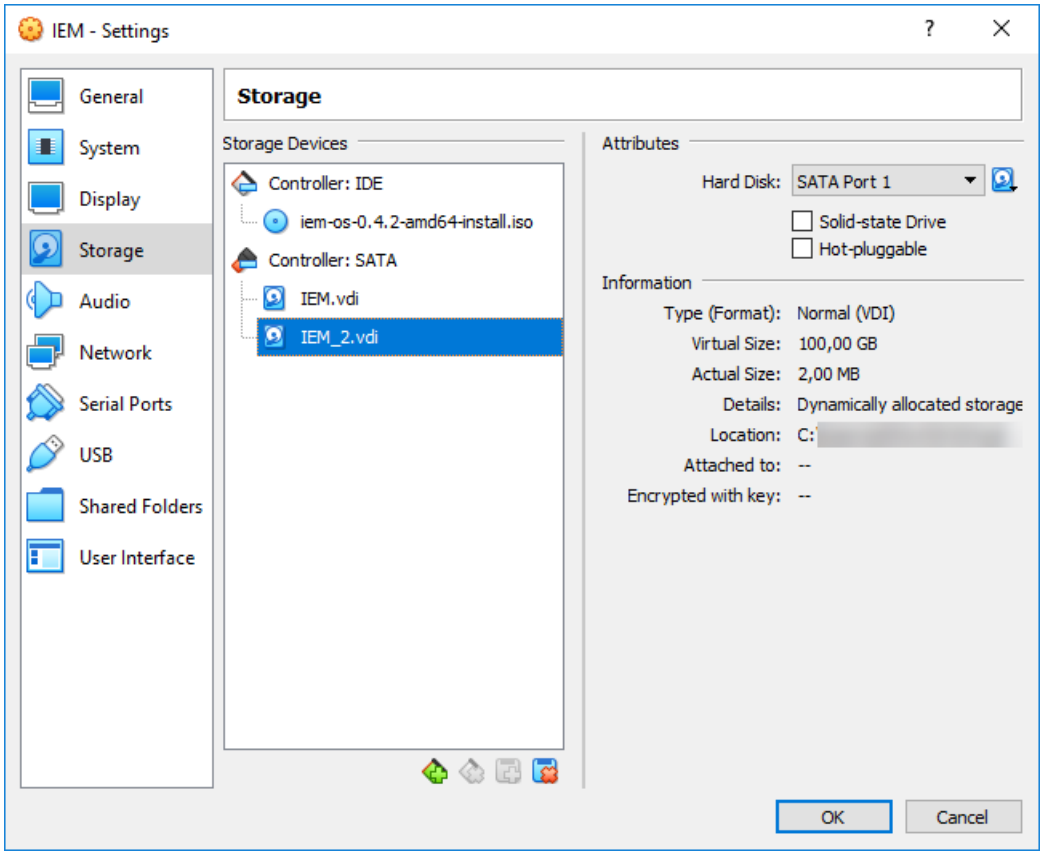
14. Select the "VDI (VirtualBox Disk Image)" check box and click "Next".
15. Select the "Dynamically allocated" check box and click "Next".
16. Select a maximum disk size that is lower than the disk size that you configured before.



The second hard disk is for the apps data storage.
Siemens recommends a maximum disk size of 100 GB for the second disk. A minimum of 50 GB is mandatory.

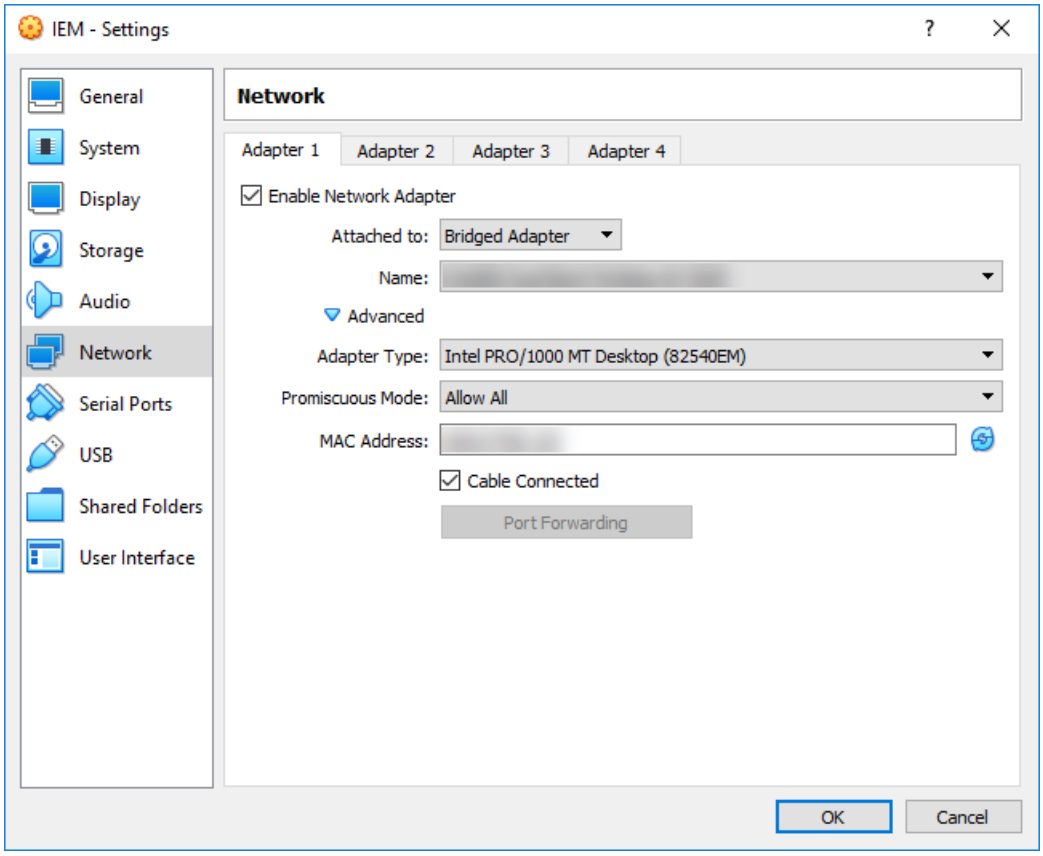
17. Click "Create".

18. Click "Choose".
    The second hard disk is added under "Controller: SATA".

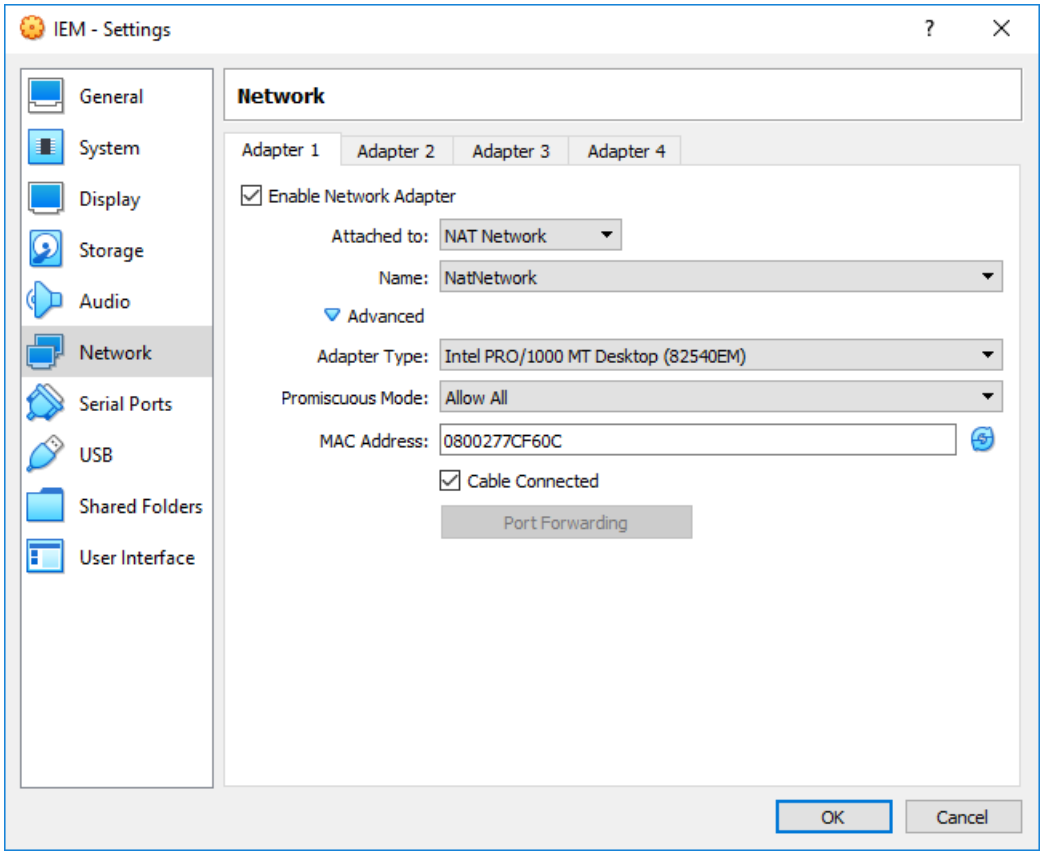


19. In the navigation on the left side, click "Network".

20. If you use a bridged network connection, the following settings must be configured under the "Adapter 1" tab:
    - Checkbox "Enable Network Adapter" selected
    - Attached to: "Bridged Adapter"
    - Name: Name of the additional network interface
    - Adapter type: Intel PRO/1000 MT Desktop (8254OEM)
    - Promiscuous Mode: Allow All
    - MAC Address: MAC address of the additional network interface
    - Checkbox "Cable Connected" selected



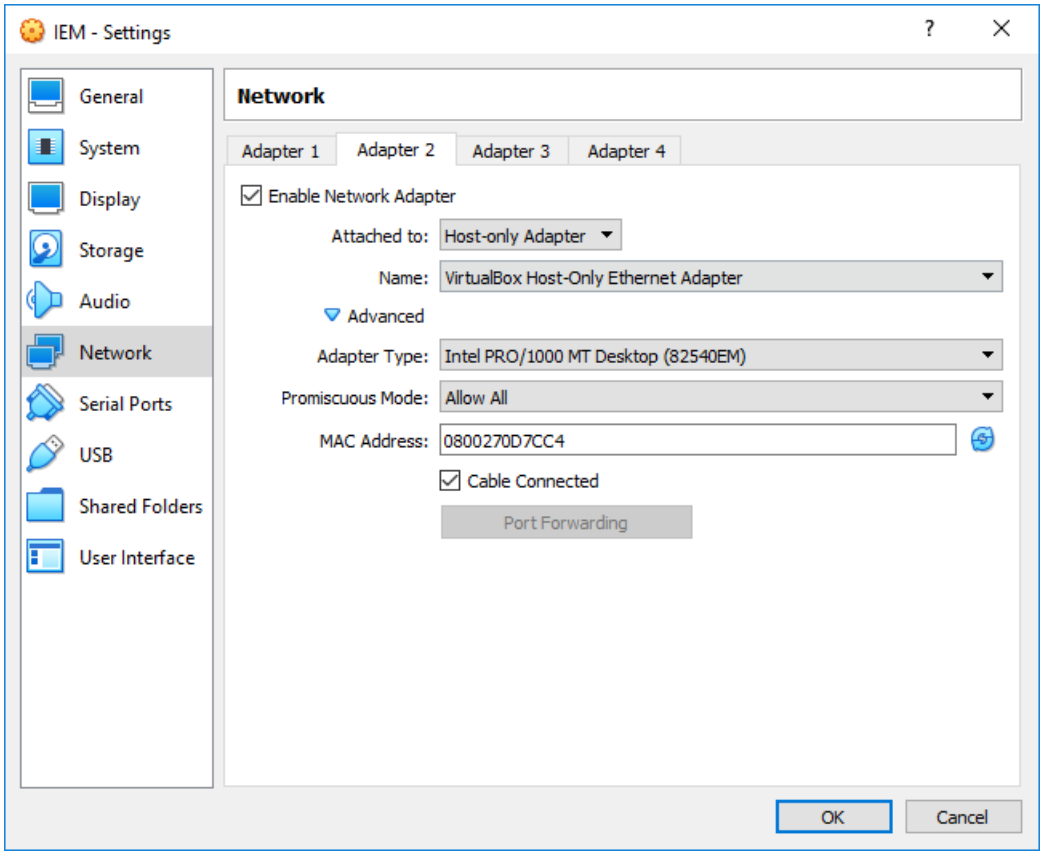
21. If you use a NAT network connection, the following settings must be configured under the "Adapter 1" tab:
    - Checkbox "Enable Network Adapter" selected
    - Attached to: "NAT Network"
    - Name: Name of the NAT network
    - Adapter type: Intel PRO/1000 MT Desktop (8254OEM)
    - Promiscuous Mode: Allow All
    - MAC Address: Random MAC address for the VM
    - Checkbox "Cable Connected" selected



For a NAT network connection, the following settings must be also configured under the "Adapter 2" tab:

- Checkbox "Enable Network Adapter" selected
- Attached to: "Host-only Adapter"
- Name: Name of the host network manager
- Adapter type: Intel PRO/1000 MT Desktop (8254OEM)
- Promiscuous Mode: Allow All
- MAC Address: Random MAC address for the VM

– Checkbox "Cable Connected" selected



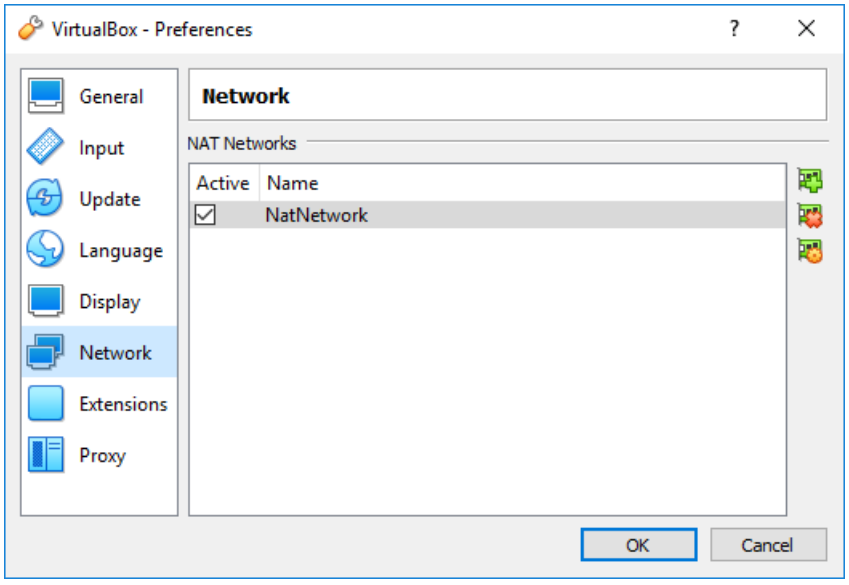
22. Click "OK".
    The VM is configured.

Creating a NAT network and a host network manager

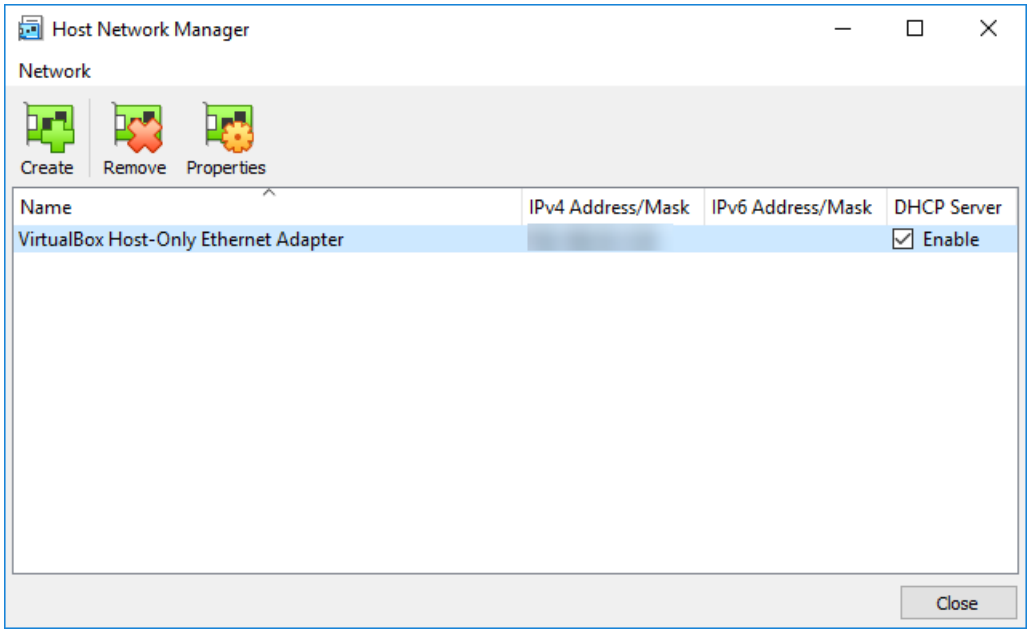
When you use a NAT network connection for the VM and neither NAT network nor host network manager are available, proceed as follows to create a NAT network and a host network manager:

1. Click the "File > Preferences" command in the "Oracle VM VirtualBox Manager" screen.
   The "Preferences" screen is displayed.
2. In the navigation, click "Network".

3. To create a new NAT network, click the icon.
   The NAT network is created.



4. Click "Ok".
5. Click the "File > Host Network Manager" command in the "Oracle VM VirtualBox Manager" screen.
   The "Host Network Manager" screen is displayed.
6. To create a new host network manager, click "Create".
   The host network manager is created.
7. To enable the host network manager, activate the "Enable" check box.

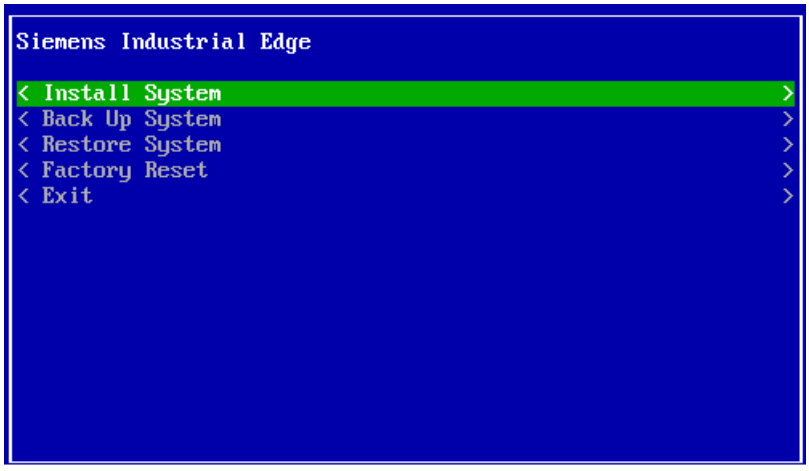


8. Click "Close".

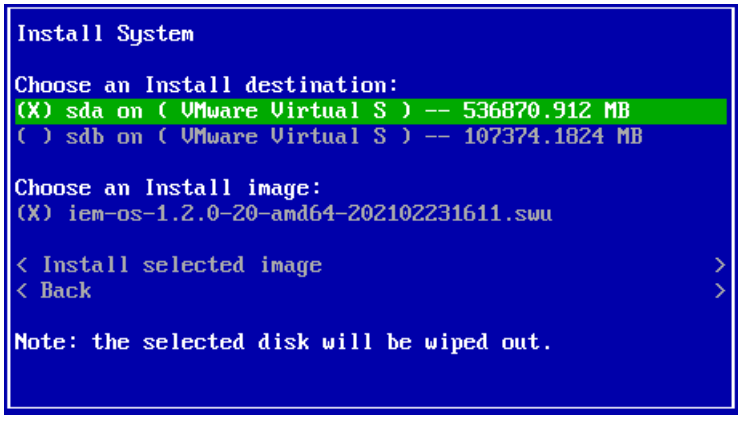
4.5.3 Installing the Industrial Edge Management OS

Procedure

1. Start the VM.
   The "Siemens Industrial Edge" screen is displayed.



2. Select "Install System".
   The "Install System" screen is displayed.
3. Select the "sda" partition.



4. Select "Install selected image".
5. If Trusted Platform Module (TPM) is not enabled on the IEM host, select "Yes" to continue without TPM.

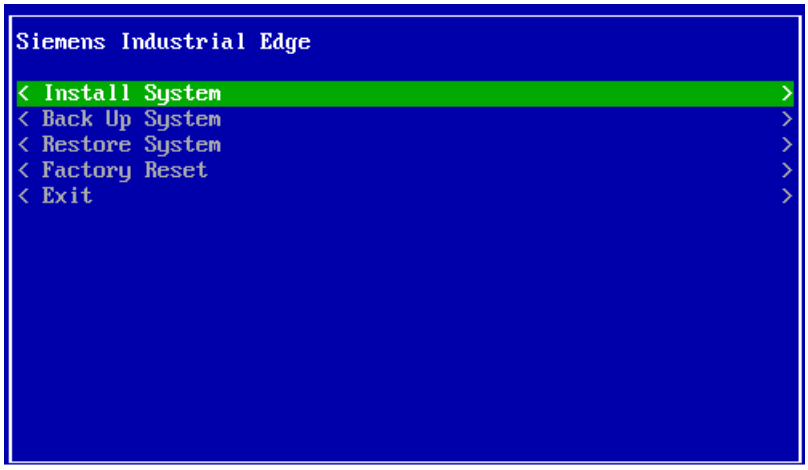
   Note

   No TPM enabled

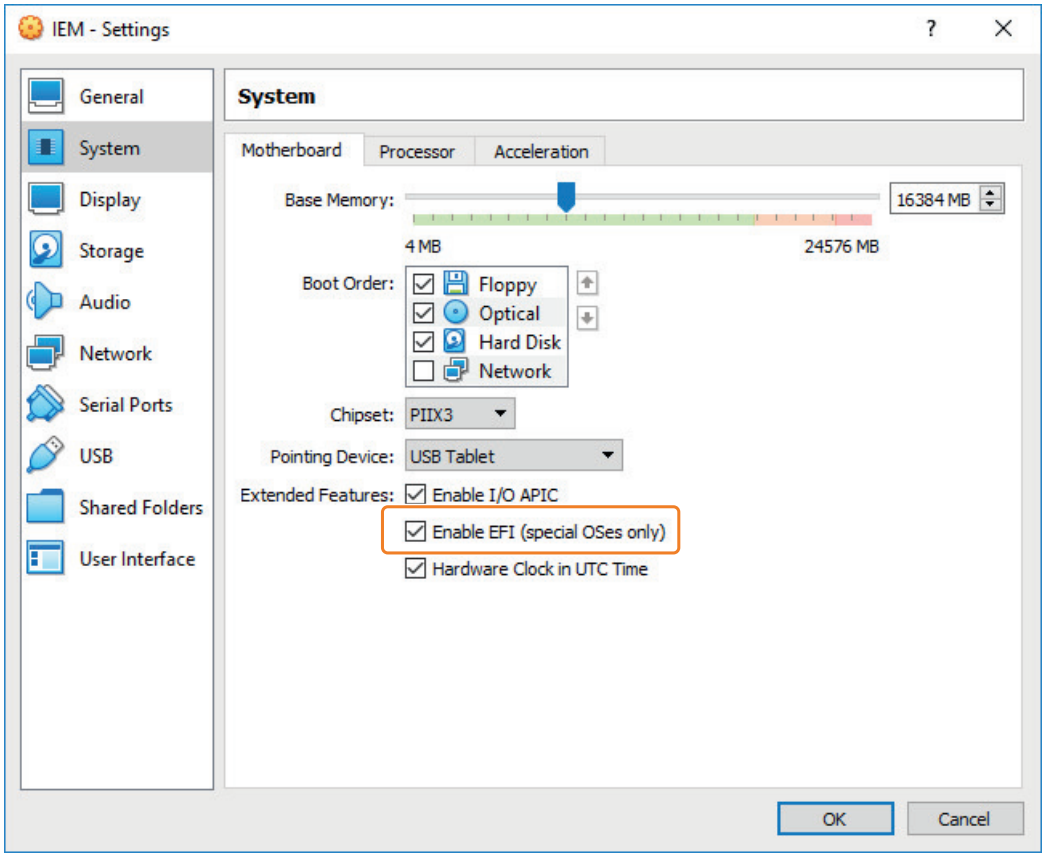
   If Trusted Platform Module (TPM) is not enabled on the IEM host and you select "No", the installation of the Industrial Edge Management OS will not start.

   The installation of the Industrial Edge Management OS is starting.
6. Wait until the installation is completed.

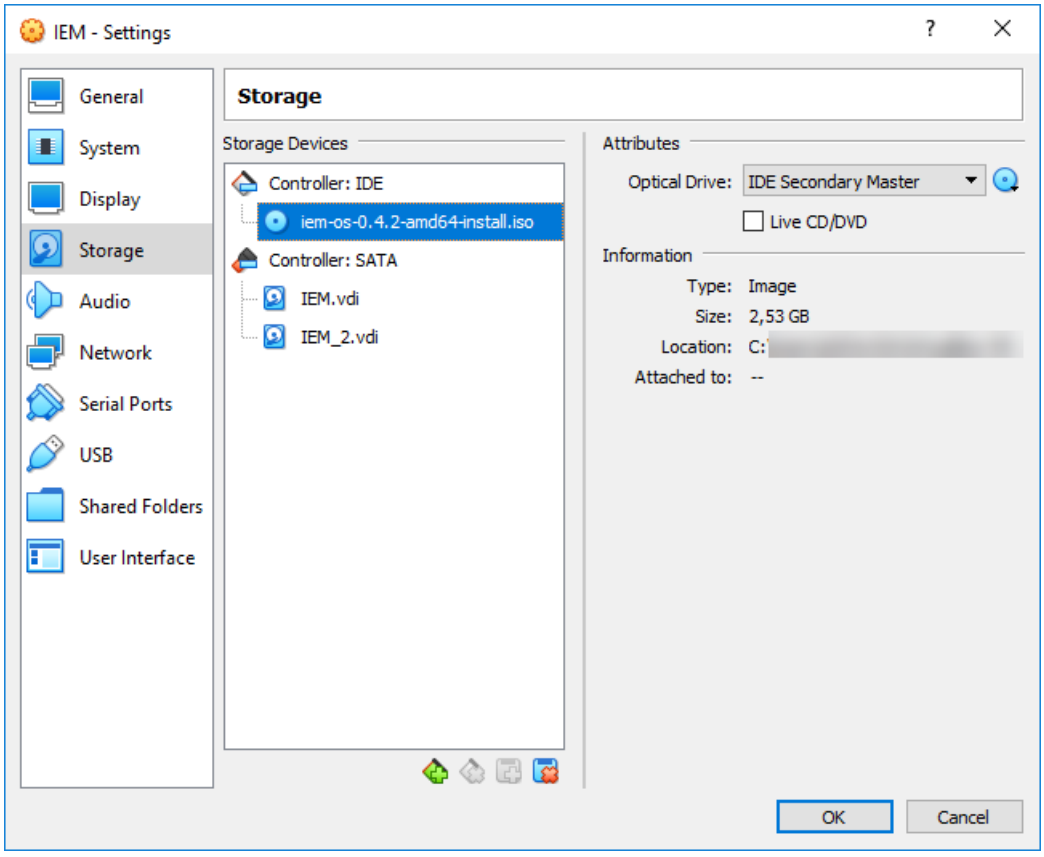
7. When the installation is completed, reboot the VM by selecting "Reboot".
   The VM is getting rebooted.
   When the VM is rebooted, the "Siemens Industrial Edge" screen is displayed again.



8. Close and shut down the VM.
9. After the VM is shut down, select the VM and click "Settings".
10. In the navigation on the left side, click "System".
11. Select the "Enable EFI (special OSes only)" check box.

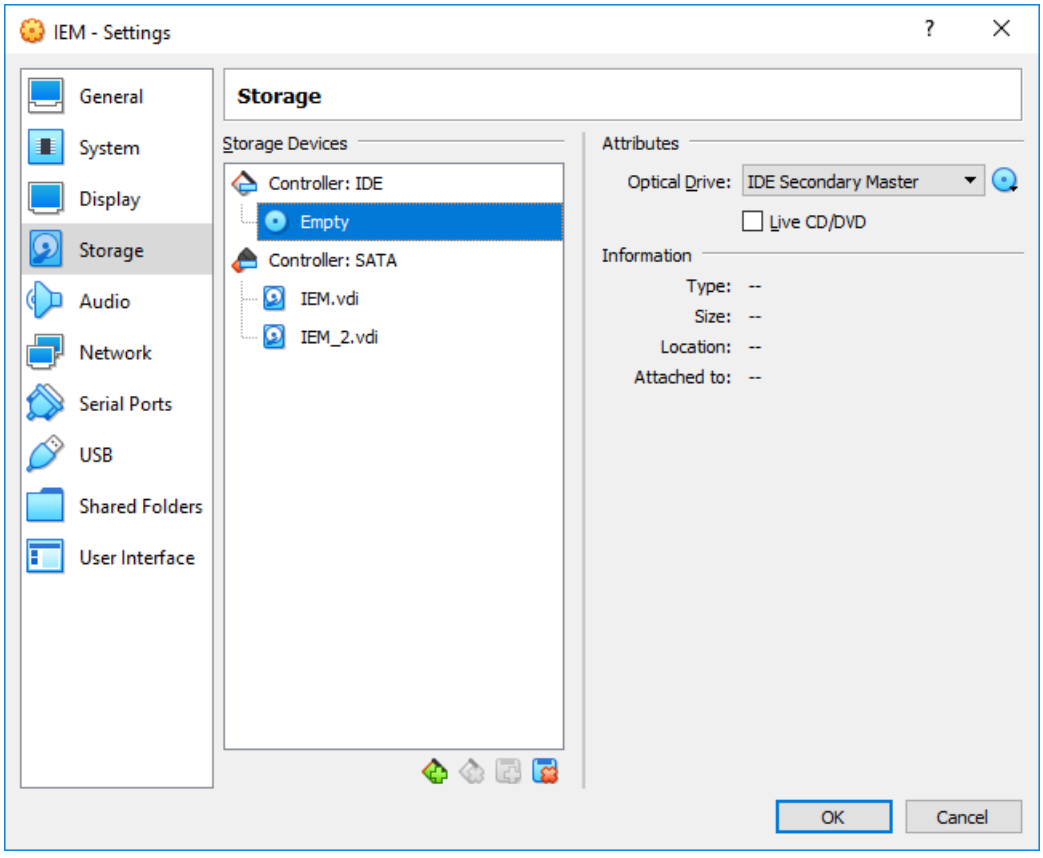


12. In the navigation on the left side, click "Storage".
13. Under "Controller: IDE", select the ISO image.



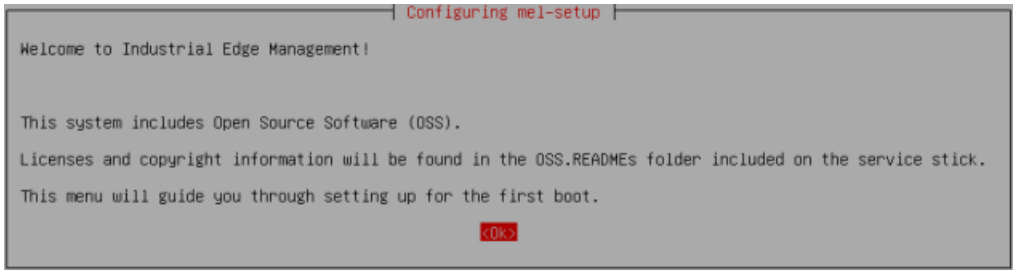
14. On the right side, click the icon.

15. Click the "Remove Disk from Virtual Drive" command.
    Under "Controller: IDE", "Empty" is displayed again.



16. Click "OK".

17. Start the VM.
    The welcome screen is displayed through which you configure the IEM-OS.

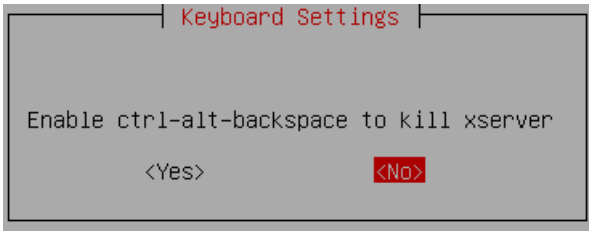


    The "Configuring the Industrial Edge Management OS (Page 63)" subsection describes how to configure the IEM-OS.

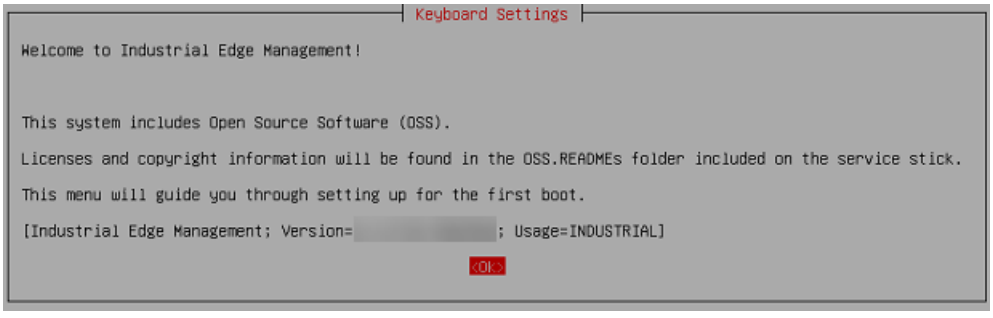
4.6 Configuring the Industrial Edge Management OS

Procedure

1. In the welcome screen, select "Ok".
2. Select the default "English: en_US.UTF-8" localization setting.
3. Select the default "pc105" keyboard model.
4. Select the default "us" keyboard layout.
5. Select the default "None" keyboard variant.
   You must select the default keyboard model, layout and variant. Otherwise you cannot install the IEM.
6. In the "Keyboard Settings", select "No" for ctrl-alt-backspace to kill xserver.

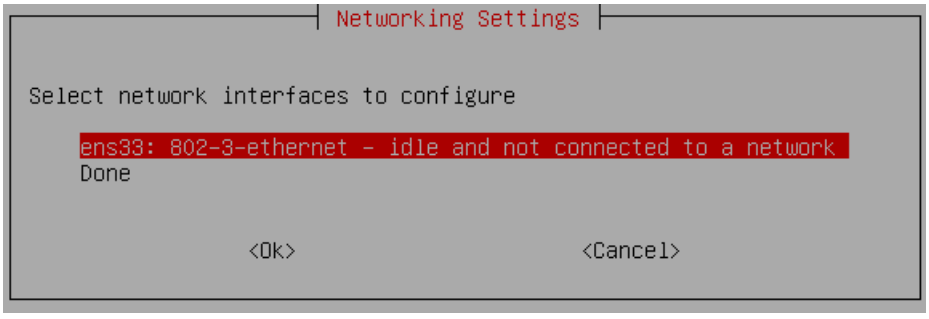


   An initialization is being performed. After the initialization process has been completed, an enhanced welcome screen is displayed.

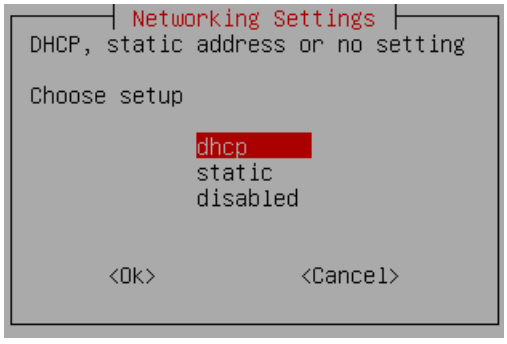


   The version of the IEM is displayed in the last row.

7. Select "OK".
   The "Network Settings" screen is displayed.



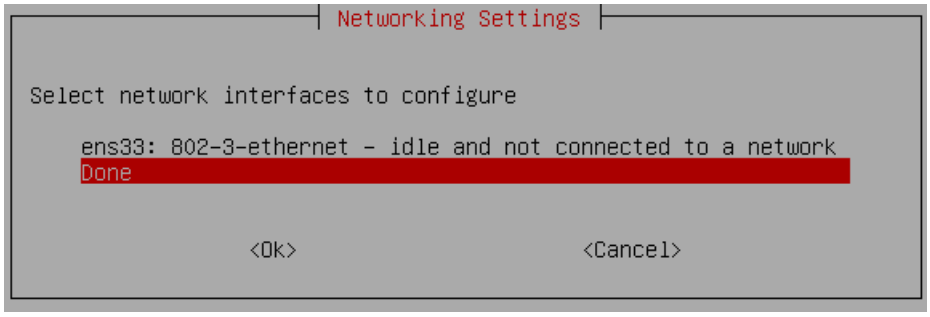
8. To start configuring your network settings, select the "ens33" network interface.
   The following screen is displayed.



9. Select your network settings as required.
   To select a network connection through DHCP, select "dhcp".
   To use a static IP configuration for the VM, select "static".
   When you choose a static IP configuration, enter the following information:
   - Static IP address
   - IP netmask
   - IP gateway
   - DNS server

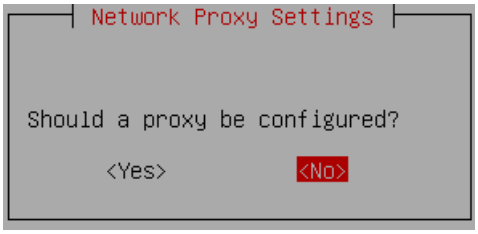
   After you have configured your network settings, the "Network Settings" screen is displayed again.

10. Select "Done".



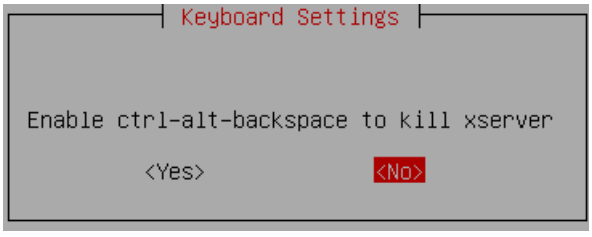
The "Network Proxy Settings" screen is displayed.

11. Select "No" for the configuration of a proxy.



To use a proxy server, you can set and configure a proxy server in the Industrial Edge Management UI.
The "Localization Settings" screen is displayed.

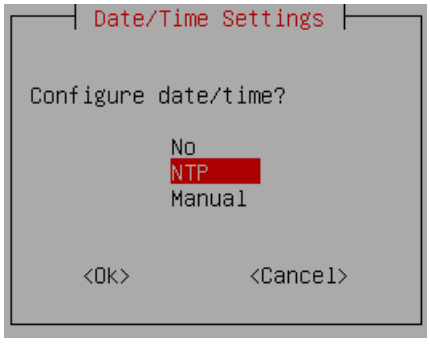
12. Select the default "English: en_US.UTF-8" localization setting.
13. Select the default "pc105" keyboard model.
14. Select the default "us" keyboard layout.
15. Select the default "None" keyboard variant.
16. In the "Keyboard Settings", select "No" for ctrl-alt-backspace to kill xserver.



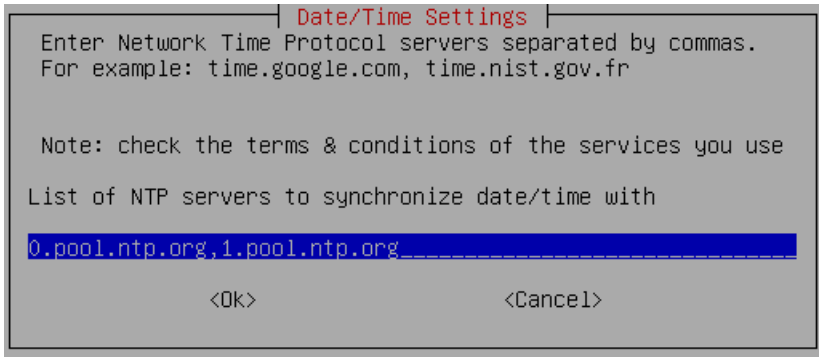
The "Timezone Settings" screen is displayed.

17. Select the "UTC" timezone.
You must select the "UTC" timezone. Otherwise you cannot install the IEM.

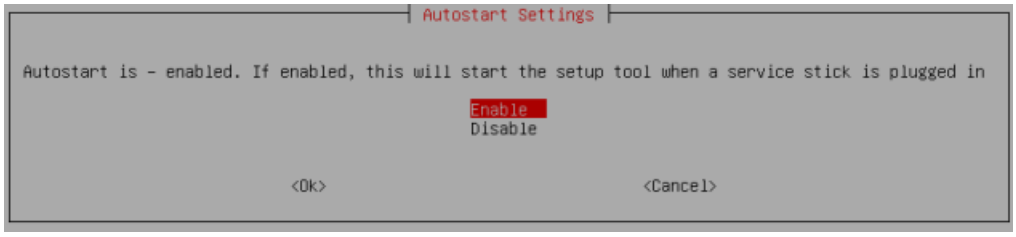
18. Select "OK".
    The "Date/Time Settings" screen is displayed.



19. Use an NTP server by selecting "NTP".
20. Enter the NTP server.
    Do not use a blank between separated NTP servers but just a comma.



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 mandatory.
After you have entered an NTP server, the "Autostart Settings" screen is displayed.



21. To lock the settings, select "Disable". To allow reconfiguration of the setup, select "Enable".

Note

Reconfiguration of the setup

After you have set up the IEM-OS, you can recall and reconfigure the setup by hotplugging the installation medium. For that, select "Enable".

The setup is being performed.
When the setup is completed, the following screen is displayed.

22. Select "Ok".
The VM is getting rebooted. This may take up to 10 minutes. When the reboot is finished, the login screen is displayed.

The configuration of the IEM-OS is completed.

Note

NAT network connection in Oracle VirtualBox

In case you use Oracle VirtualBox and a NAT network connection, 2 IP addresses are displayed. To set up the Industrial Edge Management, use the second displayed IP address.

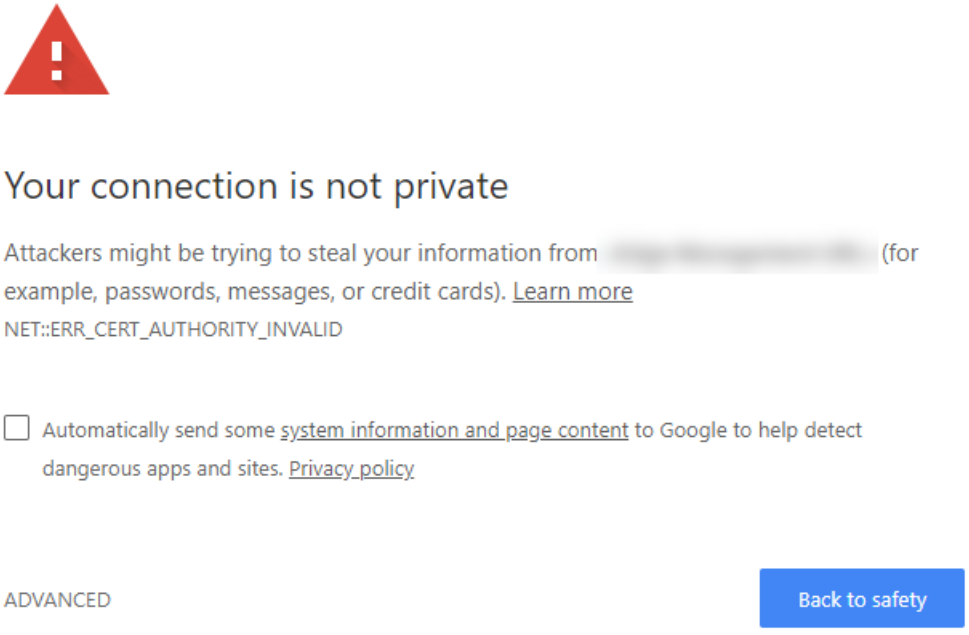
4.7 Activating & Installing the Industrial Edge Management

4.7.1 Activating the Industrial Edge Management

To activate and install the IEM, use an Internet browser on a client that is in the same network and subnet as the VM.

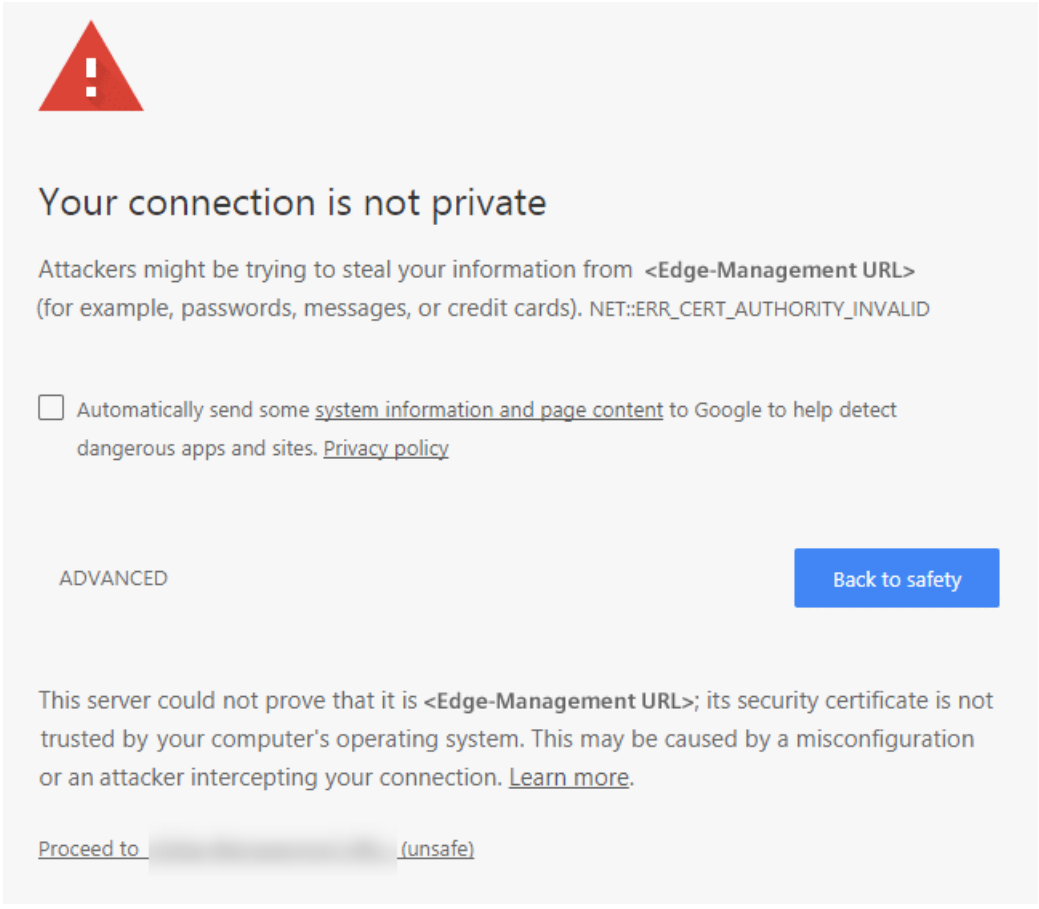
Procedure

1. Enter the IP address of the VM respectively of the IEM-OS UI in the HTTPS protocol into an Internet browser, for example "https://178.123.11.54".
   The IP address is shown in the login screen in the VM.
   A certificate warning is displayed.

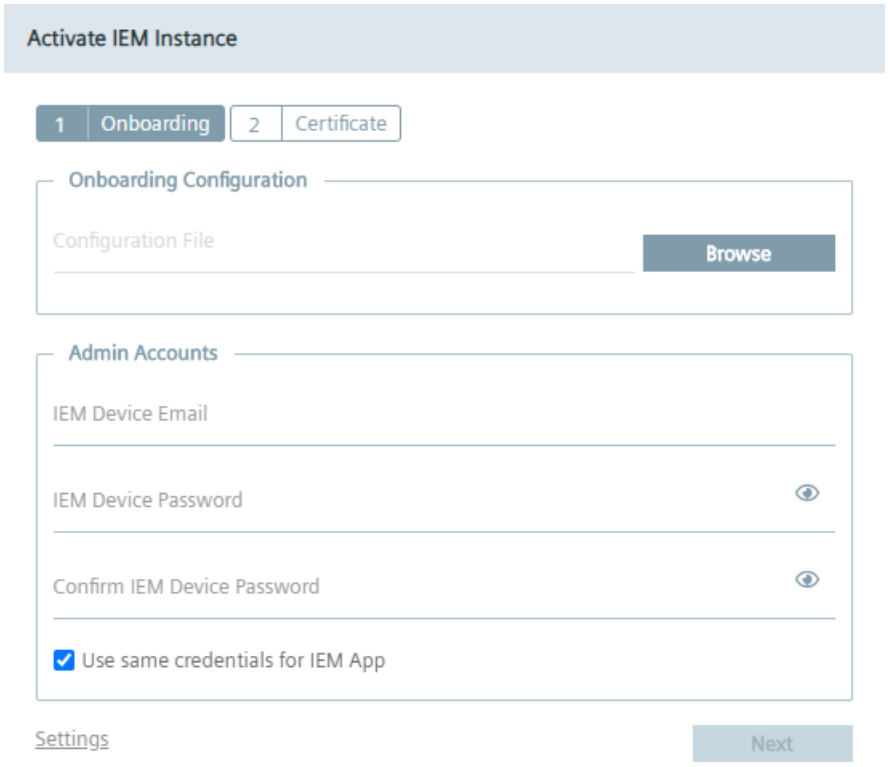


2. Click "Advanced".

3. To connect to your IEM-OS UI, click "Proceed to <IP address>".

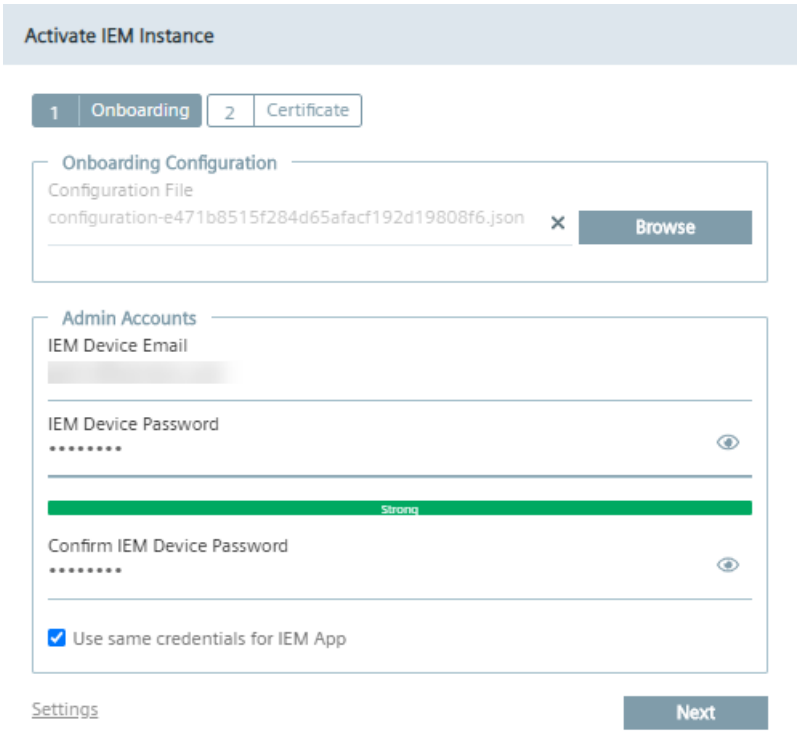


The "Activate IEM Instance" screen is displayed.



4. In the "Onboarding Configuration" section, click "Browse" and select the downloaded IEM configuration file that you created in the Industrial Edge Hub.
   This IEM configuration file contains a key that is just valid for 1 hour. After 1 hour, the configuration file is expired and you have to download a new IEM configuration file.
5. In the "Admin Accounts" section, create an admin user for the IEM-OS by entering the email address and password of the admin user.
   The password must meet the following criteria:
   - Minimum 8 characters
   - Minimum 1 upper case letter
   - Minimum 1 special character
   - Minimum 1 number

6. If you want the admin user for the IEM-OS to be also the admin user for the IEM, activate the "Use same credentials for IEM App" check box.



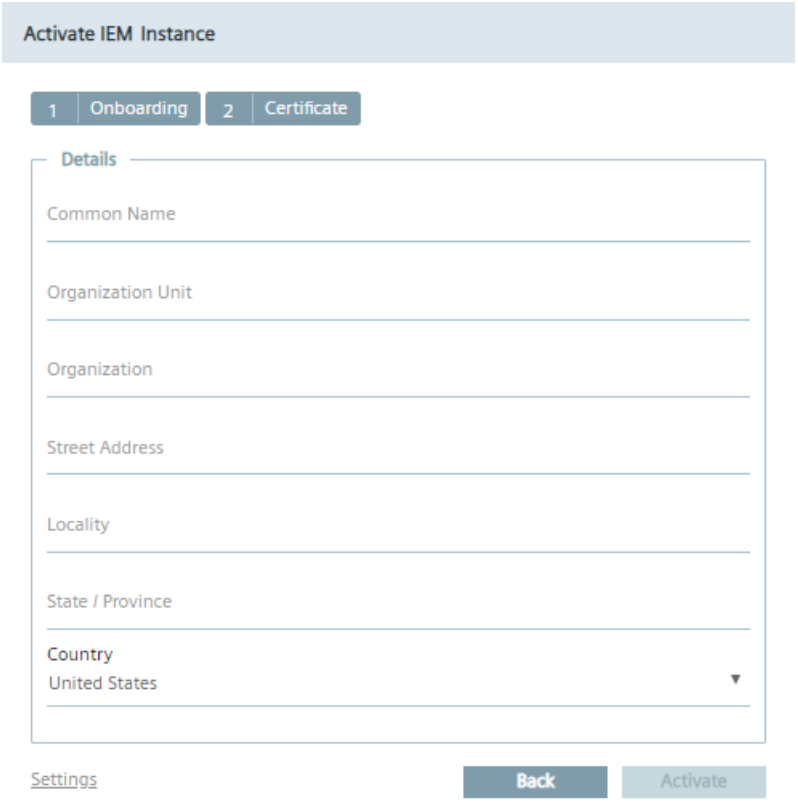
7. If you want to create a different admin user for the IEM, disable the "Use same credentials for IEM App" check box and enter the email address and password of the admin user for the IEM in the "IEM App Email" and "IEM App Password" input fields.
Creating an admin account for the IEM-OS and for the IEM is mandatory.

Note

Resolved DNS entries

If you want to use resolved DNS entries for domain names to access the IEM, ensure to resolve the DNS entries in the cloud or configure the local DNS server. Before you create the IEM-OS, add the DNS server addresses to the network settings by clicking "Settings" and then clicking the edit icon under the "LAN" tab.

8. After configuring the settings, click "Next".
   The "Certificate" tab is displayed.

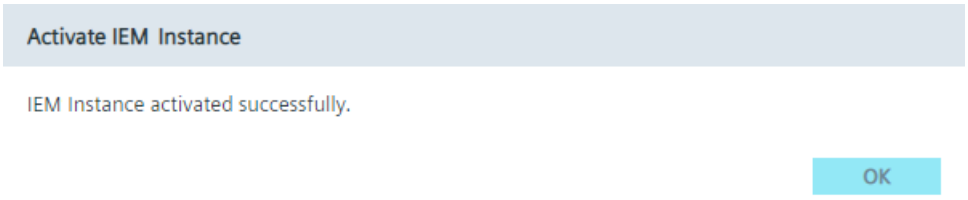


9. In the "Common Name" input field, enter the Fully Qualified Domain Name (FQDN).
   The IEM checks the "Common Name" which must correspond to the host respectively to the FQDN of the IEM. Typically, the FQDN is composed of the host domain name. The FQDN is used to generate a rootCA on the IEM-OS for the following purposes:
   - Generating certificates to configure the Edge Device's reverse proxy server TLS settings.
   - Generating certificates to configure the IEMs reverse proxy server TLS settings if the IEM is set up with default settings.
   - Generating certificates to configure the IEM-OSs reverse proxy server TLS settings.

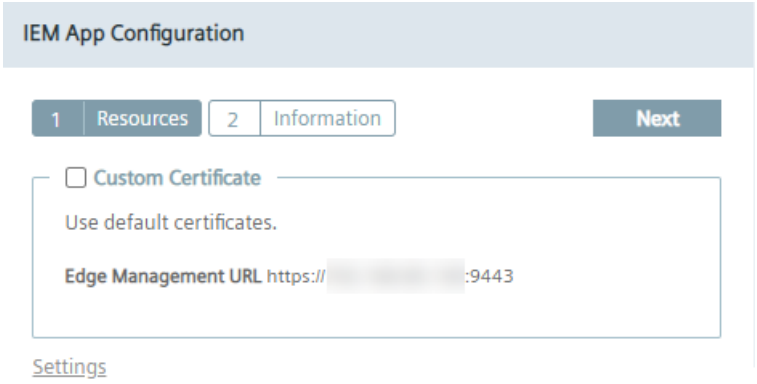
   The "Common Name" input field is mandatory, the other input fields are optional.
10. Before activating the IEM instance, configure the system settings respectively ensure that your settings are correct by clicking "Settings".
    You can configure the following settings:
    - Network
    - Proxy server
    - Docker network
    - NTP server

    You find more information on the system settings in the "Settings (Page 73)" subsection.

11. Click "Activate".
    When the activation of the IEM instance was successful, an according screen is displayed.



12. Click "OK".
    You will be redirected to the "Sign in" screen.
13. Sign in with the admin user for the IEM-OS that you created during the setup.
    The "IEM App Configuration" screen is displayed.



4.7.2 Settings

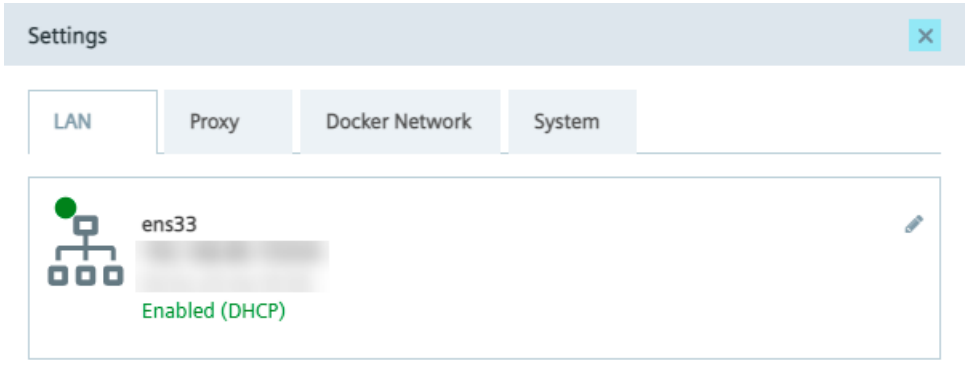
You can edit the following settings before you install the Industrial Edge Management:

- Network settings
- Proxy settings
- Docker network settings
- NTP settings

4.7.2.1 Editing network settings

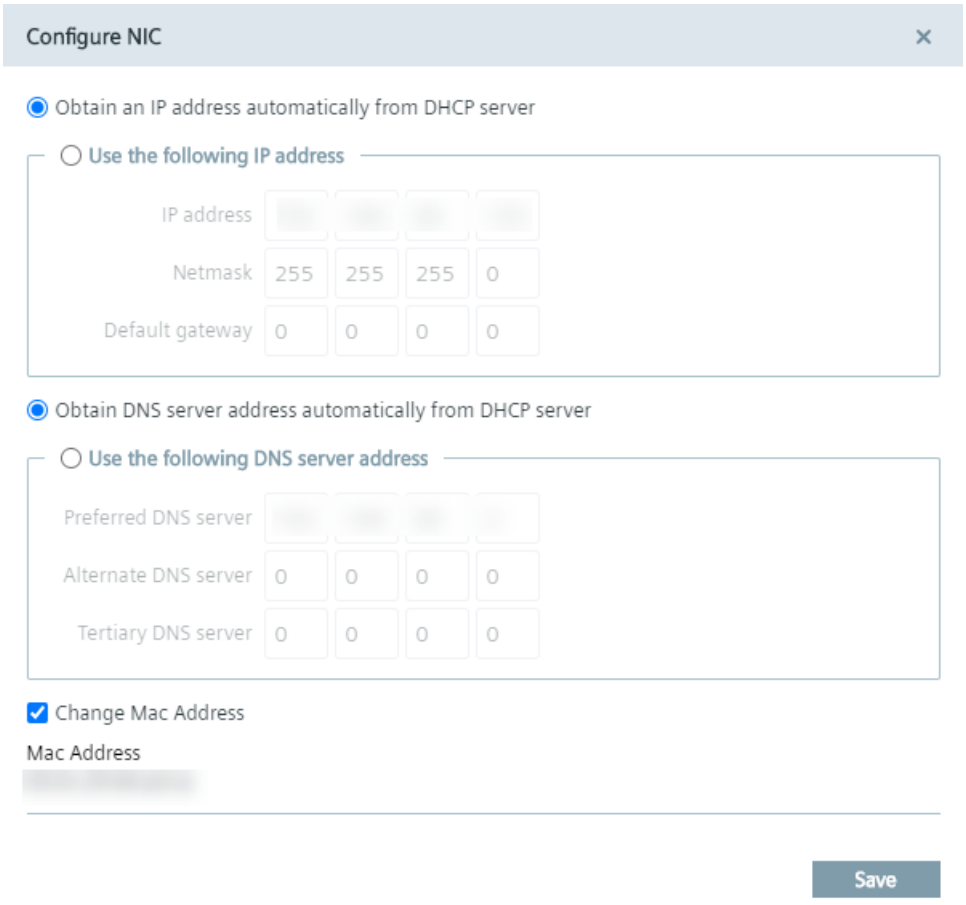
Procedure

1. In the "Activate IEM instance" screen, click "Settings".
   The "Settings" screen is displayed.



   In the "LAN" tab, the configured network settings are displayed.

2. To edit the network settings, click the icon.
   The "Configure NIC" screen is displayed.



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

   Note

   Resolved DNS entries

   If you want to use resolved DNS entries for domain names to access the IEM, ensure to resolve the DNS entries in the cloud or configure the local DNS server. Before you create the IEM-OS, add the DNS server addresses to the network settings.

4. If you want to use a specific MAC Address, activate the "Change Mac Address" check box and enter the desired MAC address.
5. Click "Save".

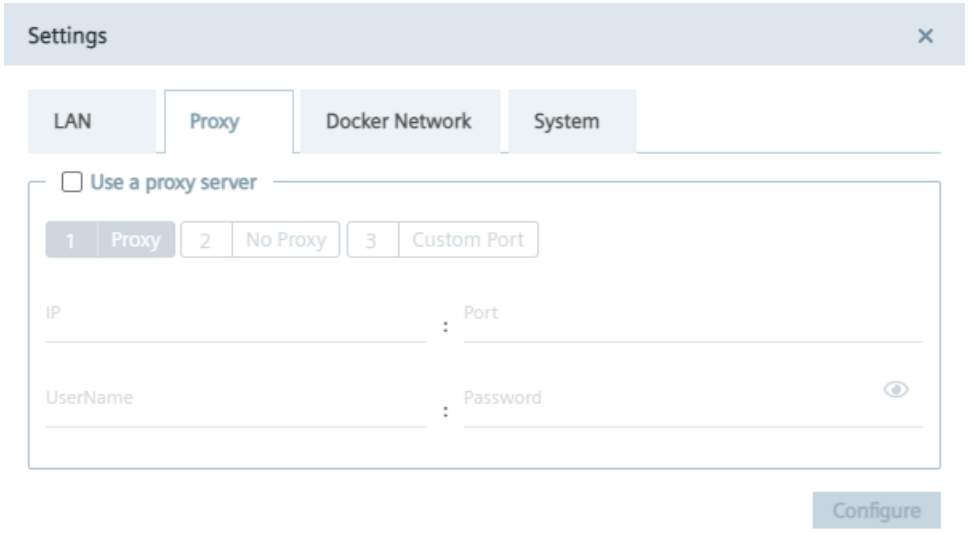
4.7.2.2 Setting up a proxy server

With the use of a proxy server, the admin of the IEM (and of Edge Devices) can add, edit and remove proxy rules to redirect specific data traffic. The admin can also disable redirection of specific data traffic through the proxy.

App developers do not need to implement their own proxy settings. The proxy settings described in this procedure apply for all IEM components.

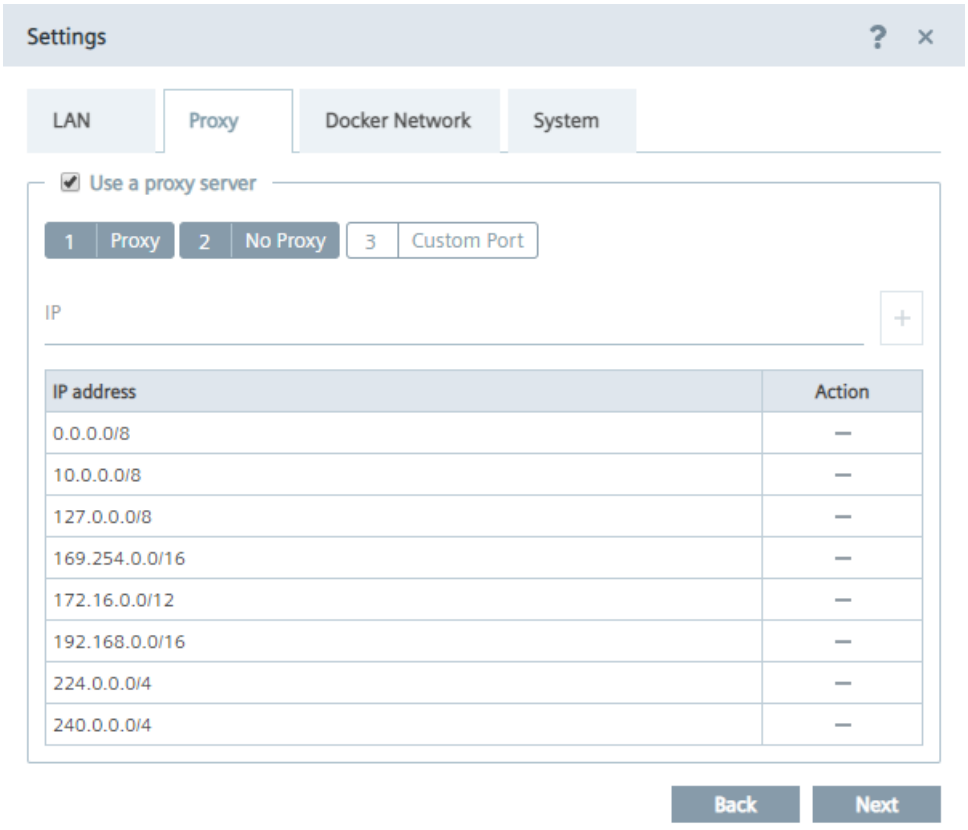
Procedure

1. Click the "Proxy" tab.



2. To use a proxy server, click the "Use a proxy server" check box.
   The input fields for the proxy server settings are enabled.
3. Enter the IP address and the corresponding port of the proxy server in the according input fields.
4. If needed, enter username and corresponding password in the according input fields in case of an additional authentication for the proxy server.
   The settings apply for HTTP and HTTPS proxy servers.

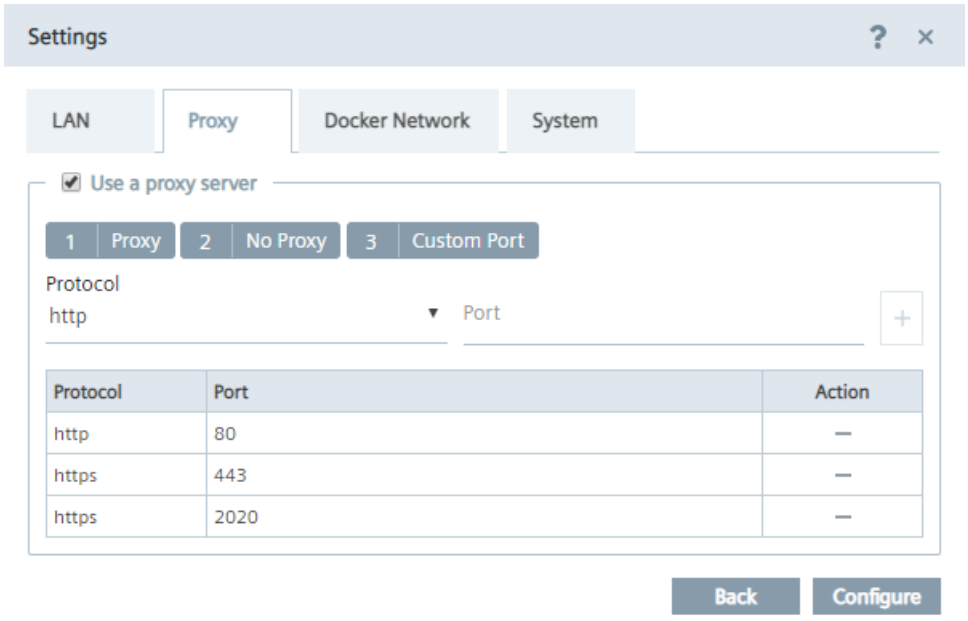
5. Click "Next".
   The "No Proxy" tab is displayed.



   In the "No Proxy" tab, add all the IP addresses which shall be accessed directly (without use of proxy).
   By default, several no proxy addresses are listed which are required by the IEM.

6. If you want to add a further IP address which shall be accessed directly, enter the IP address or domain of the no proxy address in the "IP" input field and click the + icon.
   The address is added to the no proxy list.
   When you use a proxy server to connect to the IEM after you have installed the IEM, you must add the "Edge Management URL" and "Edge Management Hub URL" name of the IEM to the no proxy address list. Otherwise, several errors can occur when you use the IEM.

7. Click "Next".
   The "Custom Port" tab is displayed.



   In the "Custom Port" tab, you configure ports for apps which use the configured ports for outgoing communication through the proxy on HTTPS or HTTP protocols.
   By default, several ports are listed which are required by the IEM.

Note

Default no proxy addresses and ports

The default no proxy addresses and ports are essential for running the IEM and cannot be deleted.

8. If you want to add a further port, select the required protocol from the "Protocol" drop-down list and enter the required port.
9. To add the port, click the + icon.
   The port is added to the port list.
10. To add the proxy settings, click "Configure".
11. Confirm the proxy settings by clicking "Ok".
    The proxy settings are saved.

Note

Setting up a proxy server after IEM installation

You can also configure and update the proxy settings after the IEM installation. In the IEM-OS UI, navigate to the "Settings > Connectivity > Proxy" section and set the proxy settings.

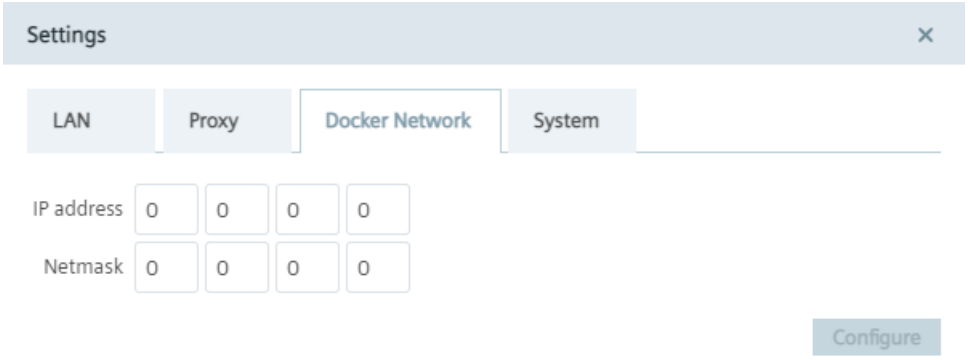
4.7.2.3 Configuring the Docker network

By default, the Docker server creates and configures the host system's network interface called docker0. The Docker server configures the docker0 network with an IP address, a netmask and an IP allocation range. The default docker0 network range is 172.17.0.0/16. If this network range conflicts with the existing system's network configuration, certain services do not work and you are not able to access the IEM-OS UI in a browser.

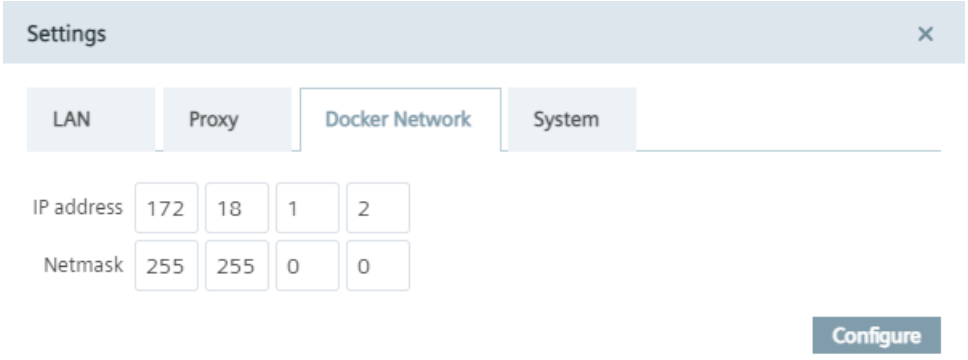
To prevent this scenario, you can configure the docker0 network range as described in the following.

Procedure

1. In the "Settings" screen, click the "Docker Network" tab.



2. In the "IP address" input field, enter the IP address that you want to use for the docker0 network.
   The IP address of the docker0 network is the start of the docker0 network.
3. In the "Netmask" input field, enter the subnet mask of the docker0 network.

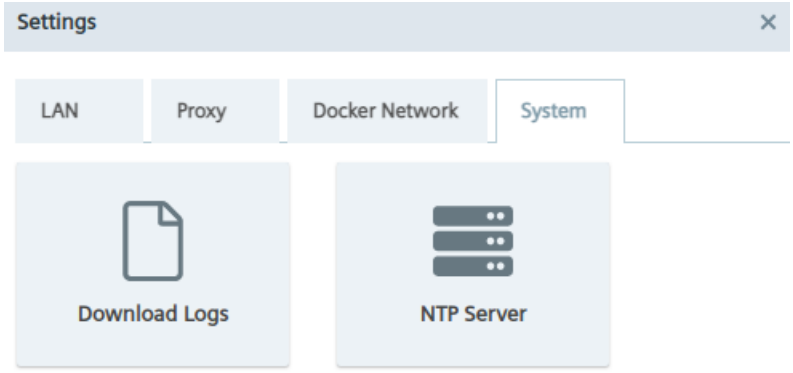


4. To save the settings, click "Configure".

4.7.2.4 Downloading logs

Procedure

1. Click the "System" tab.



2. Click the "Download Logs" tile.
   The log file is being downloaded to the standard download folder of your Internet browser.

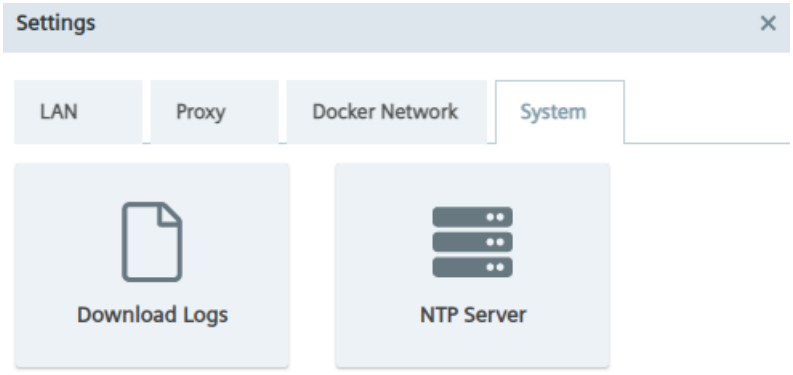
4.7.2.5 Adding an NTP server

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 mandatory.

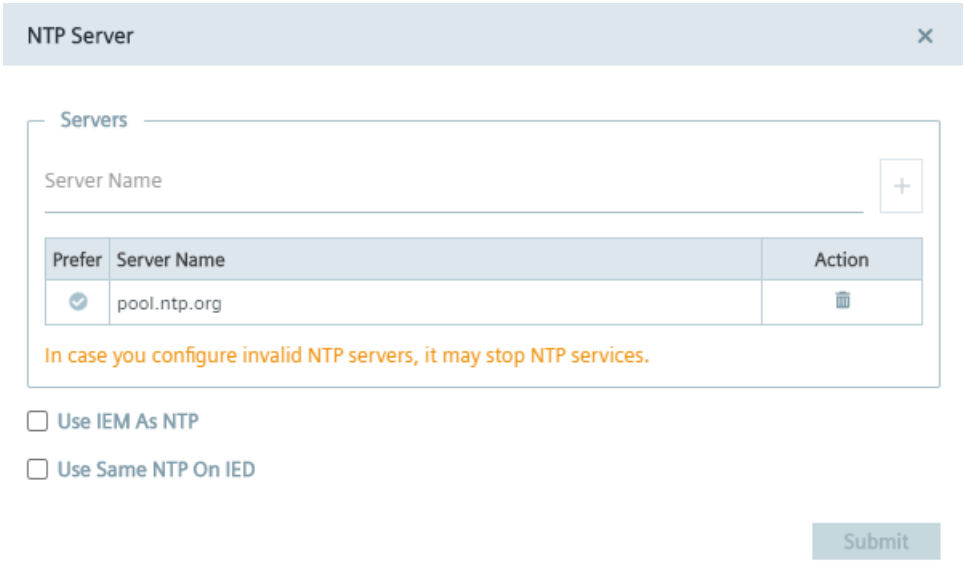
If you already have added an NTP server during the configuration of the Industrial Edge Management OS, you can skip this procedure.

Procedure

1. Click the "System" tab.



2. Click the "NTP Server" tile.
   The "NTP Server" screen is displayed.



   If you have added an NTP server during the configuration of the Industrial Edge Management OS, the NTP server is displayed in the server list.

3. If you have not added minimum 1 NTP server or you want to add an other NTP server, enter the NTP server in the "Server Name" input field.
4. To add the NTP server, click the plus icon.
   The NTP server is added to the server list.
5. By clicking the icon, you select the NTP server as preferred NTP server which signals the NTP service to always select this NTP server as synchronization source, in case the server is available.
   Preferred NTP servers are marked with .

6. By selecting the "Use IEM As NTP" check box, the NTP services in the IEM serve as an NTP server for other NTP clients, for example Edge Devices.
   This option removes the dependency that an NTP server must be configured in the local automation network and serves Edge Devices which cannot access any global or local servers within the local network.
7. By selecting the "Use Same NTP On IED" check box, Edge Devices that are getting connected to this IEM use the same preferred NTP server for time synchronization.

   Note
   Selecting NTP server
   You can just select either the "Use IEM As NTP" or the "Use Same NTP On IED" at the same time.

8. Click "Submit".

4.7.3 Installing the Industrial Edge Management

In the following, the term "cluster" is a synonym for the IEM-OS.

Procedure

1. To use created and self-signed certificates by the IEM itself, disable the "Custom Certificate" check box in the "IEM App Configuration" screen and go to step 11.

   Note
   Edge Management URL
   At the bottom of the screen the URL, with which you open the IEM, is displayed.

   Note
   Importing certificates after the setup
   When you do not use your own certificates but the certificates from the IEM, you cannot import your own certificates after the setup of the IEM anymore.

2. If you want to use your own certificates, enable the "Custom Certificate" check box.
   The IEM and its components require full chain certificates with rootCA, that means that the used certificates must be certificated and trusted by a higher certificate instance.
   The private keys and certificates must be uploaded in the *.pem format, for example "portal.key" and "portal.crt" files.
   You must select certificates for the IEM and for the Registry server.
3. In the "Edge Management SSL Key" field, click "Browse" and select your private key for the IEM.
4. In the "Edge Management SSL Certificate" field, click "Browse" and select your certificate for the IEM.
   When you use 2 different certificates with different domain names, select 1 for the IEM and 1 for the Registry server.
   When you use wildcard certificates issued for the "*.<domain.name>" domain, you can use the certificates for both the IEM and the Registry server.
   When you use SAN certificates with 2 different domain names, you can use the certificates for both the IEM and the Registry server.

5. In the "Edge Management URL" input field, enter the FQDN of the IEM that you want to use to open the IEM, for example "iem.my.domain.name.com".
   The "Edge Management URL" is needed for the API and the UI of the IEM. If you use resolved DNS entries for domain names, you can use the URL of the IEM to access the IEM by entering the domain name instead of the IP address.

   Note

   Avoid warnings

   Add the IP address into the SAN field. With that, the IEM can be opened without warnings by systems which cannot resolve the DNS.

   Note

   Multiple DNS servers

   If you are using multiple DNS servers, ensure to resolve the URL of the IEM in each DNS server. Otherwise, connection problems can occur during the access to the IEM.

   The "Edge Management URL" text field is being adapted according to your configuration. When you enter the URL of your IEM, the "Public Trusted" check box is enabled.

6. In the "Registry SSL Key" field, click "Browse" and select your private key for the Registry server.
7. In the "Registry SSL Certificate" field, click "Browse" and select your private certificate for the Registry server.
   Adding your private certificates and keys is mandatory when you do not use the created and self-signed certificates by the IEM itself.

   Note

   Missing certificates and keys

   If you select the "Custom Certificate" check box and click "Next" without providing the certificates and keys, the default certificates from the IEM are being used.

8. In the "Registry URL" input field, enter a FQDN for the Registry server, for example "iem-registry.my.domain.name.com".

   Note

   Registry URL

   Use for the "Registry URL" input field an own FQDN like for the "Edge Management URL" input field.

   The "Registry URL" is needed for using Docker images of Edge Apps.

9. If the selected certificates are wildcard or SAN certificates and thus public trusted, activate the "Public Trusted" check box.
   If the certificates are public trusted, you do not have to manage certificates for other components, for example the IE App Publisher or Edge Devices, to accept and use your certificates.
10. If the certificates are not public trusted, deselect the "Public Trusted" check box.
    In that case, you must import and accept the full chain certificates with rootCA for each other component in Industrial Edge.

11. Click "Next".
    The "Information" tab is displayed.

    The "IEM Cluster Network" section is editable, the "Configuration", "Network" and "Storage" sections are non-editable and are just displayed for your information.

12. If needed, edit the "Service Network" and the "POD Network" sections.
    The networks are needed for internal services. These network ranges must not overlap the LAN network in which the IEM is installed and both network ranges must not overlap each other.
    The "Range" entry indicates a network subnet and is the subnet in the Classless Inter-Domain Routing (CIDR) format, for example "67.67.0.0/12".

Note

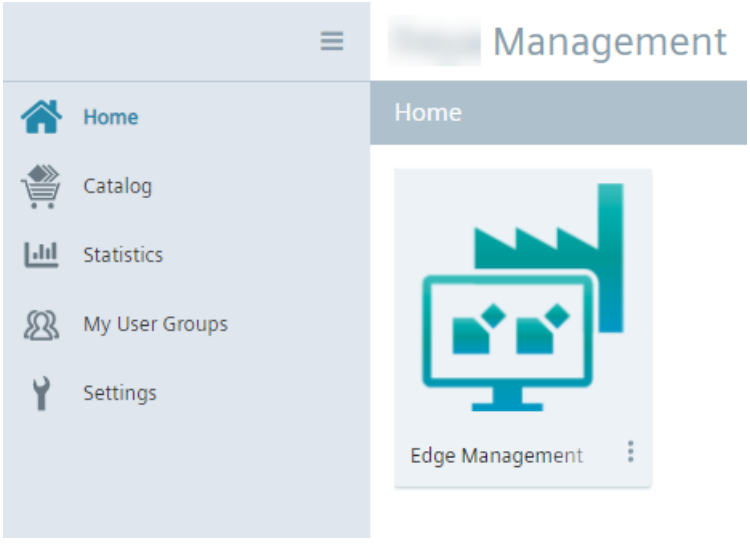
IEM Cluster Network settings

Siemens recommends to not change these settings.

13. Click "Create Cluster".
    You will be redirected to the URL of the IEM-OS.
    The IEM-OS is being created automatically. The "Create cluster" screen is displayed.

    This process takes approximately 10 minutes.

14. When the "Cluster created successfully" message is displayed, click "Ok".
    Automatically, the IEM has been installed as "Edge Management" app.



Note

Installation of the IEM

When the app is installed, the IEM-OS automatically downloads 3 images of approximately 1.5 GB. Depending on the Internet speed, the download of these images takes approximately 10 minutes.

Note

Automatic installation of IE services

With upcoming releases, several IE services, for example the IE State Service and the IE App Configuration Service, are also getting installed automatically as apps in the IEM-OS. You can check which IE services are getting installed automatically, and also the installation progress respectively status of the IE service, by clicking the icon.

4.8 Installing system configurators

System configurators are essential for using the functionalities of the IEM.

The following apps are the system configurators:

- SIMATIC S7 Connector Configurator
- IE Databus Configurator
- IE Cloud Connector Configurator

To use the system configurators, you must install the system configurators from the "Catalog" in the IEM-OS UI.

The following procedure describes the installation of the "IE Databus Configurator". To install other system configurators, proceed in the same manner.

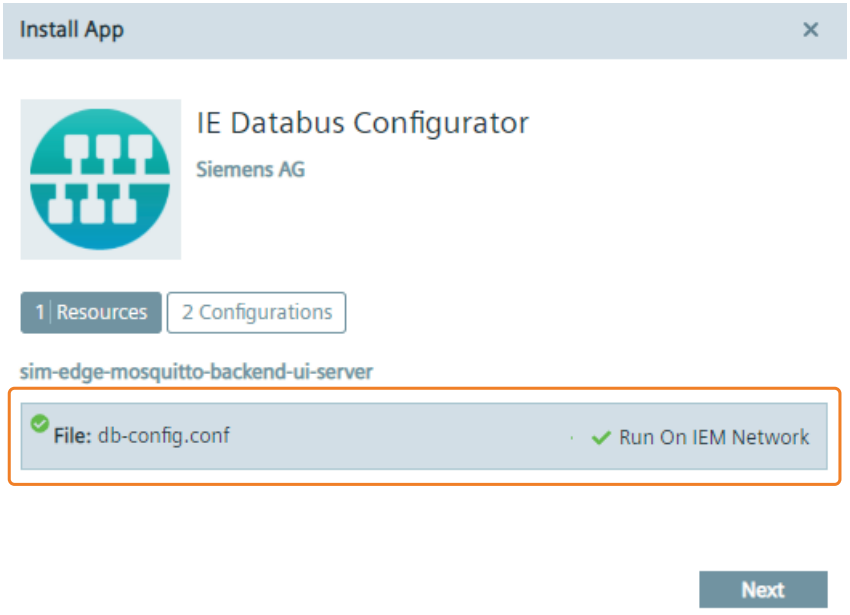
Note

System configurators documentation

You find more information on the functionalities and the operation of the system configurators in the manual of each system configurator in SIOS (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26128&lc=en-WW).

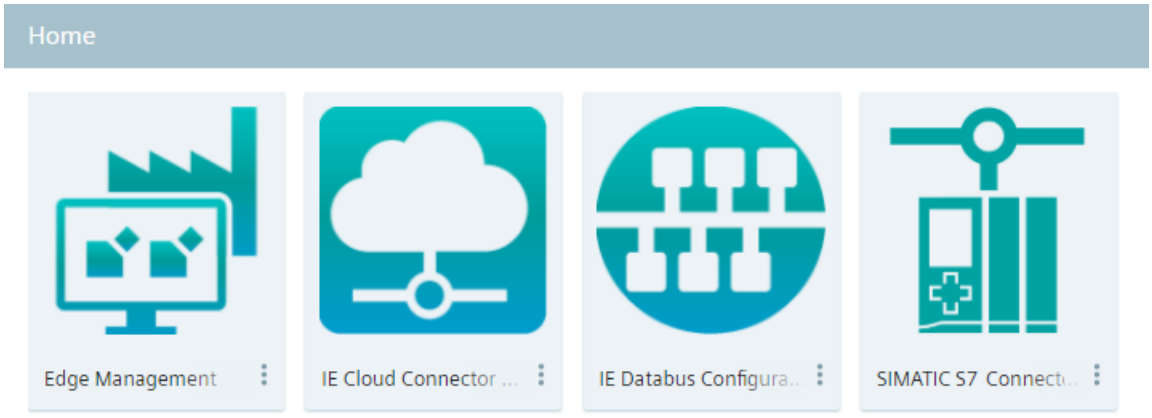
Procedure

1. In the navigation menu of the IEM-OS UI, click "Catalog".
2. Click the "IE Databus Configurator" app.
   The "Install App" screen is displayed.
   Ensure that the available resource file in the "Resources" tab is activated.



3. Click "Next".
4. To install the app, click either "Install Later" or "Install Now".
   "Install Now" installs the app immediately. When you click "Install Later", select an installation time.
   The app is being installed.
5. Click "Ok".
6. To check the installation status, click the tasks icon.

7. Wait for the app to be installed.
8. Before you continue, install the other system configurators in the same manner and wait until all system configurators are installed and available in the IEM-OS.



Note

Using the system configurators

By clicking the tile of a system configurator, the system configurator will be launched with an error. To use the system configurator, you must install the according system apps on the Edge Devices. After installing the system apps on your Edge Devices, you can use the system configurators.

You find the procedure on the installation of the system apps in the "Installing system apps (Page 93)" subsection.

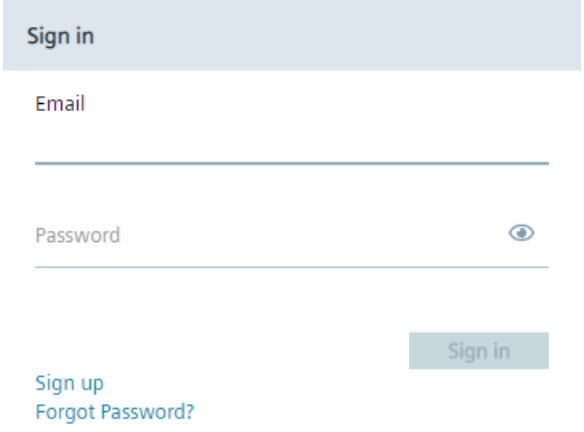
4.9 Adding a relay server

When your Edge Devices are placed in your plant network that is separated for example by NAT Gateway from the control plane network in which the IEM is running, the direct access from the control network is not possible. Normal operation is still possible, as the Edge Devices always initiate the communication from their side. For direct access through "remote access", for example for debugging on Edge Devices, a relay server is needed. The Edge Devices in the plant network establish the connection to the relay server. The IEM can act as a relay server for your Edge Devices. For that, you must add the IP address of the IEM server. Afterwards, you can use the "remote access" through the IEM after activation. Only 1 relay server per IEM is allowed.

Procedure

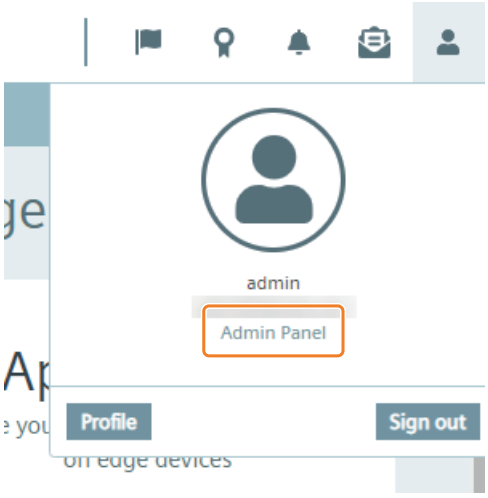
1. When the "Edge Management" app and the system configurators are installed, open the IEM by clicking on the "Edge Management" app.
   Alternatively, you open the IEM by entering the URL of the IEM that you entered during the setup of the IEM-OS into an Internet browser, for example "iem.my.domain.name.com".
   The login screen of the IEM is displayed.

2. Click "Sign in".
   The "Sign in" screen is displayed.



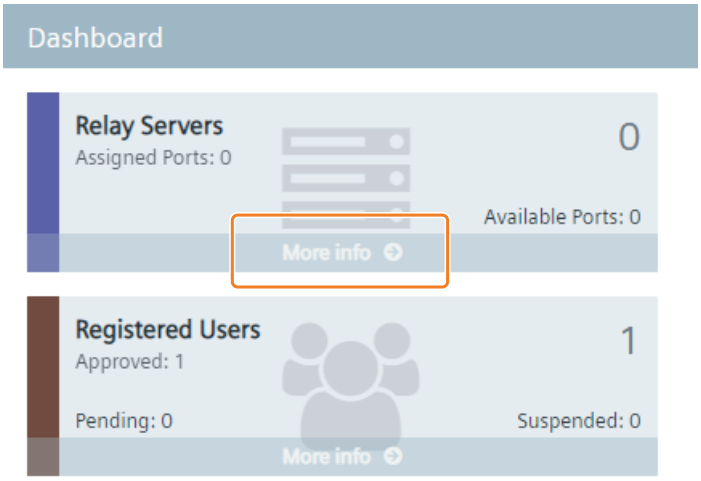
3. Log in with the admin credentials that you configured during the setup of the IEM-OS.
   The home page of the IEM is displayed.

4. In the top-right corner, click the username.
5. To open the admin management, click "Admin Panel".



The "Dashboard" screen of the admin management is displayed.

6. In the "Relay Servers" section, click "More Info".



   The "Relay Servers" screen is displayed.

7. Click "Add Relay Server".
   The "Add Relay Server" screen is displayed.

8. To add a relay server, enter the IP address of your IEM-OS respectively your VM in the "IP Address" input field.

Note

VM IP address

You get the IP address of your VM from the login screen in the VM.

9. Click "Add".
   The relay server is added to the relay servers list.
   The setup of the IEM is completed. In the next sections, you find the procedure on how to install the system apps and connect Edge Devices to the IEM.

Installing system apps

5

To use the system configurators, you must install the according system apps on your Edge Devices. The system configurators are only usable and available for the Edge Devices on which the specific system apps are installed.

To load apps in general to the IEM, you have the following possibilities:

- Copying the app directly from the IE Hub to the IEM
- Uploading apps through the IE App Publisher to the IEM
- Importing apps through the "Import Application" button in the "Catalog" screen in the IEM

The following describes the procedure on how to copy the system apps from the IE Hub to the IEM.

5.1 Copying system apps to the IEM

The following procedures describe the transfer and installation of the "IE Databus" system app. Proceed in the same manner for every other system app.

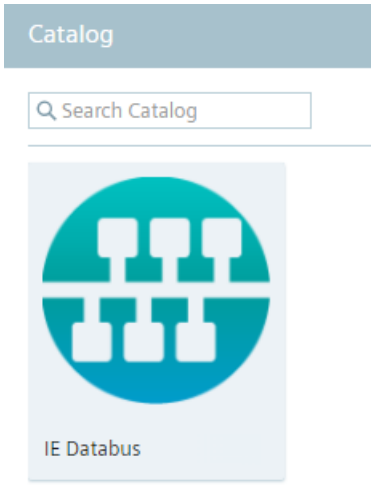
Procedure

1. Log into the IE Hub.
2. In the navigation menu, click "Library".
3. Click the copy icon of the "IE Databus" app.

The "Copy Application to IEM catalog" screen is displayed.

4. From the drop-down list, select the IEM instance to which you want to copy the app to.
5. Click "Copy".
   The app is being transferred to the catalog of the selected IEM instance. You can check the status of the transfer by clicking the jobs icon in the IEM instance.

When the transfer is completed, the system app is available in the catalog.



To install the system app, you must add Edge Devices to the IEM.

5.2 Connecting an Edge Device

When you add an Edge Device to the IEM, an Edge Device configuration file is created. With this configuration file, you have the following options to connect the Edge Device with the IEM:

- Connecting through an USB flash drive
- Connecting through the IEM

Both options require the Edge Device configuration file.

Requirements for adding an Edge Device

- The Edge Device is switched on.
- The Edge Device is connected to the local network.
- The Industrial Edge Device OS is installed on the Edge Device.

5.2.1 Layer 2 network access

Some Edge Apps need to communicate with automation devices via automation protocols, such as Profinet, DCP and LLDP. That means, these Edge Apps require to be directly connected to the physical network at the data link layer (Layer 2 network access). This Layer 2 network access is used only for communication with automation devices on the physical network, it is not designed to provide communication between app containers. For communication between app containers, standard app container communication means must be used.

When you add an Edge Device to the IEM, you define the IP address range of the Layer 2 network access which is then reserved for the communication with automation devices. To install and use these Edge Apps on Edge Devices, you must enable the Layer 2 network access for Edge Devices when you add Edge Devices to the IEM. The Layer 2 network access configurations are then saved to the Edge Device configuration file. Edge Apps that require a Layer 2 network access can only be installed on Edge Devices with an according configured Layer 2 network access. Once you have configured the Layer 2 network access of an Edge Device, you cannot edit the Layer 2 network access. If you want to reconfigure the Layer 2 network access of an Edge Device, you must perform the "Hard Reset" system command for the Edge Device and afterwards re-onboard the reset Edge Device to the IEM with new Layer 2 network access configurations. If you want to remove the Layer 2 network access from an Edge Device, you must perform the "Hard Reset" system command for the Edge Device.

Note

Hard reset of an Edge Device

If you perform the "Hard Reset" system command for an Edge Device, all data on the Edge Device is being deleted.

You find information on how to enable the Layer 2 network access for an Edge Device and how to configure the IP address range in the following subsections.

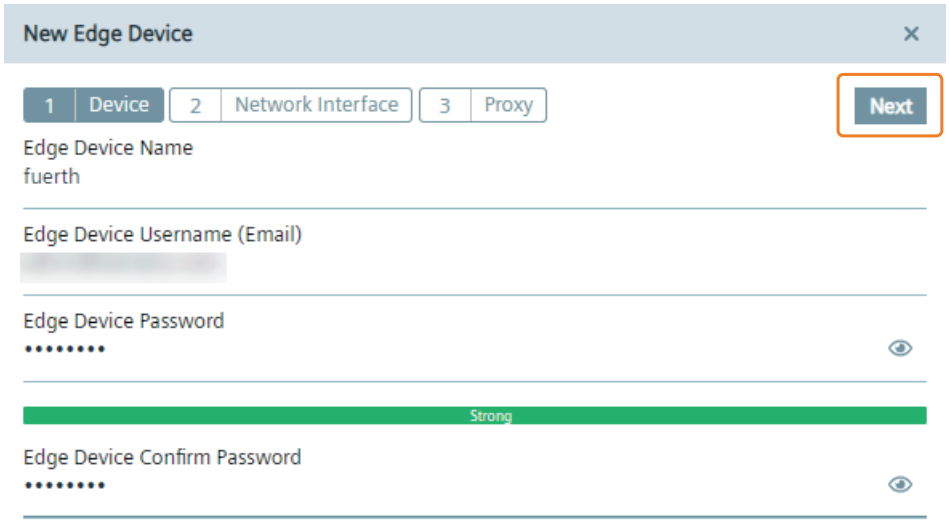
You find information on how to create Edge Apps that require a Layer 2 network access in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual in the "Creating a Layer 2 network access" subsection.

5.2.2 Creating the Edge Device configuration file

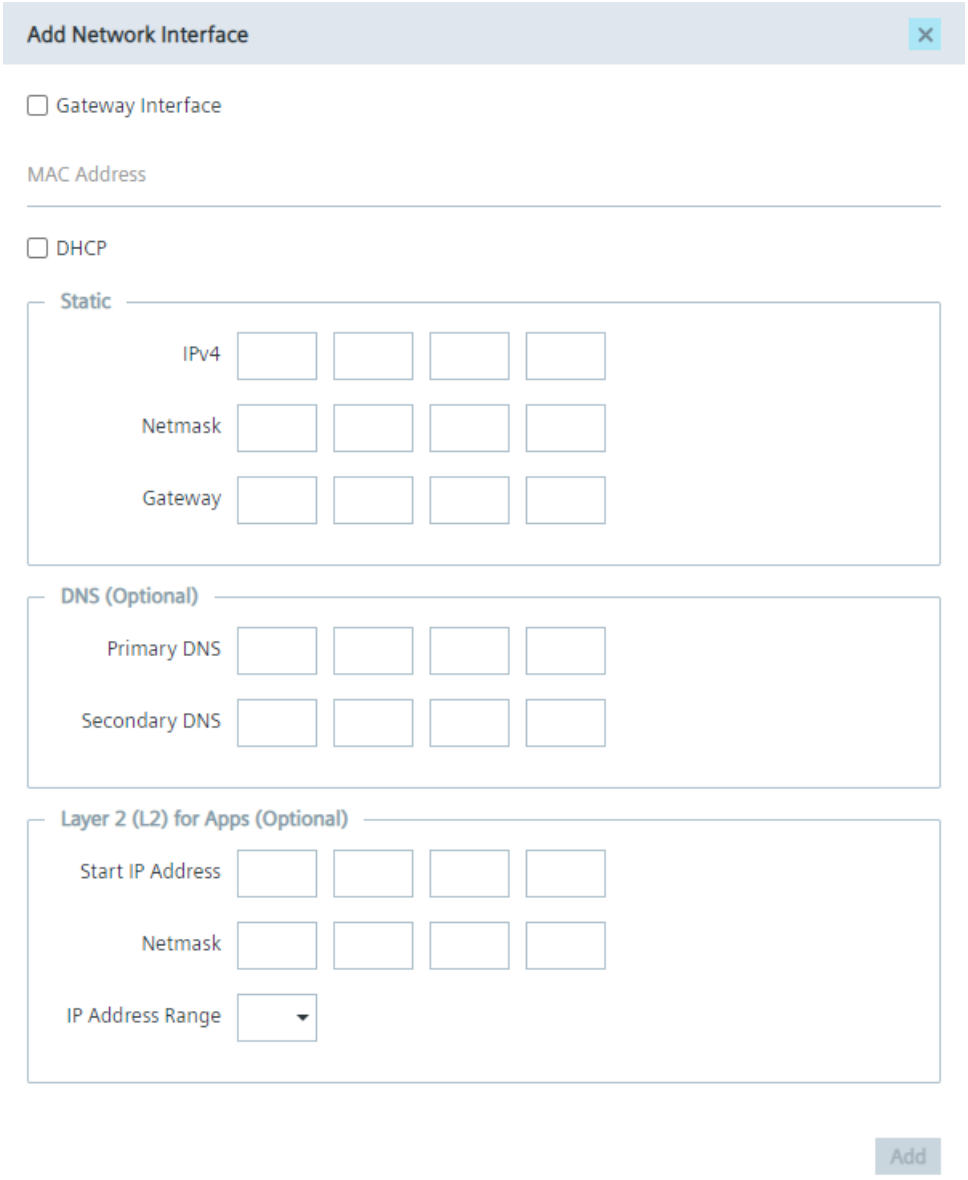
Procedure

1. Open and log into the IEM.
2. Navigate to the "Edge Devices > My Edge Devices" menu item.
3. In the "My Edge Devices" screen, click "New Edge Device".
   The "New Edge Device" screen is displayed.
4. In the "Device" tab, enter all the required information according to the "New Edge Device - Parameters (Page 101)" subsection.

5. After entering all required information, click "Next".



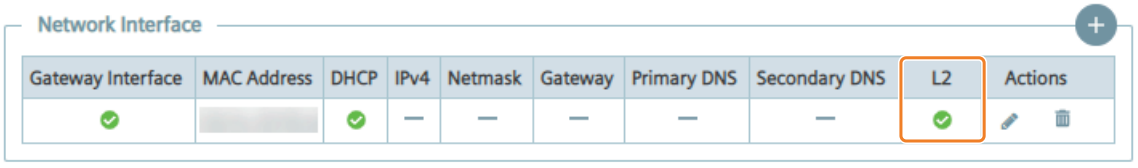
6. In the "Network Interface" tab, click the + icon under the "Network Interface" section to enter the network properties of the Edge Device.
   The "Add Network Interface" screen is displayed.



   To complete the connecting process, minimum 1 network interface must be added.

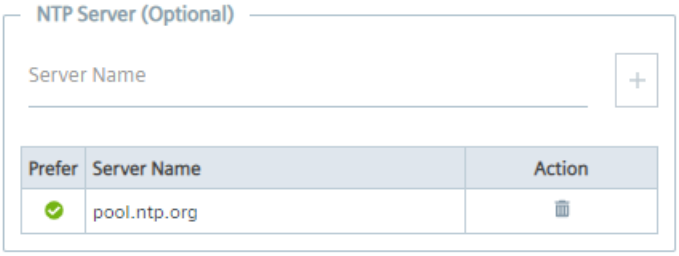
7. Enter the network properties of the Edge Device according to the "New Edge Device - Parameters (Page 101)" subsection.

8. Click "Add".
   The network interface is added.
   If you have completed the "Layer 2 for Apps (L2)" section, the L2 check mark is activated which means that the L2 network access is enabled.

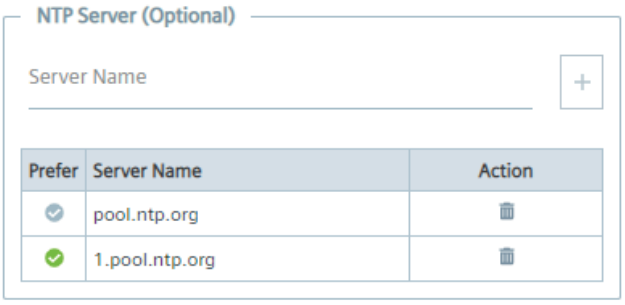


If you click again the + button to add another network interface, the "Layer 2 for Apps (L2)" section displays "Already configured". You can just configure 1 L2 network access per Edge Device.

9. Select 1 Network Time Protocol (NTP) server you want to use for this Edge Device under the "NTP Server" section.
   When you already have configured an NTP server during the setup of the Industrial Edge Management or when you added an NTP server in the IEM-OS UI settings and selected the "Use Same NTP On IED" check box, the NTP servers are displayed under the "NTP Server" section .



   If you want to use an other NTP server, enter the NTP server in the "NTP Server" input field, click the plus icon and select the newly added NTP server.



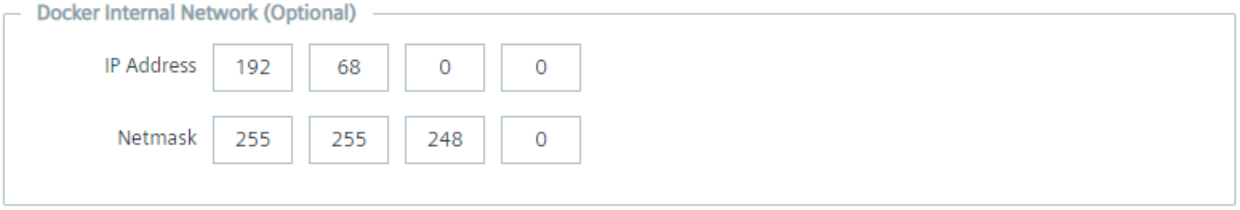
Note

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.

10. In the "IP Address" input field under the "Docker Internal Network" section, enter the IP address of the docker0 interface of the Edge Device, if necessary.
    The input of the docker0 interface is optional. The IP address of the docker0 interface is the start of the docker0 interface. By default, the docker0 interface starts with 172.17.0.0.

11. In the "Netmask" input field under the "Docker Internal Network" section, enter the subnet mask of the Docker network.

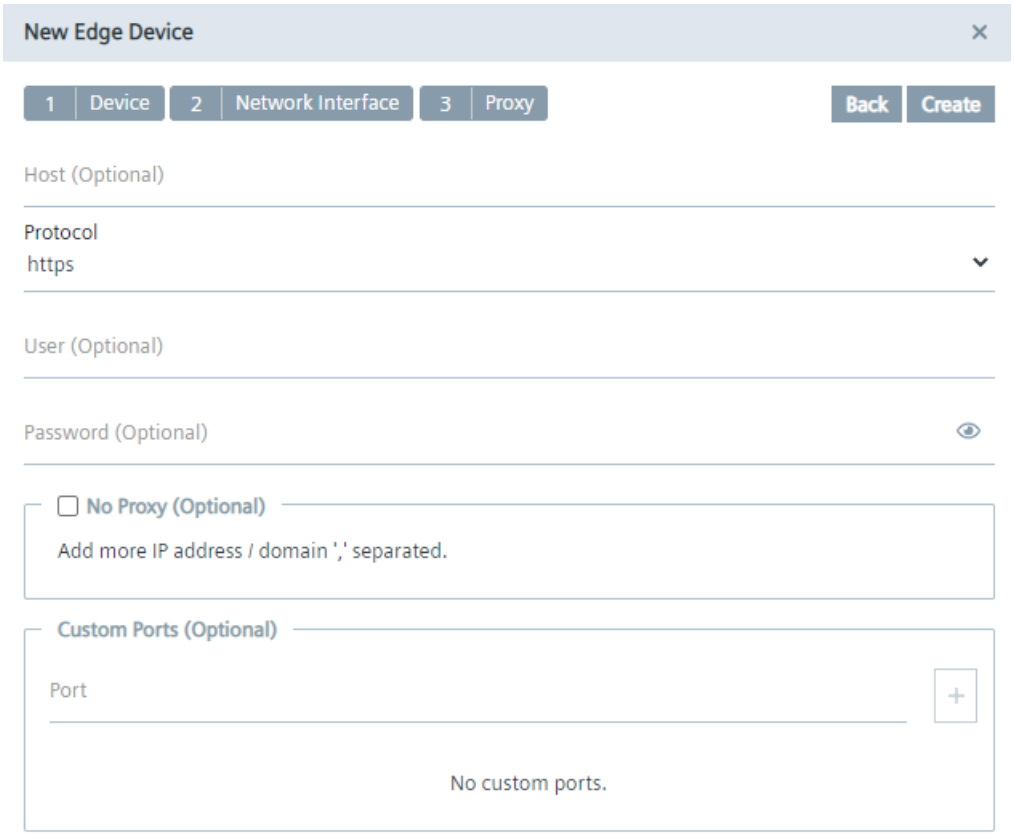


With the subnet mask of the Docker network, you define the amount of creatable Docker networks. By default, the Edge Device contains 2 Docker networks, 1 for the proxy-redirect and 1 for the docker0 interface (that you create in the "IP Address" input field). When you install an app which creates a new Docker network on the Edge Device, the Docker network of the installed app must not overlap the Docker networks of the Edge Device and need free Docker network IP ranges on the Edge Device. Thus, before onboarding the Edge Device, you must ensure that several Docker network IP ranges are available for apps that create a Docker network. Otherwise, if you want to install an app that tries to create a new Docker network on the Edge Device but the Edge Device has no free Docker network IP ranges, the app installation fails.
The following subnet masks of the Docker network show the amount of installable apps that create a new Docker network as an example:

- 255.255.252.0: 2 apps with new Docker networks are installable
- 255.255.248.0: 6 apps with new Docker networks are installable

12. Click "Next".

13. In the "Proxy" tab, enter, if needed, all required proxy information according to the "New Edge Device - Parameters (Page 101)" subsection.



14. Click "Create".
A configuration file named "device-<Edge Device Name>" is downloaded to the standard download folder of your Internet browser.

5.2.3 New Edge Device - Parameters

Device

Parameter	Description
Edge Device Name	• Unique domain wide name of the Edge Device • Must contain 3 - 15 characters • Only lower case letters and numbers
Edge Device Username	Valid email address of the user for signing into the Edge Device

Parameter	Description
Edge Device Password	• Password for signing into the Edge Device • Minimum 8 characters • Minimum 1 upper case letter • Minimum 1 special character • Minimum 1 number
Edge Device Confirm Password	Confirm Edge Device password

Network Interface

Parameter	Description
Gateway Interface	• Select this check box and set this network interface as interface to connect to the IEM • 1 interface must be selected as "Gateway Interface"
MAC Address	• MAC address of the interface which is currently configured • Use colons as separations • Input of the MAC address is mandatory • Example MAC address: 00:0c:29:82:3f:81
DHCP	• Enable or disable IP address assignment through DHCP • If this check box is selected, the IP address is assigned through DHCP • When the check box is disabled, static IP address assignment is used
IPv4	• Only enabled when DHCP is disabled • IP address of the Edge Device in the network • Input of the IP address is mandatory when DHCP is disabled
Netmask	• Only enabled when DHCP is disabled • Subnet mask in the "255 255 0 0" format, for example • Input of the subnet mask is mandatory when DHCP is disabled
Gateway	• Only enabled when DHCP is disabled • IP address of the gateway • Input of the IP address is mandatory when DHCP is disabled
Primary DNS	• Primary DNS server address • Input of the DNS server address is optional
Secondary DNS	• Secondary DNS server address • Input of the DNS server address is optional
Start IP Address	• L2 network access is optional • Start of the L2 network access IP address range • Number in the last octet must be even • Input of Start IP Address is mandatory for L2 network access usage

Parameter	Description
Netmask	• Netmask defines the section in which the IP addresses are located • Input of netmask is mandatory for L2 network access usage
IP Address Range	• Length of the IP address range for usage of Edge Apps with direct L2 network access • Minimum IP address range is 2, maximum range is 256 • Valid displayed IP address range depends on last number in Start IP address, for example: – If last number of Start IP address is 16: 1, 2, 4, 8 and 16 is available – If last number Start IP address is 172: 1, 2 and 4 is available – If last number Start IP address is 0: 1, 2, 4, 8, 16, 32, 64, 128 and 256 is available • Input of IP address range is mandatory for L2 network access usage

The parameters in the "Layer 2 for Apps (L2)" section and thus the configured Layer 2 network access is independent of the "DHCP" and "Gateway Interface" configuration.

Ensure that the Edge Device IP addresses and the configured L2 network access configurations do not collide with addresses of other devices in the network.

Note

IP address and broadcast IP address of subnet

Do not use the IP address and the broadcast IP address of the subnet defined by the netmask for the configured IP address range.

For more information regarding the configuration of Docker IP address ranges, check the official Docker documentation (https://docs.docker.com/network/macvlan/).

Proxy

Parameter	Description
Host	• IP address and port of the proxy • Input in the format <IP>:<PORT> • Proxy host address is optional
Protocol	Transport protocol of the proxy server
User	Username for authentication on the proxy server, if necessary
Password	Password for authentication on the proxy server, if necessary
No Proxy (optional)	• Enable and enter IP addresses which shall be accessed directly (without use of proxy) • Separate multiple no proxy addresses by a comma • Input of no proxy address is optional but mandatory if you select this check box
Custom Ports	• Ports that are needed for using apps on the Edge Device • Add further ports by clicking the plus button • Input of ports is optional

5.2.4 Connecting the Edge Device through an USB flash drive

Requirement

- 1 USB flash drive is available.
- The Edge Device configuration file has been created.

Procedure

1. Copy the Edge Device configuration file on an USB flash drive.
   Ensure that just 1 configuration file is saved to the USB flash drive. Otherwise, the connecting process causes problems and fails.
2. Insert the USB flash drive into the Edge Device.
   The connecting process is being started automatically. The "Run" LED flashes green and the "Maintenance" LED flashes yellow.
3. Wait until the connecting process is completed.
   When the Edge Device is connected successfully to the IEM, the "Run" LED lights up green.

Note

Connection successful

When the Edge Device is connected successfully to the IEM, the status indicator at the top of the Edge Device tile in the IEM switches to green and the IP address of the Edge Device is displayed under the name of the Edge Device.

To open the UI of the Edge Device, either click on the tile of the Edge Device, if the remote access is enabled, or enter the IP address of the Edge Device into your Internet browser. Use the HTTPS protocol, for example "https://192.168.80.123".

Note

Log file "conf-usb.log" and log file "services.log"

During the connecting process, the "conf-usb.log" and "services.log" files are created in the USB flash drive. In case of any errors, open these log files in a text editor for detailed information. In addition, you can check the steps of each service, if it was successful or not, in the "services.log" file.

5.2.5 Example logs

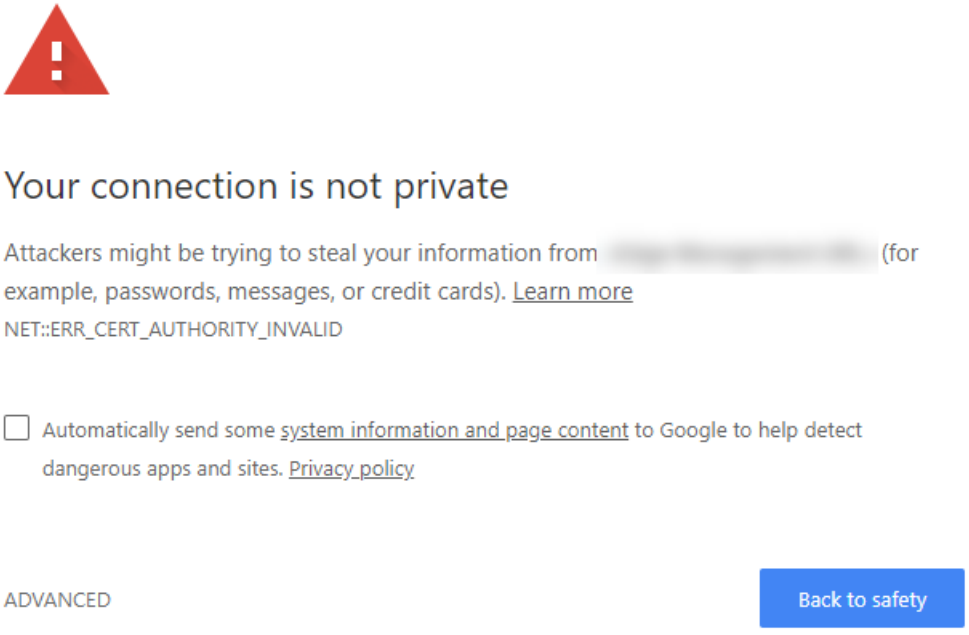
The following are examples of the output of the "conf-usb.log" file after the onboarding process:

- In case of success:
```
[INFO ] STARTED, Applying configurations
[INFO ] SUCCEED, Network Manager --- Message: Configuration
Successfully Applied.
[INFO ] SUCCEED, Onboarding Manager --- Message: Device has been
activated successfully.
[INFO ] FINISHED, Applying configurations
```
- In case of an error (network interface success, onboarding failed):
```
[INFO ] SUCCEED, Network Manager --- Message: Configuration
Successfully Applied.
[ERROR ] FAILED, Onboarding Manager
[ERROR ] {"code":500,"message":"Unable to
activate.","errorExplanation":"Unable to activate."}
```
- In case of error (network interface failed: No onboarding attempt and rollback to the previous network settings):
```
[ERROR ] FAILED, Network Manager
[ERROR ] Exception while applying config due to 'Any interface
could not be found for '20:87:56:b5:ed:e4' MAC address on the
device.'
[INFO ] Rolling back Network Manager
[INFO ] Rolled back Network Manager, Result: True, Configuration
Successfully Applied.
[INFO ] FAILED, Reason: 'Failed to apply configurations and
rollback to old configurations'
```

5.2.6 Connecting the Edge Device through a browser

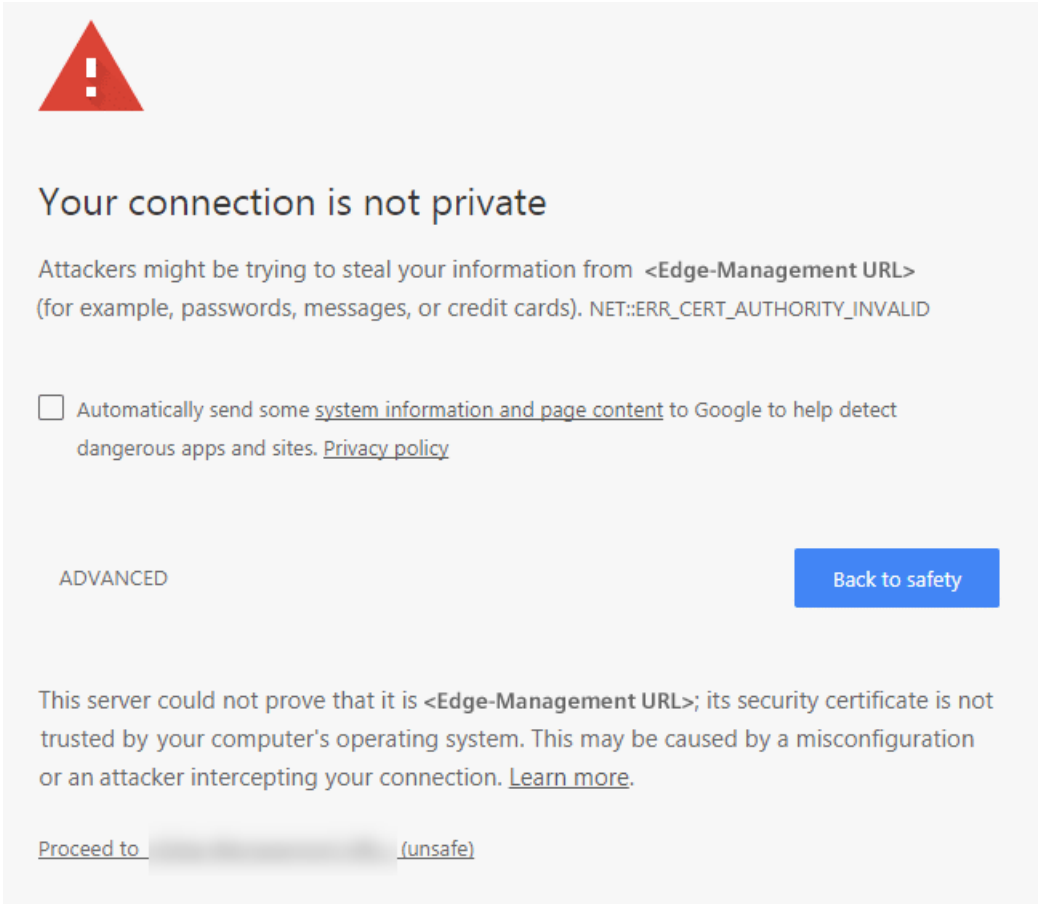
Procedure

1. Open the Edge Device UI by entering the IP address of the Edge Device in HTTPS protocol into your Internet browser, for example "https://192.168.80.123".
   A certificate warning is displayed.

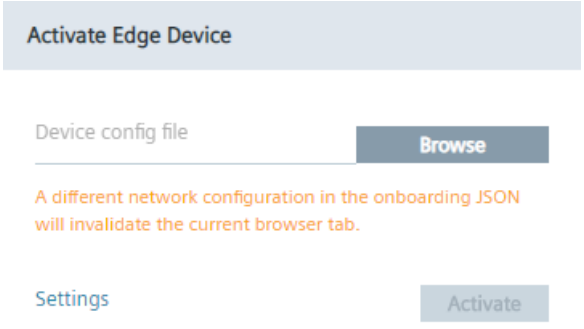


2. Click "Advanced".

3. Click "Proceed to <IP address>".



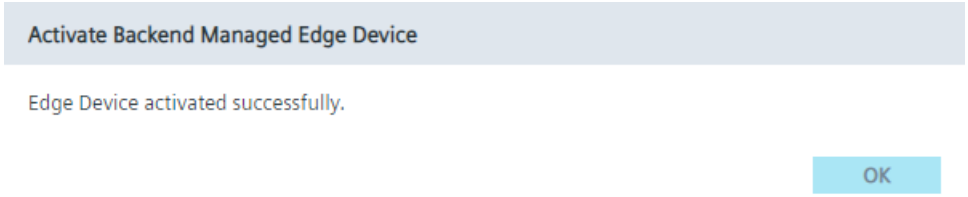
The "Activate Edge Device" screen is displayed.



4. Click "Browse" and select the created Edge Device configuration file.

5. Click "Settings" to configure the following settings:
   - Network settings
   - Proxy settings
   - Docker network settings
   - System settings

   You find the procedure on how to configure each setting in the "Settings" subsection.
6. After configuring the settings, click "Activate".
   The Edge Device is being connected to the IEM. When the connecting process was successful, an according message is displayed.



7. Click "Ok".
   You will be redirected to the Edge Device UI.

Note

Connection successful

When the Edge Device is connected successfully to the IEM, the status indicator at the top of the Edge Device tile in the IEM switches to green and the IP address of the Edge Device is displayed under the name of the Edge Device.

8. Sign in with your email address and password that you have entered in the "New Edge Device" screen.
   The home page of the Edge Device UI is displayed.

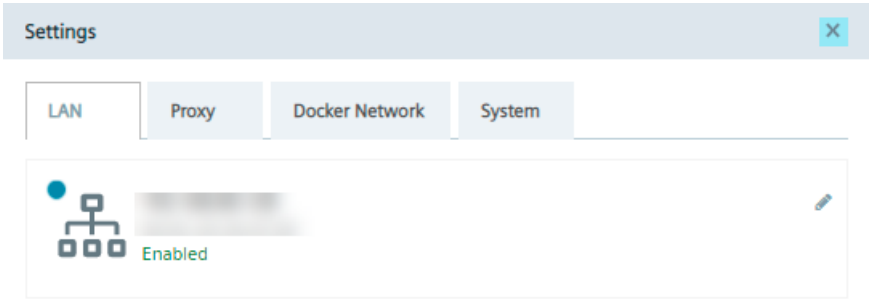
5.2.7 Settings

5.2.7.1 Editing network and Layer 2 network access settings

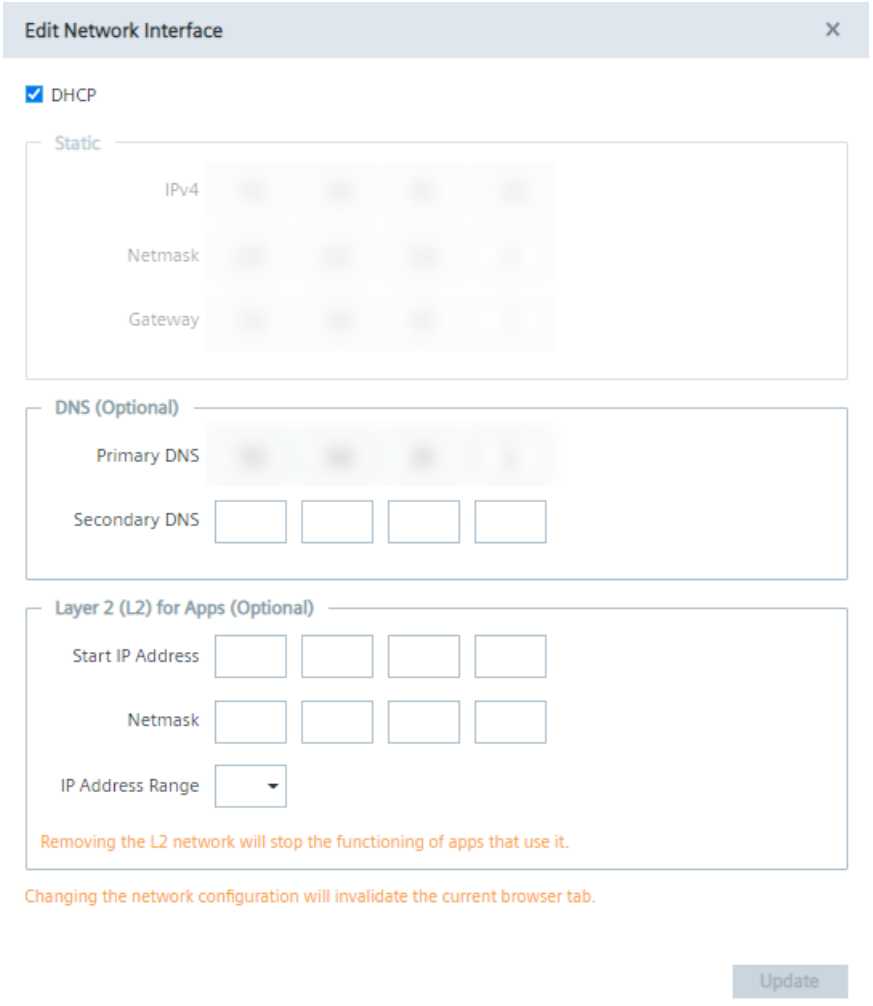
If you want to, you can again edit the configured network settings or set up a Layer 2 network access on this Edge Device before you onboard the Edge Device to the IEM.

Procedure

1. In the "Activate Edge Device" screen, click "Settings".
   The "Settings" screen is displayed.

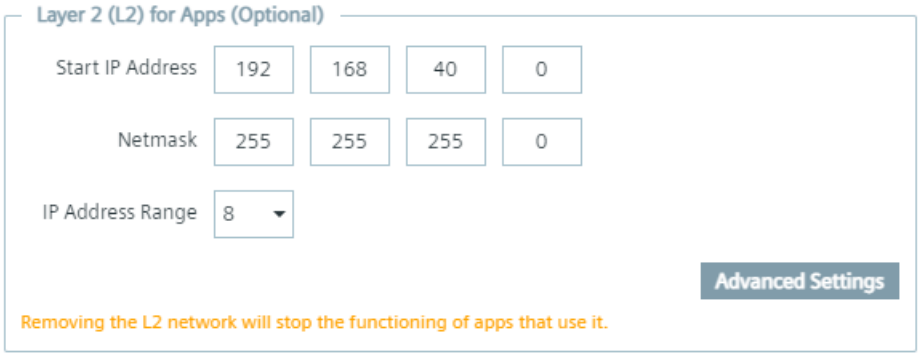


2. To edit the network settings, click the icon.
   The "Edit Network Interface" screen is displayed.



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

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



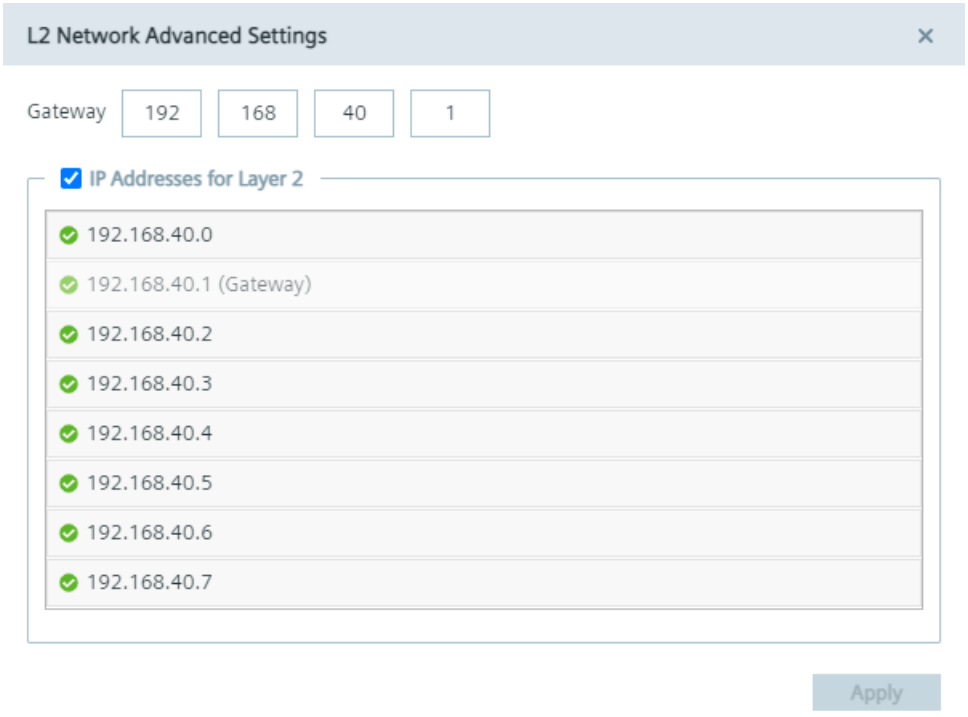
Note

Removing Layer 2 network access

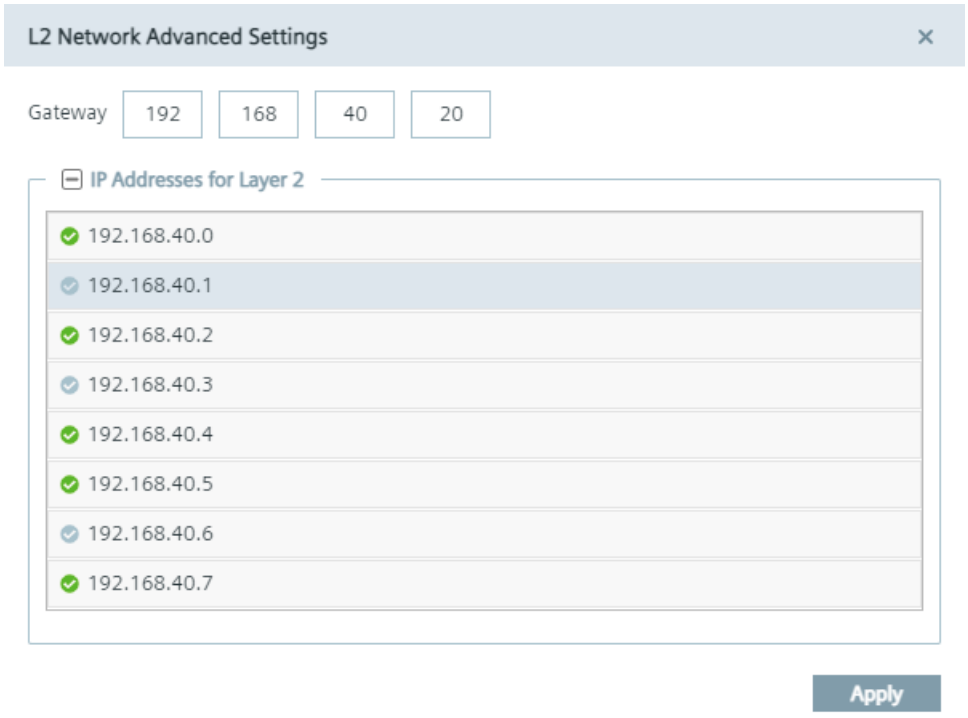
If you remove a configured Layer 2 network access on this Edge Device and if apps, that are running on this Edge Device, are using the Layer 2 network access, the apps will not work anymore.

You find more information on the Layer 2 network access in the "Layer 2 network access" and the "New Edge Device - Parameters" subsections.

5. 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 below for example:



   By selecting an IP address, the IP address can be used for the Layer 2 network access for apps. By not selecting 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 1 more available IP address in the given IP range, but the IP address of the gateway must be within the entered subnet.



6. To save the Layer 2 network access changes, click "Apply".
7. To save all changes, click "Update".

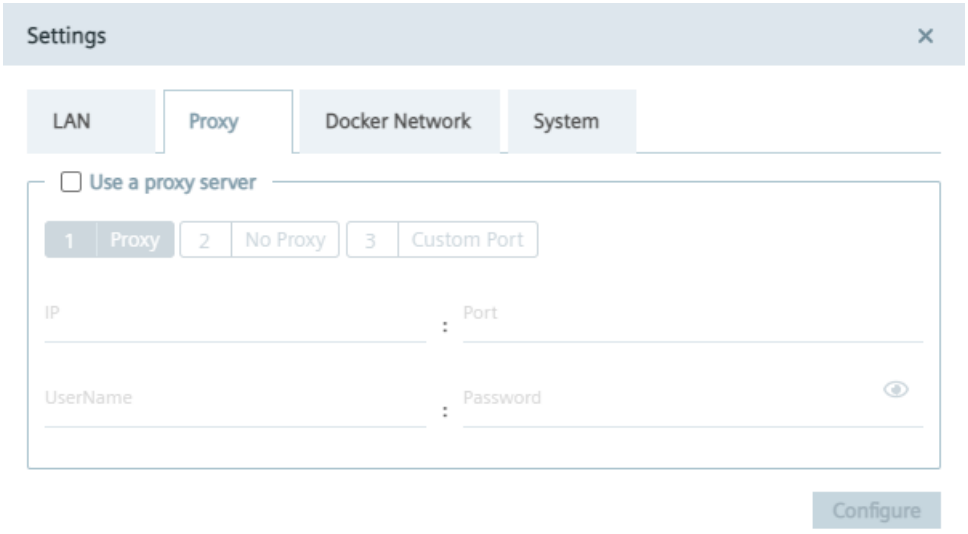
5.2.7.2 Setting up a proxy server

With the use of a proxy server, the admin of the IEM (and of Edge Devices) can add, edit and remove proxy rules to redirect specific data traffic. The admin can also disable redirection of specific data traffic through the proxy.

App developers do not need to implement their own proxy settings. The proxy settings described in this procedure apply for all IEM components.

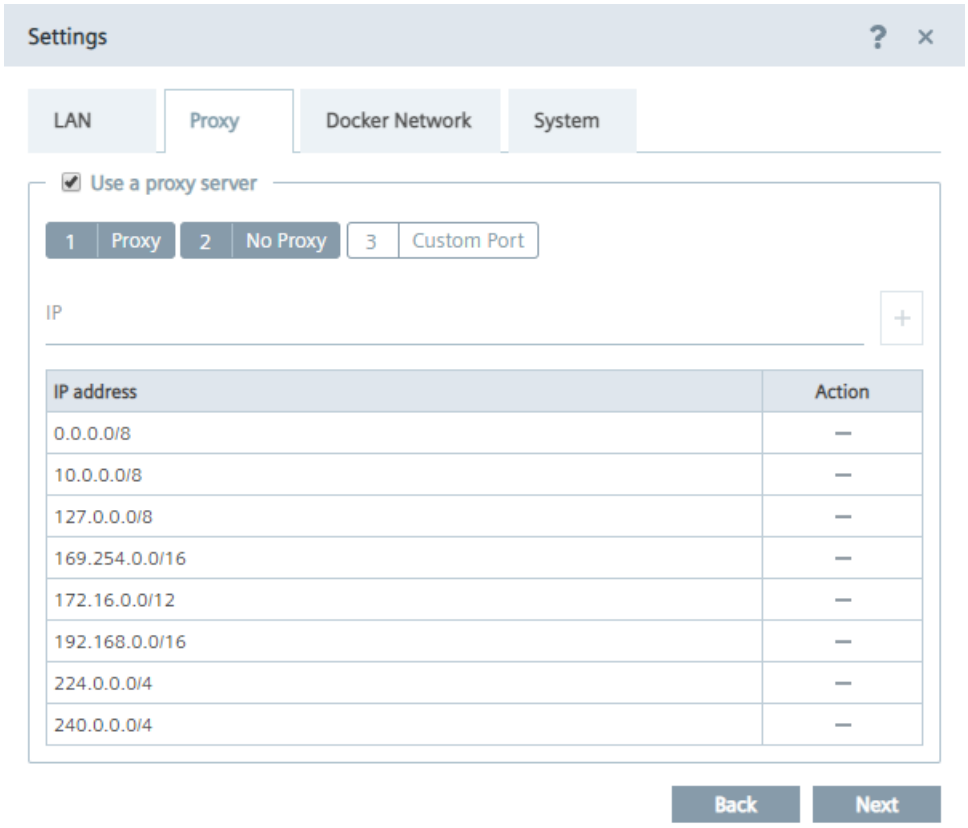
Procedure

1. Click the "Proxy" tab.



2. To use a proxy server, click the "Use a proxy server" check box.
   The input fields for the proxy server settings are enabled.
3. Enter the IP address and the corresponding port of the proxy server in the according input fields.
4. If needed, enter username and corresponding password in the according input fields in case of an additional authentication for the proxy server.
   The settings apply for HTTP and HTTPS proxy servers.

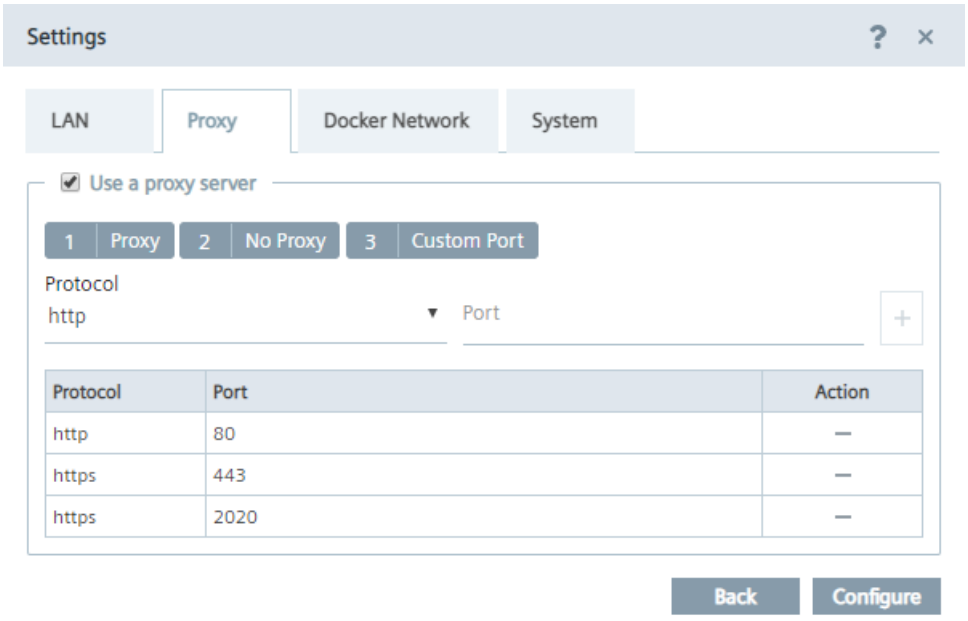
5. Click "Next".
   The "No Proxy" tab is displayed.



   In the "No Proxy" tab, add all the IP addresses which shall be accessed directly (without use of proxy).
   By default, several no proxy addresses are listed which are required by the IEM.

6. If you want to add a further IP address which shall be accessed directly, enter the IP address or domain of the no proxy address in the "IP" input field and click the + icon.
   The address is added to the no proxy list.

7. Click "Next".
   The "Custom Port" tab is displayed.



   In the "Custom Port" tab, you configure ports for apps which use the configured ports for outgoing communication through the proxy on HTTPS or HTTP protocols. For your apps, use ports between the port range 32768-60999.
   By default, several ports are listed which are required by the IEM.

   Note

   Default no proxy addresses and ports

   The default no proxy addresses and ports are essential for running the IEM and cannot be deleted.

8. If you want to add a further port, select the required protocol from the "Protocol" drop-down list and enter the required port.
9. To add the port, click the + icon.
   The port is added to the port list.
10. To add the proxy settings, click "Configure".
11. Confirm the proxy settings by clicking "Ok".
    The proxy settings are saved.

    Note

    Setting up a proxy server after onboarding the Edge Device

    You can also configure and update the proxy settings after you have onboarded the Edge Device to the IEM. In the Edge Device UI, navigate to the "Settings > Connectivity > Proxy Network" section and set the proxy settings.

5.2.7.3 Configuring the Docker network

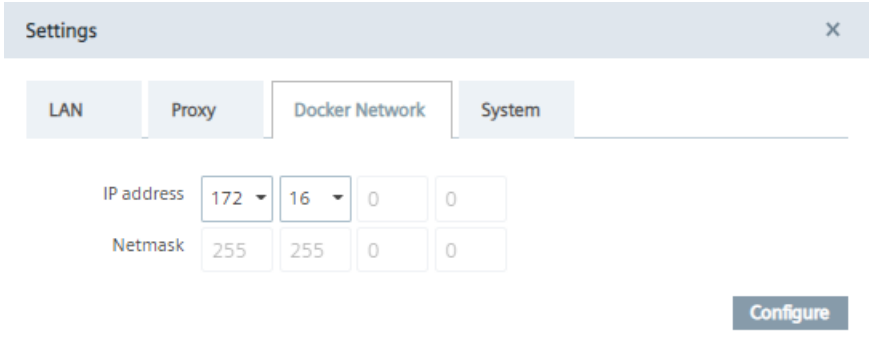
In the "Docker Network" tab, you can edit the IP range of the docker0 interface of the Edge Device, if necessary.

The IP address of the docker0 interface is the start of the docker0 interface. By default, the docker0 interface starts with 172.17.0.0. By default, the Edge Device contains 2 Docker networks, 1 for the proxy-redirect and 1 for the docker0 interface (that you create in the "IP Address" input field). When you install an app which 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 need free Docker network IP ranges on the Edge Device. Otherwise, if you want to install an app that tries to create a new Docker network on the Edge Device but the Edge Device has no free Docker network IP ranges, the app installation fails.

You can just edit the IP range in a given range with a specific netmask to prevent errors in the system.

Procedure

1. In the "Settings" screen, click the "Docker Network" tab.
2. In the "IP address" input field, enter the IP address that you want to use for the docker0 network.

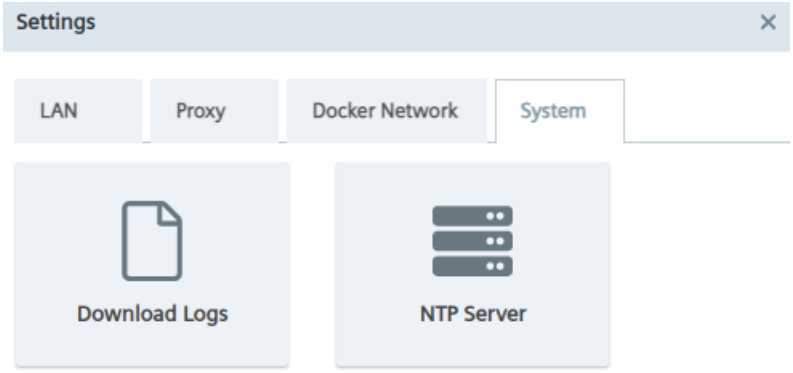


3. To save the settings, click "Configure".

5.2.7.4 Downloading logs

Procedure

1. Click the "System" tab.



2. Click the "Download Logs" tile.
   The log file is being downloaded to the standard download folder of your Internet browser.

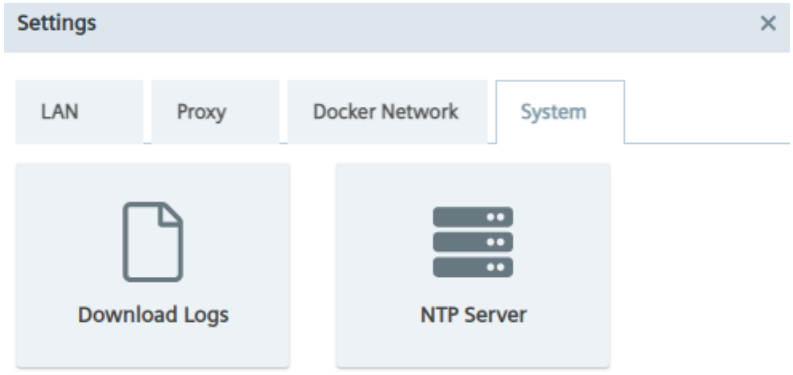
5.2.7.5 Adding an NTP server

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 mandatory.

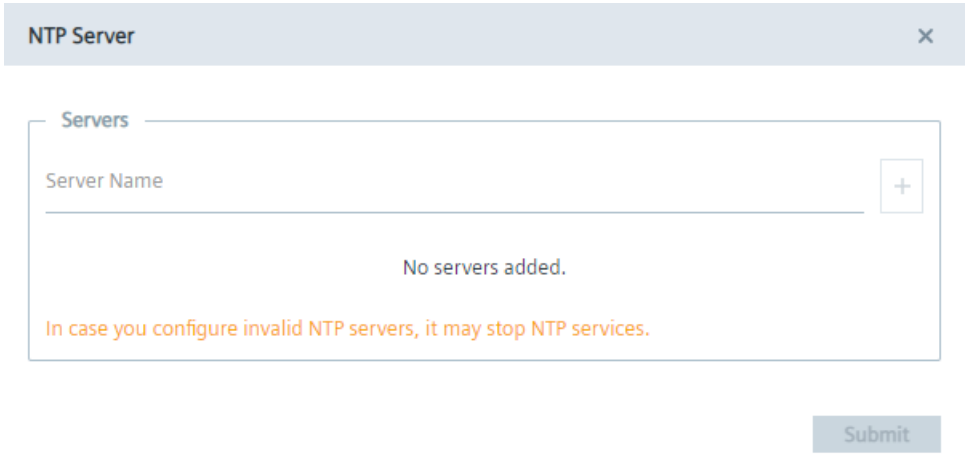
If you already have added an NTP server during the configuration of the Industrial Edge Management OS and use the same NTP server for your Edge Devices, you can skip this procedure.

Procedure

1. Click the "System" tab.



2. Click the "NTP Server" tile.
   The "NTP Server" screen is displayed.



3. If you have not added minimum 1 NTP server or you want to add more NTP servers, enter the NTP server in the "Server Name" input field.
4. To add the NTP server, click the plus icon.
   The NTP server is added to the server list. You can add several NTP servers. In case that 1 of them is unavailable, the next NTP server from the list will get active.
5. Click "Submit".

5.2.8 Certificate management for connected Edge Devices

Connected Edge Device with self-signed certificates or certificates from the IEM

When you create a new Edge Device in the IEM with self-signed certificates or certificates from the IEM and enter the IP address of the Edge Device into the Internet browser, you notice that the connection is not secure. After you browse the created configuration file of the Edge Device and connect the Edge Device to the IEM, the connection to the Edge Device is still not secure. Import the self-signed certificates or the certificates from the IEM to the settings of the Internet browser according to the "Importing certificates to the Internet browser" subsection and to the Edge Device according to the "Importing certificates" subsection, both described in the "Industrial Edge Management - Operation (https://support.industry.siemens.com/cs/us/en/view/109780393)" manual. After you imported the certificates, refresh the Internet browser of the Edge Device UI. The connection is secure now.

Connected Edge Device with wildcard or SAN certificates

When you create a new Edge Device in the IEM with wildcard or SAN certificates and enter the IP address of the Edge Device into the Internet browser, you notice that the connection is not secure. After you browse the created configuration file of the Edge Device and connect the Edge Device to the IEM, the connection to the Edge Device is secure. This secure connection requires that the CA-chain is imported to the settings of the Internet browser.

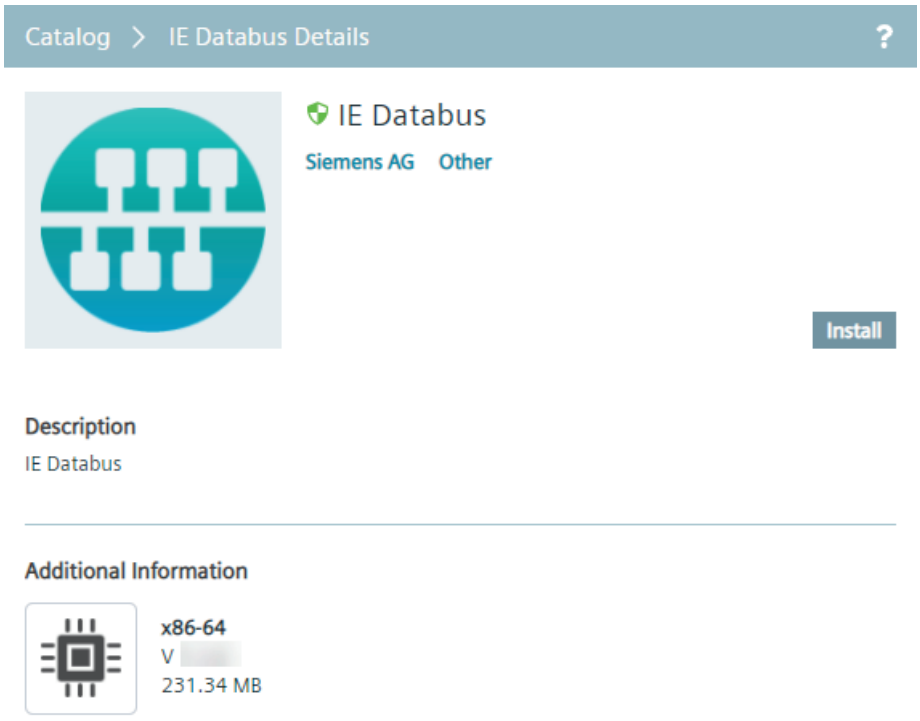
5.3 Installing system apps on Edge Devices

Requirement

- Minimum 1 Edge Device is connected and running in the IEM.
- The system app is available in the IEM catalog.

Procedure

1. In the navigation menu in the IEM, click "Catalog".
2. Click the tile of the system app, in this example the "IE Databus" app.
   The details of the system app are displayed.



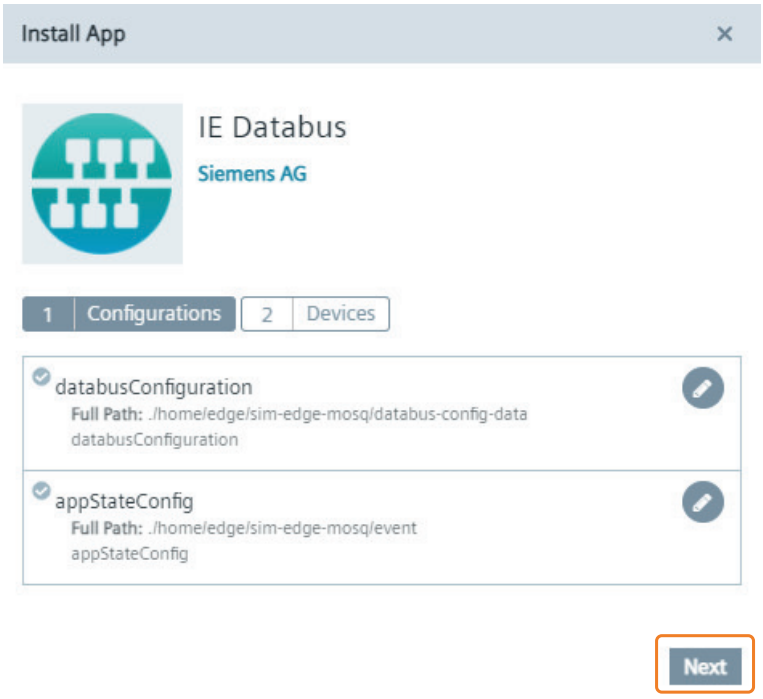
Note

Verified Edge Apps

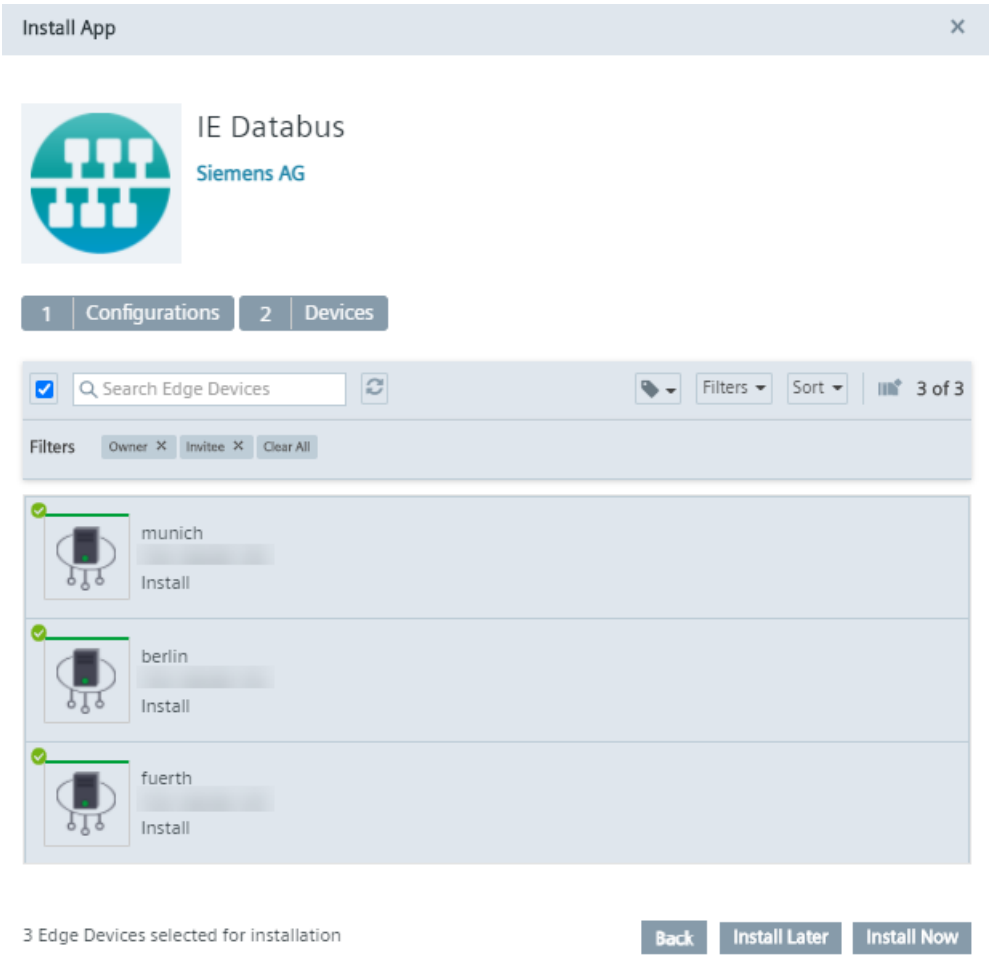
Verified and trusted Edge Apps by Siemens are marked with the icon.

3. Click "Install".
   The "Install App" screen is displayed.

4. Without selecting a configuration, click "Next".



5. Select the Edge Devices on which you want to install the system app.



You can select several Edge Devices to install the app to.
The system configurators are only available for the Edge Devices on which the specific system apps are installed.

6. Click either "Install Later" or "Install Now".
"Install Now" installs the app immediately. When you click "Install Later", select an installation time.
You can check the installation status in the "Job Status" menu item.

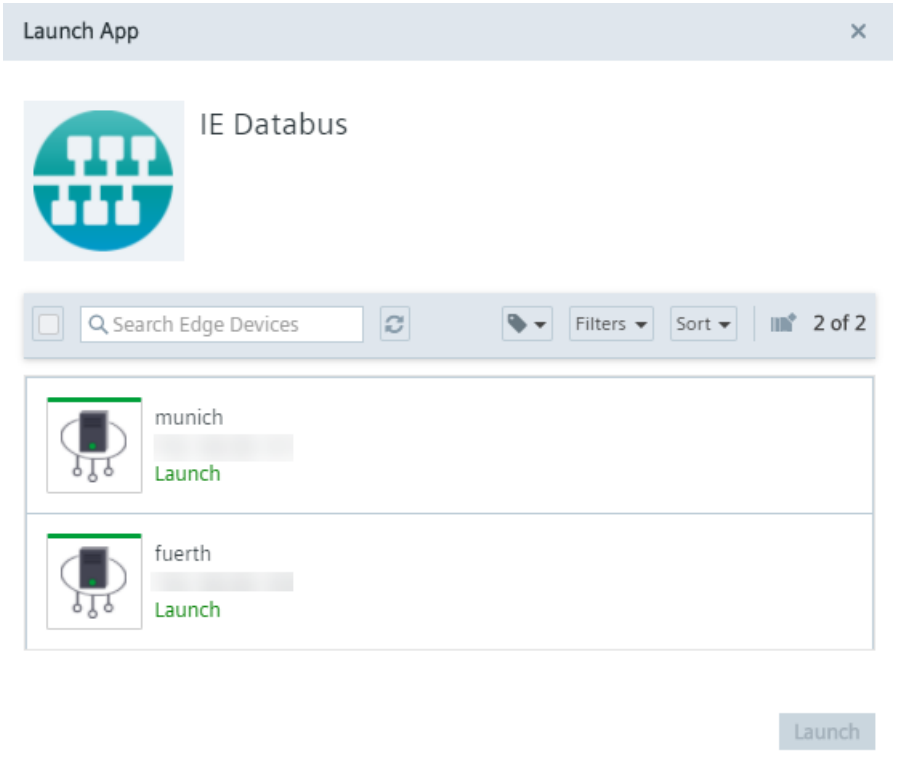
5.4 Launching system apps

Requirement

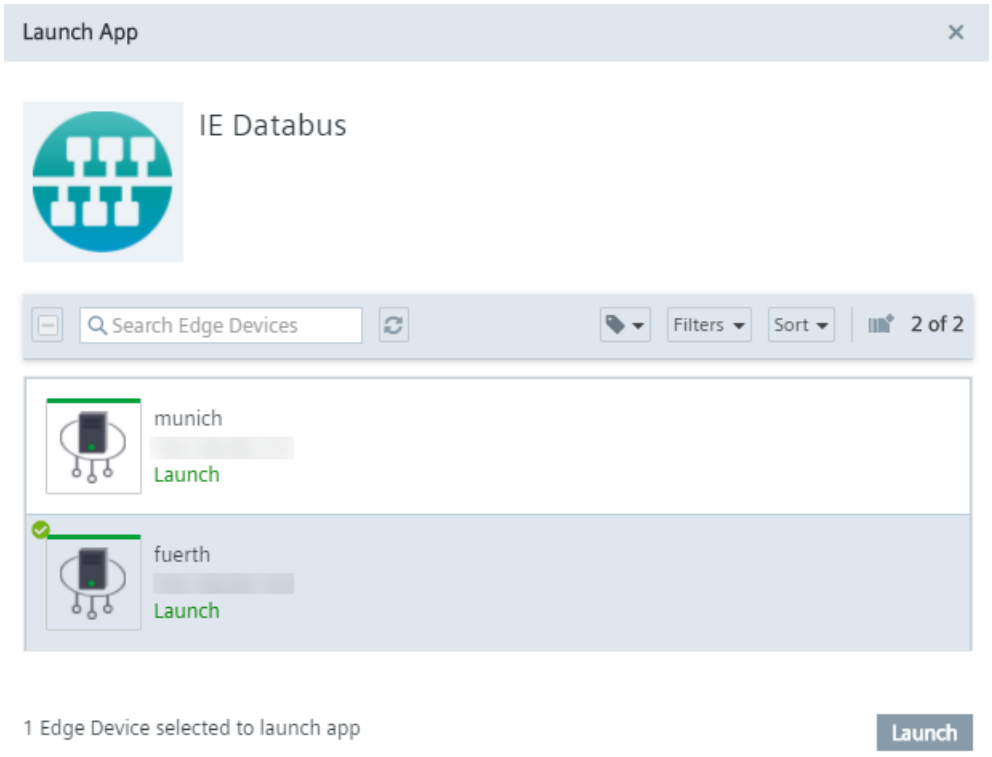
- The system app is installed on an Edge Device.
- The according system configurator is installed on the IEM-OS.

Launching system apps

1. In the IEM, navigate to "Data Connections".
   The available system apps are displayed in the "All System Apps" tab.
2. Click the tile of the respective system app.
   The "Launch App" screen is displayed.



3. Select the desired Edge Device on which the system app is installed.



You can only select 1 Edge Device. Only Edge Devices on which the system app is installed are available.

4. Click "Launch".
The system app is launched and opened in a new tab inside the "Data Connections" screen. In that way, you can open several system apps on different Edge Devices and swicth between the apps through the tabs.

The tab displays the app name and the respective Edge Device.

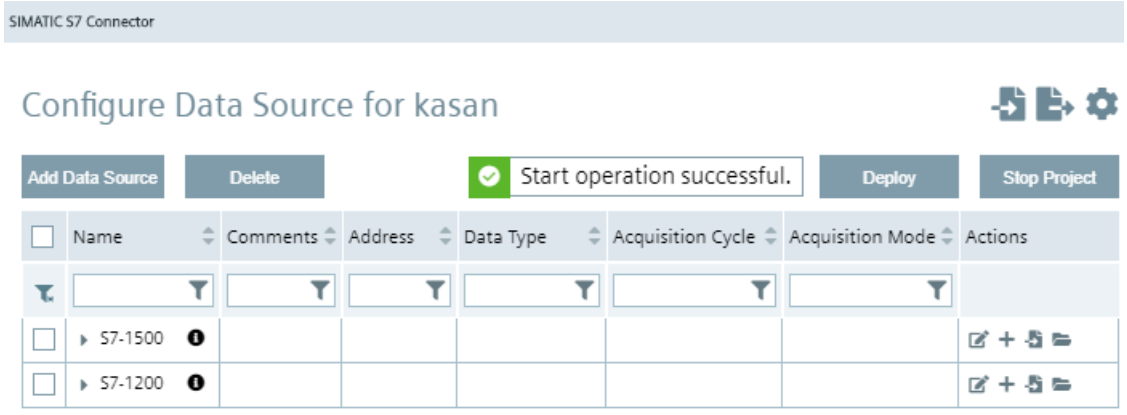
Working with the IEM

6

The IEM runs and you want to use data from your controllers for your own developed apps or for the Edge Apps from the IE Hub.
Execute the steps described in the following to dispose of your data and use these data for your tasks.

Procedure

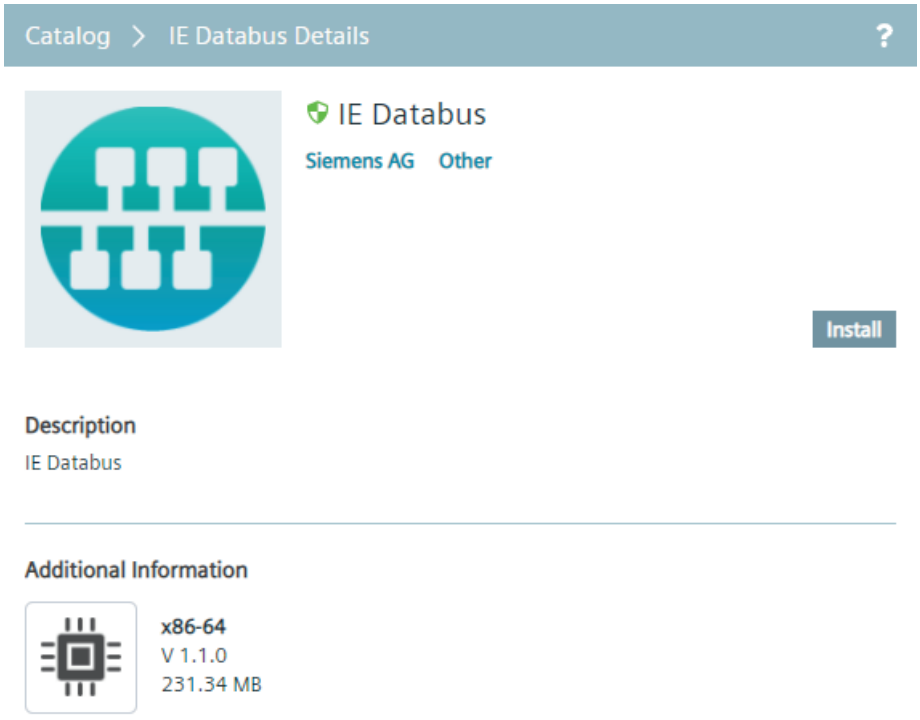
1. After adding Edge Devices to your IEM and installing the system apps on the Edge Devices, use the SIMATIC S7 Connector Configurator to connect the controllers in your plant network with the Edge Device in your IEM.



You find information on connecting controllers with your Edge Devices in the operating manual of the SIMATIC S7 Connector Configurator (https://support.industry.siemens.com/cs/us/en/view/109783783).

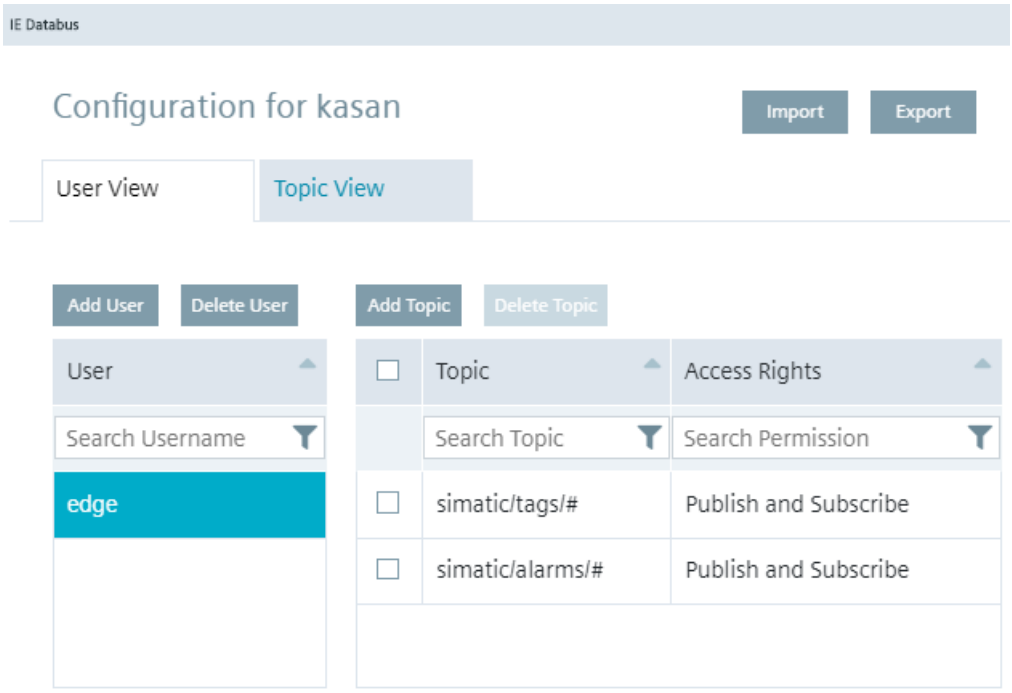
2. Publish your own app into the IEM by using the IE App Publisher or copy respectively transfer available Edge Apps from the IE Hub to the IEM.

3. Use the "Applications > My Projects" menu item to install your own app, or the "Catalog" menu item to install public Edge Apps from the IE Hub, on your Edge Devices.



You find information on installing apps in the IEM in the "Applications > My Projects" respectively in the "Catalog" section in the "Industrial Edge Management - Operation (https://support.industry.siemens.com/cs/us/en/view/109780393)" manual.

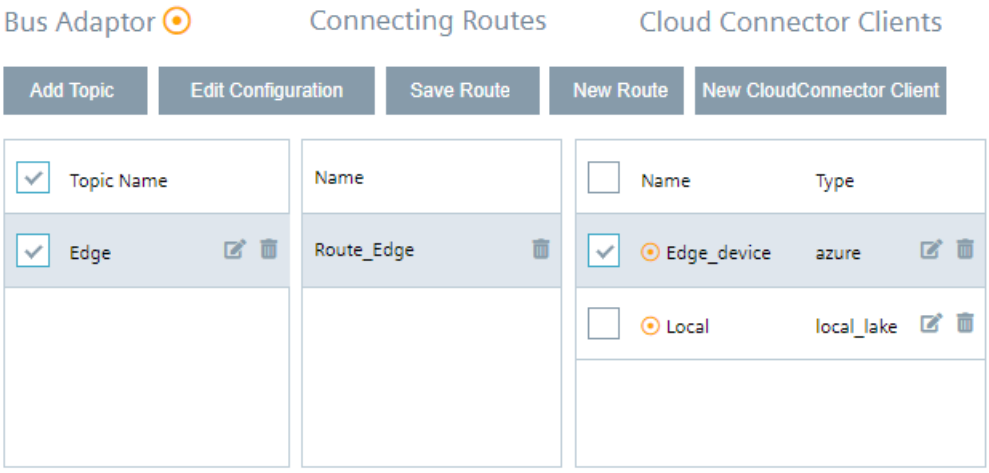
4. Use the IE Databus Configurator to grant your app access to data of the controllers that you have configured through the SIMATIC S7 Connector Configurator.



You find information on access rights for IE Databus data in the operating manual of the IE Databus Configurator (https://support.industry.siemens.com/cs/us/en/view/109783784).

5. Open respectively start your app from the Edge Device UI of the Edge Device on which the app is installed.

6. Use the data of your app for your tasks.
7. If you want to send data to the cloud, use the IE Cloud Connector Configurator.



You find information on sending data to the cloud in the operating manual of the IE Cloud Connector Configurator (https://support.industry.siemens.com/cs/us/en/view/109783786).

Example of use - Monitoring bottle filling process 7

7.1 Description

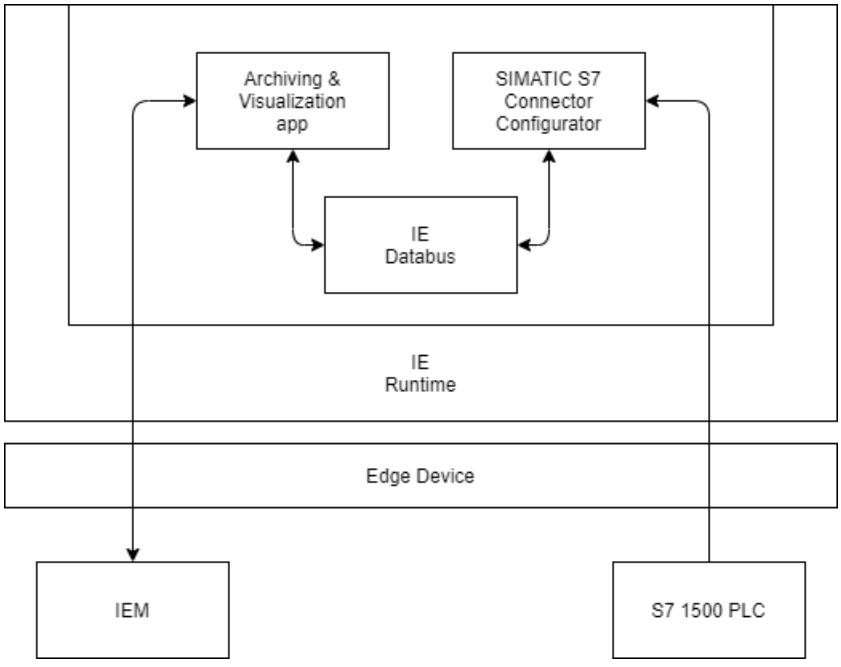
This example uses the self-created "Archiving & Visualization" app which is based on a bottle filling process application from which data values are collected, stored in an Influx-Database (InfluxDB) and visualized via a Grafana dashboard.

General task

The "Archiving & Visualization" app collects data from an S7-1500 PLC by using the SIMATIC S7 Connector Configurator. The collected data is automatically published to the IE Databus which is an internal MQTT broker of Industrial Edge. The "Archiving & Visualization" app uses a MQTT client (data collector) to subscribe to the IE Databus and write these values into an Influx-Database. The time series of the collected data can then be plotted within the Grafana dashboard.

Structural overview

The following figure shows a simplified structural overview of this example:



7.2 System setup and requirements

System setup

This example is applied with the following system setup:

- Industrial Edge App Publisher: V1.2.7
- Industrial Edge Management: V1.2.0
- SIMATIC S7 Connector Configurator: V1.2.8
- SIMATIC S7 system app: V1.2.26
- IE Databus Configurator: V1.2.20
- IE Databus system app: V1.2.16
- Industrial Edge Device: V1.0.0

Additional tools and requirements

- OS: Linux
- Docker version 18.09
- Docker-compose version 2.4
- Development environment Visual Studio Code
- TIA Portal V16
- PLC: CPU 1511 FW 2.8.3

SIMATIC S7 Connector Configurator

In this example, the SIMATIC S7 Connector Configurator is used in the "Bulk Publish" mode to collect tags from the TIA Portal project "Tank Application". The used PLC name is "PLC_1" and the following tags are being collected:

- GDB_signals_tankSignals_actLevel (Read/100ms)
- GDB_signals_tankSignals_actTemperature (Read/100ms)
- GDB_process_numberProdued (Read/100ms)
- GDB_process_numberFaulty (Read/100ms)
- GDB_hmiSignals_HMI_Nextbottle (Read&Write/100ms)

IE Databus Configurator

In this example, the IE Databus Configurator is configured with following parameters:

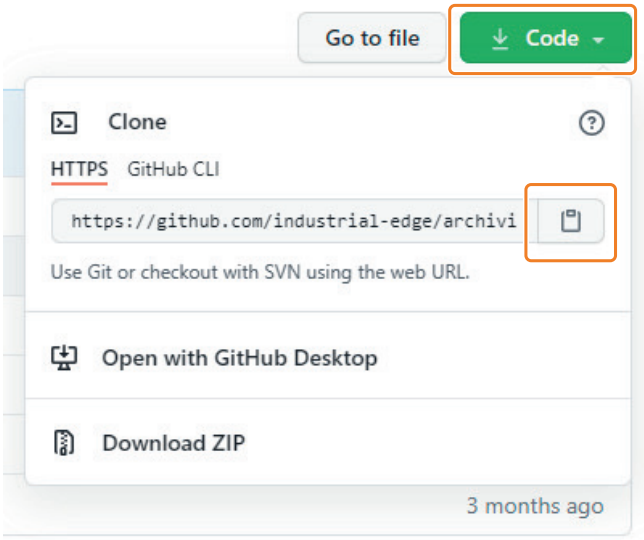
- Topic: ie/#
- Username: edge
- Password: edge

7.3 Building the app

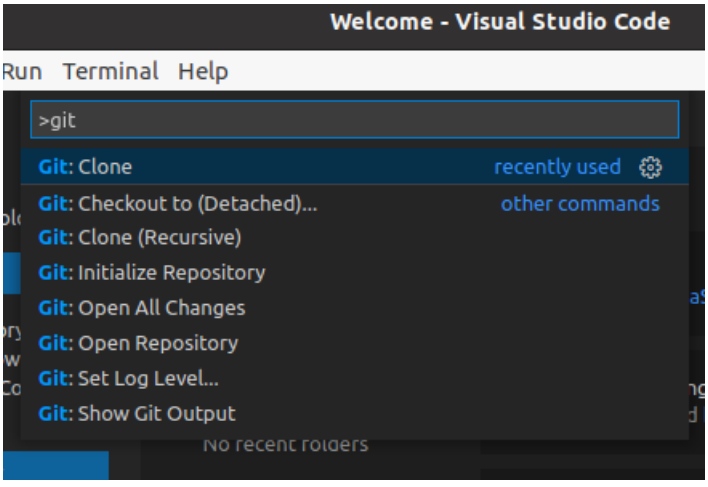
To build respectively create the app, you must download the needed resources from a public Github repository and afterwards build the app in your IDE, in this case Visual Studio Code.

Procedure

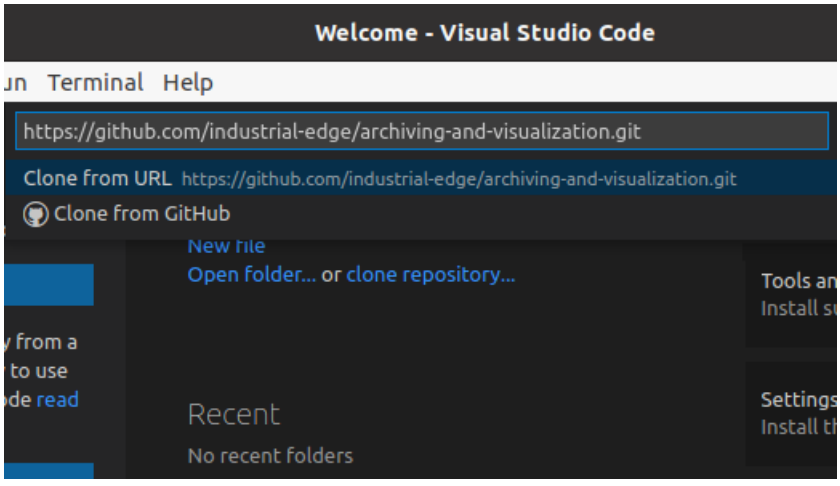
1. Open the Github repository under the following link (https://github.com/industrial-edge/archiving-and-visualization).
2. Clone the repository by clicking "Code" and the download icon under the "HTTPS" section.



3. Open Visual Studio Code.
4. Display the command palette by entering <CTRL>+<SHIFT>+<P>.
5. In the command palette, search for "Git: Clone" and select it.



6. Paste the cloned GitHub repository and perform the "Clone from URL" command.



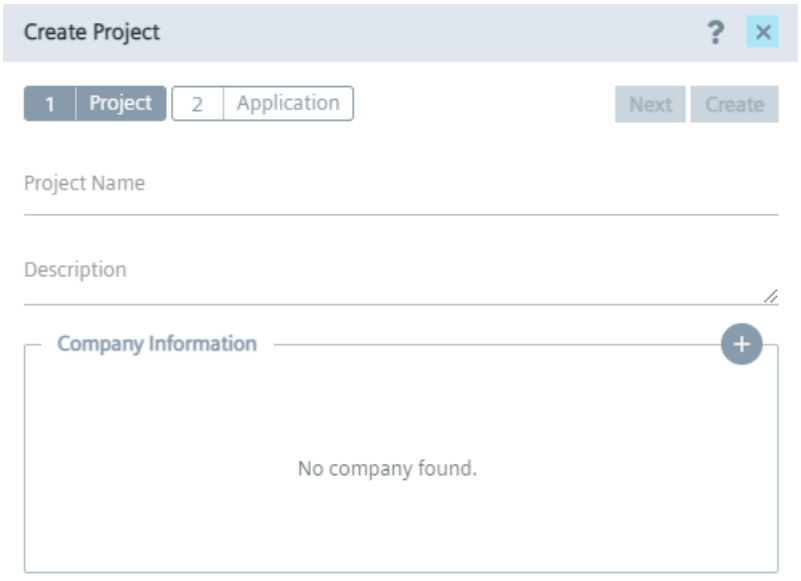
7. Select or create the folder you want to clone the repository to.
   The repository is cloned to the selected folder.
8. In the command shell, navigate to the ".../archiving-and-visualization/" folder of the cloned repository.
   The docker-compose.yml file should be located in this folder.
9. Build the app by entering the `docker-compose build` command into the command shell.
   The InfluxDB and Grafana container are being created.

7.4 Creating the project and app in the Industrial Edge Management

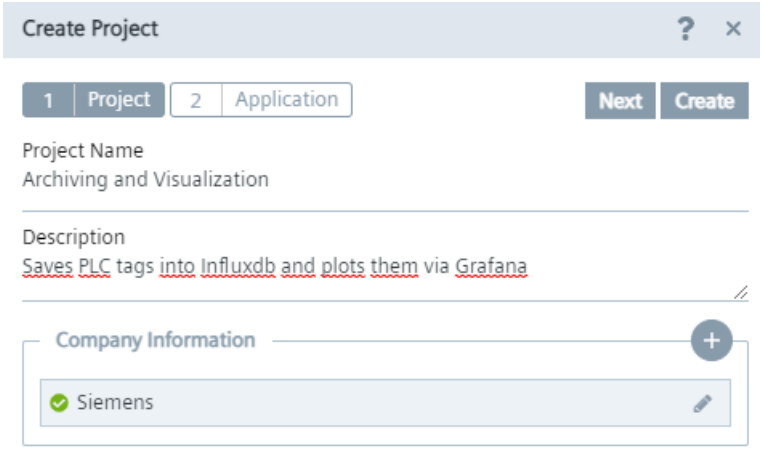
Procedure

1. Open and log into the IEM.
2. Navigate to "Applications > My Projects".

3. Create an own project for the app by clicking "Create Project".
   The "Create Project" screen is displayed.

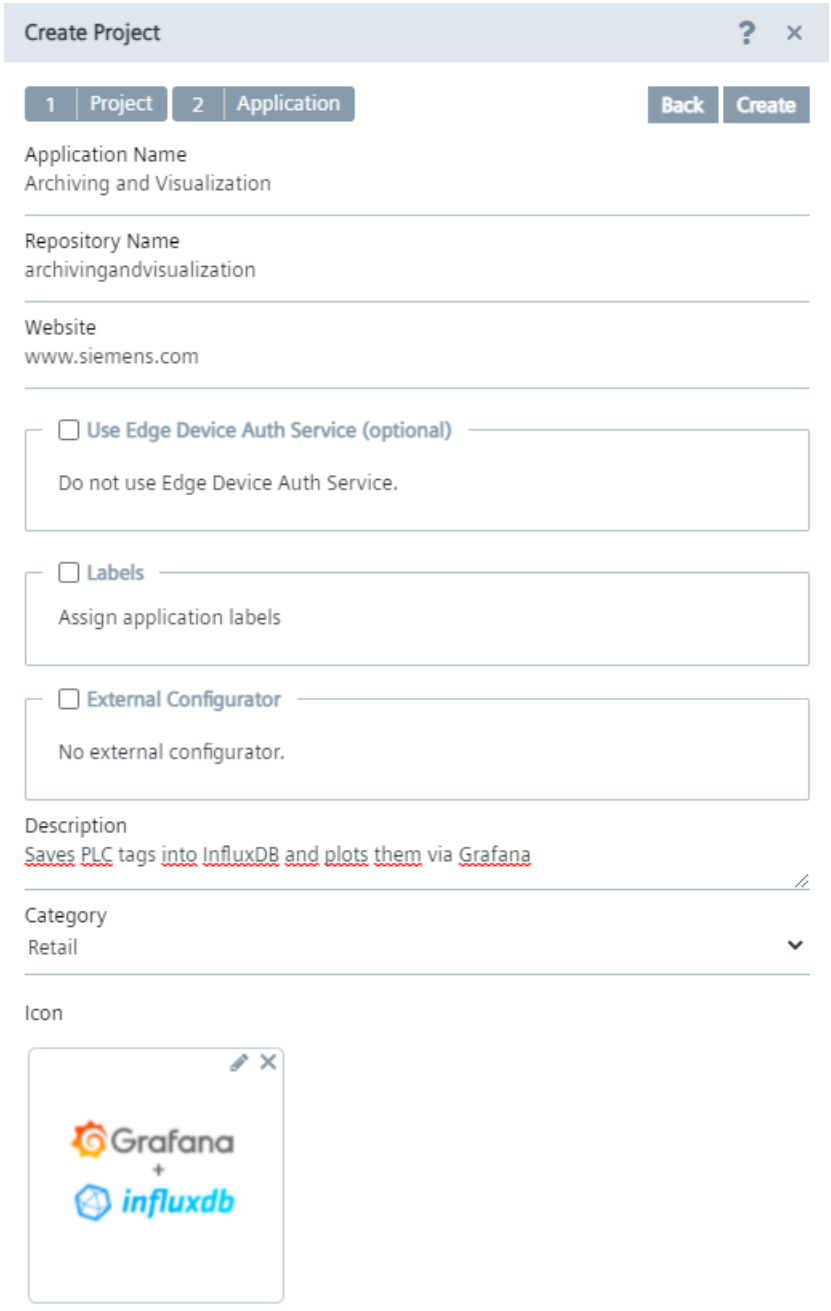


4. Enter all required information:
   - Project Name
   - Description
   - Company Information



5. Click "Next".
   In the following screen you create the app on the IEM side.

6. Enter all required information:
   - Application Name
   - Repository Name
   - Website
   - Description
   - Category
   - Icon



Note

"Use Edge Device Auth Service", "Labels" and "External configurator"

Do not select these options since it is not required for this app.

7. Click "Create".
   The project and app has been created in the IEM.
   Now you must create the app version including its configuration in the IE App Publisher and upload it to the created project respectively app.

7.5 Creating the app version in the IE App Publisher

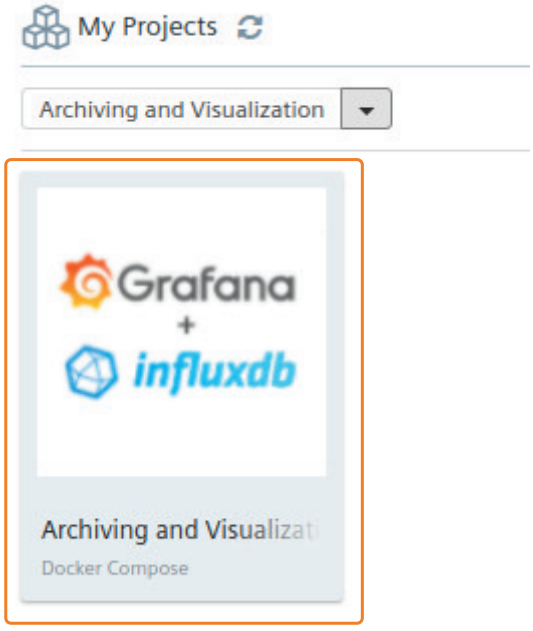
Requirement

- Connected to the IEM.
- Connected to a Docker engine.

You find information on how to connect to the IEM and to a Docker engine in the "Connecting the IE App Publisher" section in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

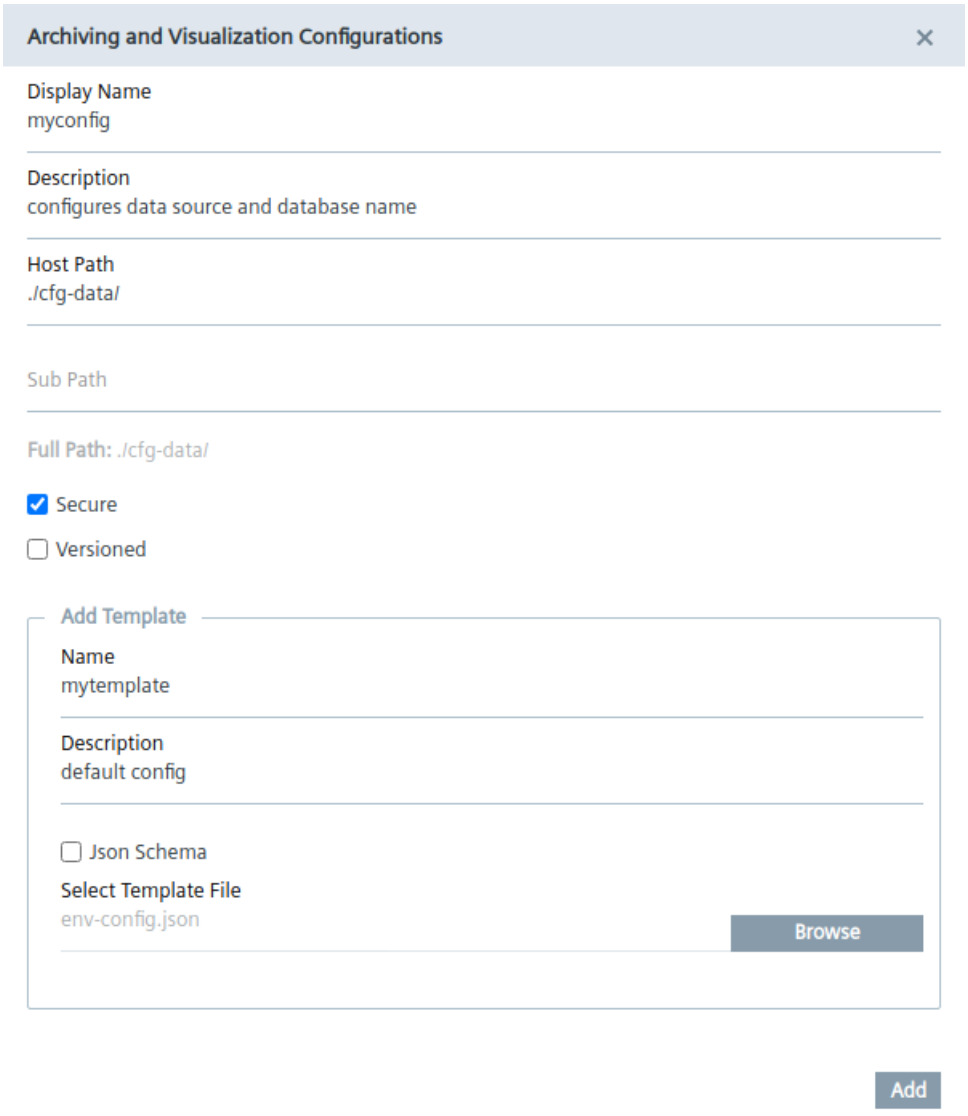
Procedure

1. Open and log into the IE App Publisher.
2. In the "My Projects" section, select the created project and click the newly created app tile.

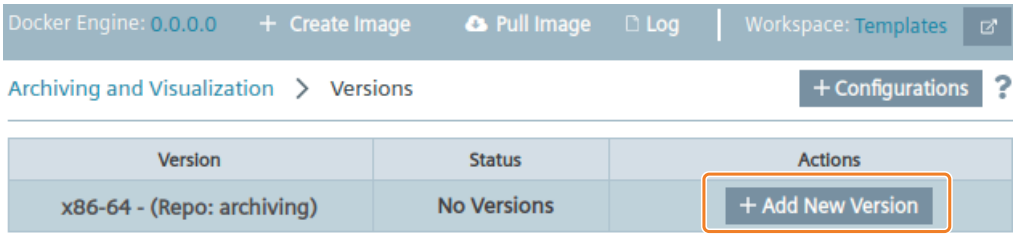


   The version table is displayed.
3. Click "Configurations".
4. Add a new configuration by clicking "Add Configuration".
   The app configuration screen is displayed.
5. Enter all required information:
   - Display Name
   - Description
   - Host Path
   - Template Name
   - Template Description
   - Template File

6. For the template file, click "Browse" and select the "env-config.json" file which is contained in the ".../cfg-data/" folder in the cloned repository.

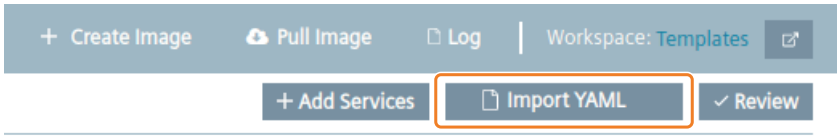


7. Click "Add".
   The app configuration has been created.
8. In the version table, click "Add New Version".

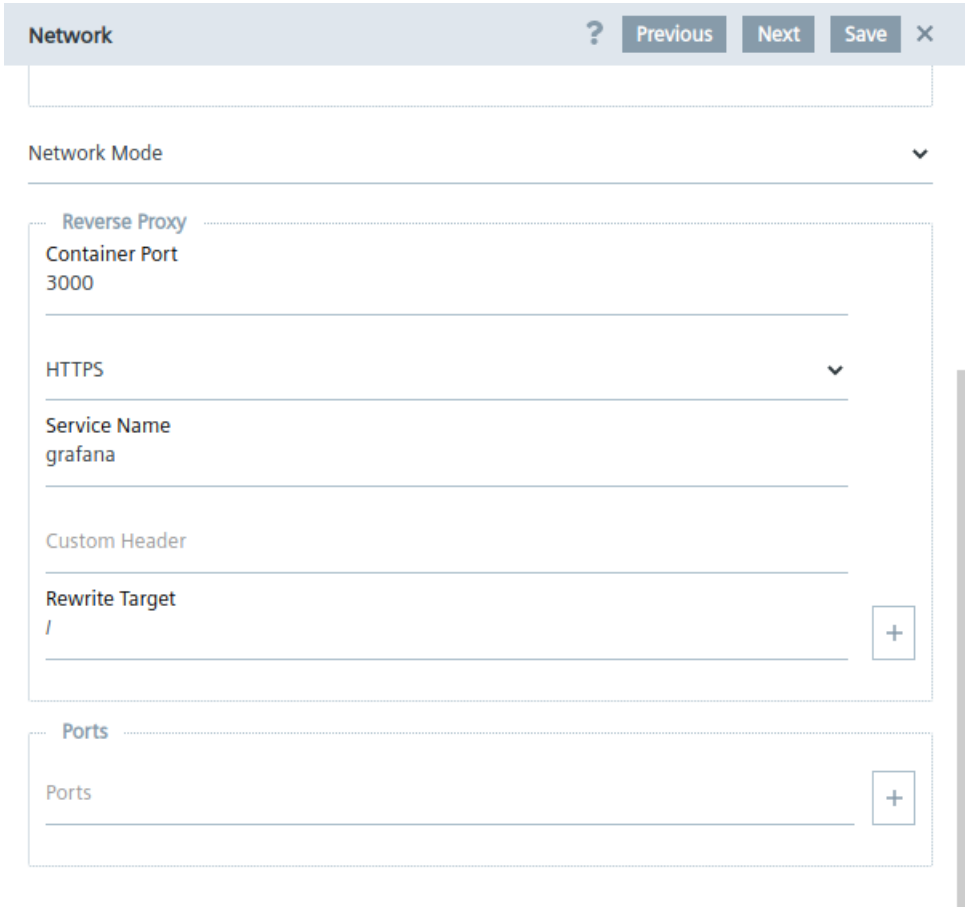


   The "Create Version" screen is displayed.

9. From the drop-down list, select the 2.4 docker-compose version and click "Ok".
10. Click "Import YAML" and select the "docker-compose.yml" file from the cloned repository.



11. Click "Ok".
    The contained services and network parameters are displayed.
12. If needed, configure a reverse proxy by clicking the icon in the "grafana" service section and clicking the "Network" tile.
    In the "Network" screen, add the reverse proxy information.



Note

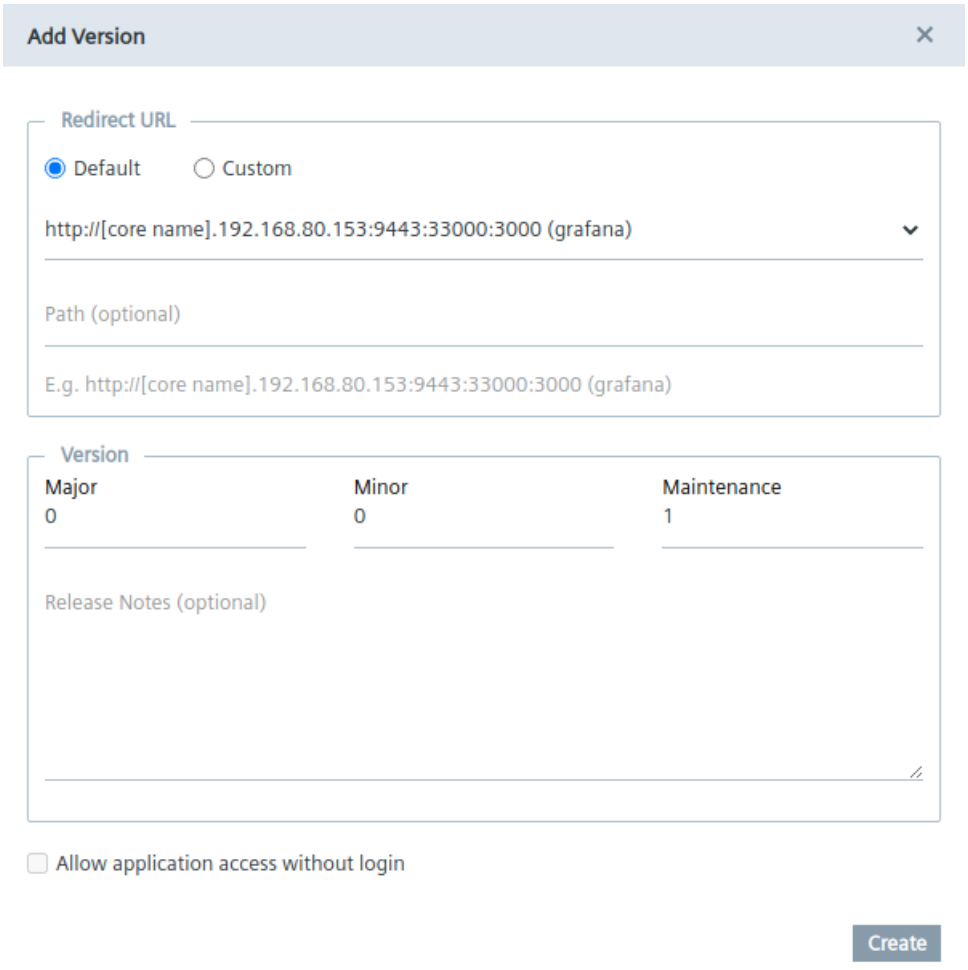
Port exposure

Port exposure must be removed in this case. For that, click the icon at the bottom of the "Network" screen.

After you have configured, the reverse proxy, save the changes.

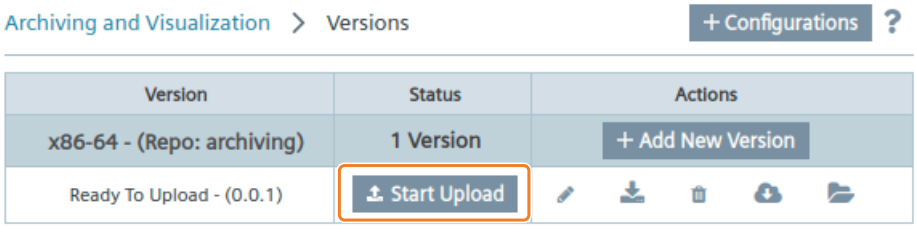
13. Click "Review".

14. Click "Validate & Create".
    The "Add Version" screen is displayed.



15. Click "Create".
    This process may take some time. After the app version has been created, the version is listed in the version table and ready to upload.

16. Click "Start Upload".

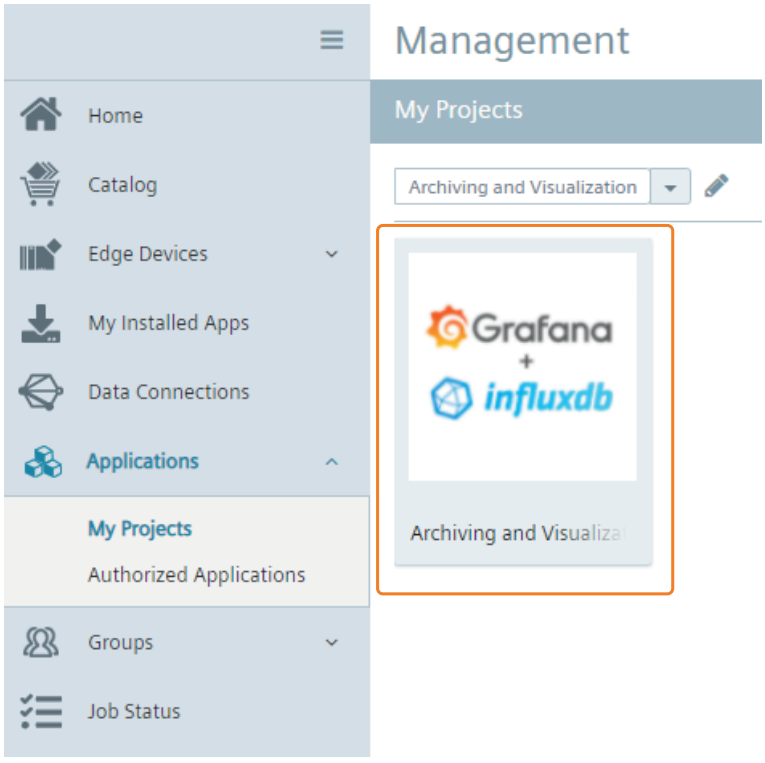


The app version is getting uploaded to the IEM. Once the app version is successfully uploaded to the IEM, you must install the app version onto your Edge Device.

7.6 Installing the app

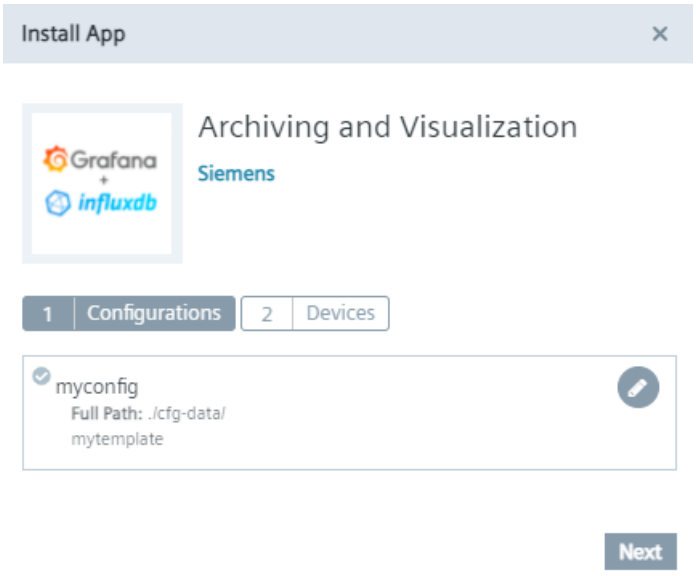
Procedure

1. In the IEM, navigate to "Applications > My Projects".
2. Click the tile of the created app.

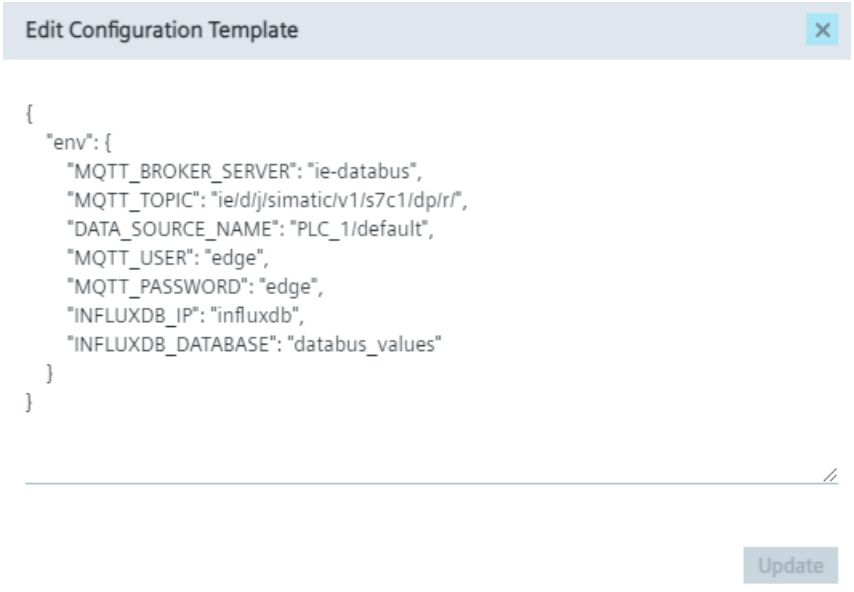


All available versions of the app are displayed.

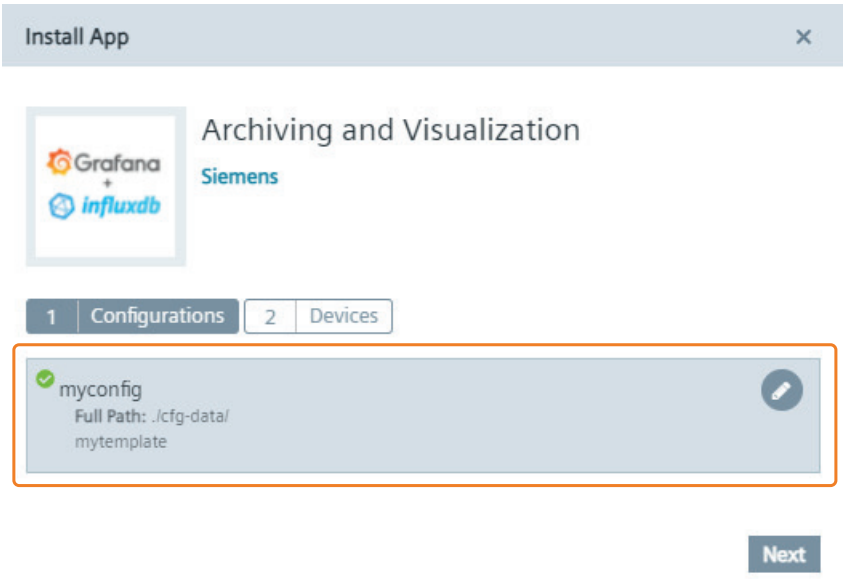
3. Install the app version by clicking the icon under "Actions".
   The "Install App" screen is displayed.



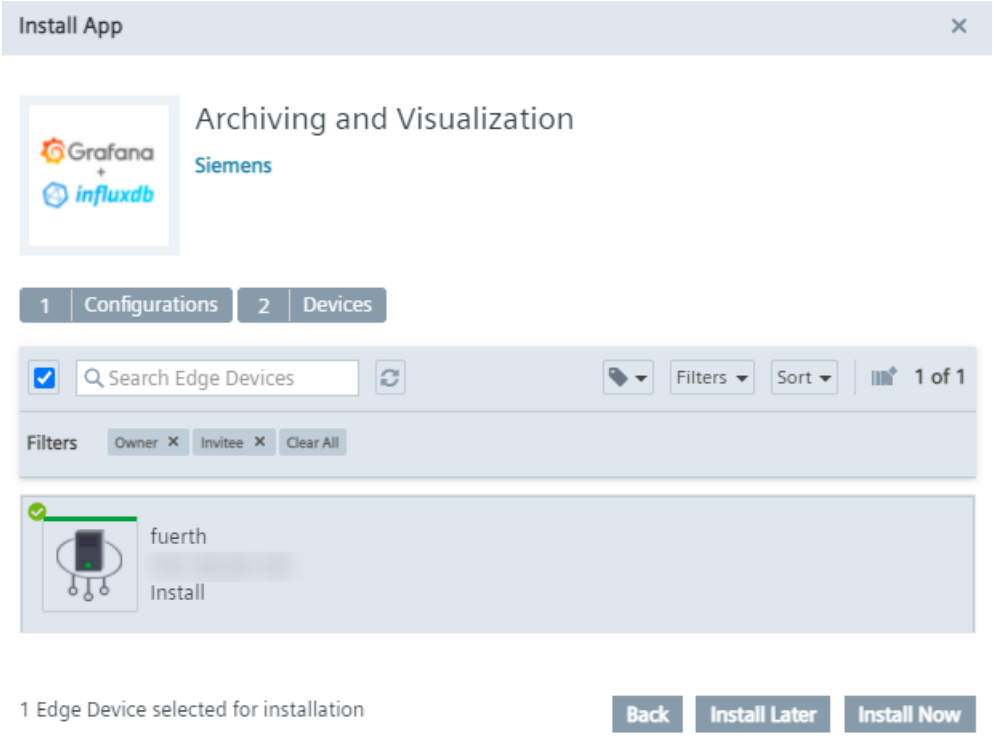
4. In the "Configurations" tab, click the icon to review your configuration file.
   Based on this configuration, you can configure the app to use a different database name, different credentials for the IE Databus or a different datasource name.
   In this example, "PLC_1/default" is entered under "DATA_SOURCE_NAME" because the used PLC name in the SIMATIC S7 Connector is "PLC_1" and the "Bulk Publish" publish option is enabled, so the "default" keyword is needed.



5. Select the configuration file.



6. Click "Next".
7. Select the Edge Device on which you want to install the app.



8. Click "Install Now".
9. Click "Allow" to install the app.
   The app is being installed. You can check the installation status in the "Job Status" menu item. When the app has been installed successfully, you can start the app from the Edge Device UI of the respective Edge Device.

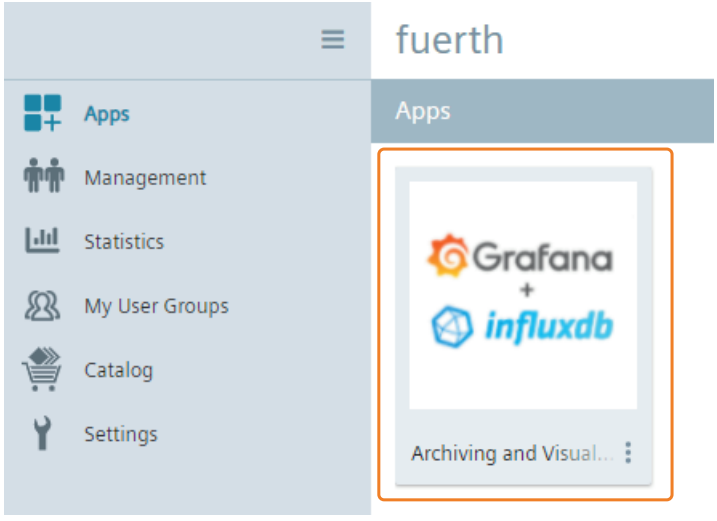
7.7 Starting the app

Requirement

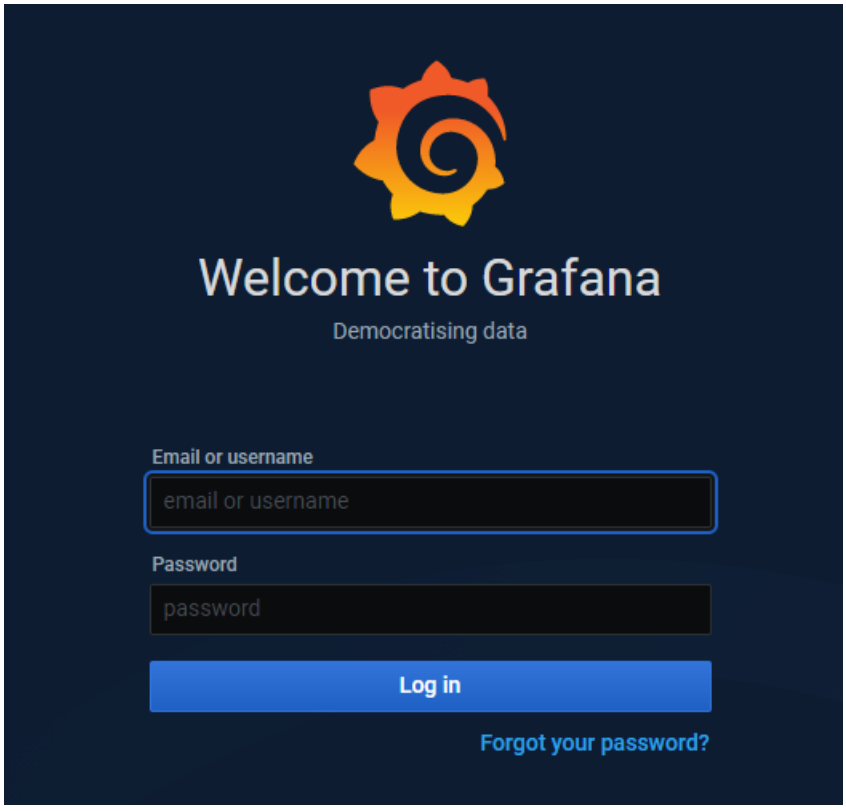
- The SIMATIC S7 Connector project is started.
- Your PLC is in "Start" mode.
- "GDB".hmiSignals.HMI_Start is set to TRUE on your PLC.

Procedure

1. Open and log into the Edge Device UI on which you installed the app.
2. In the "Apps" screen, click the tile of the app to start it.

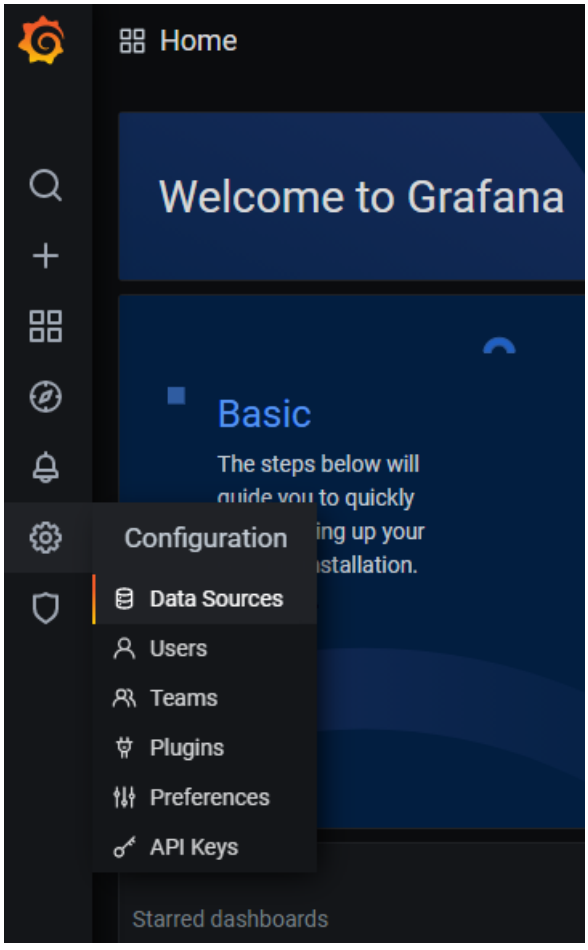


The app will be opened in a new tab and the Grafana login screen is displayed.



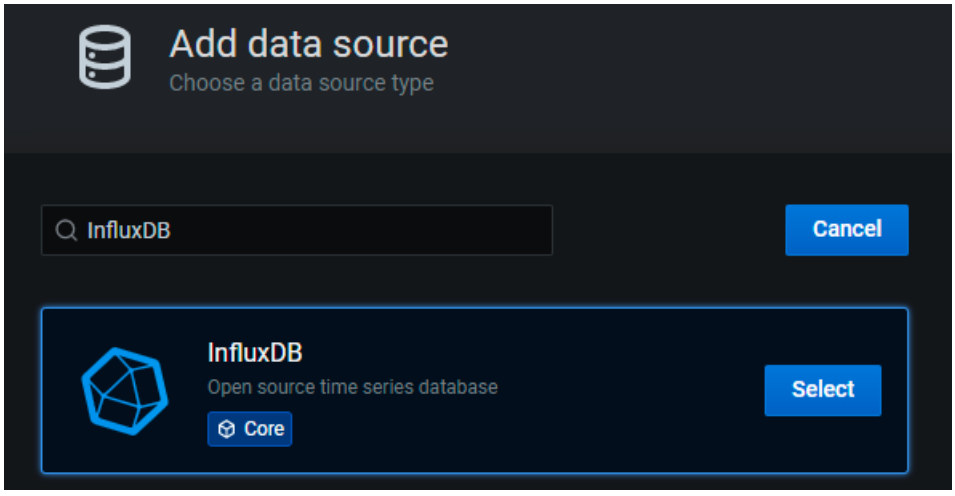
3. Log in with the following credentials:
   - Username: admin
   - Password: admin

4. Change the password.
   The Grafana home screen is displayed.
5. On the left side, navigate to "Configuration > Data Sources".



6. Click "Add data source".

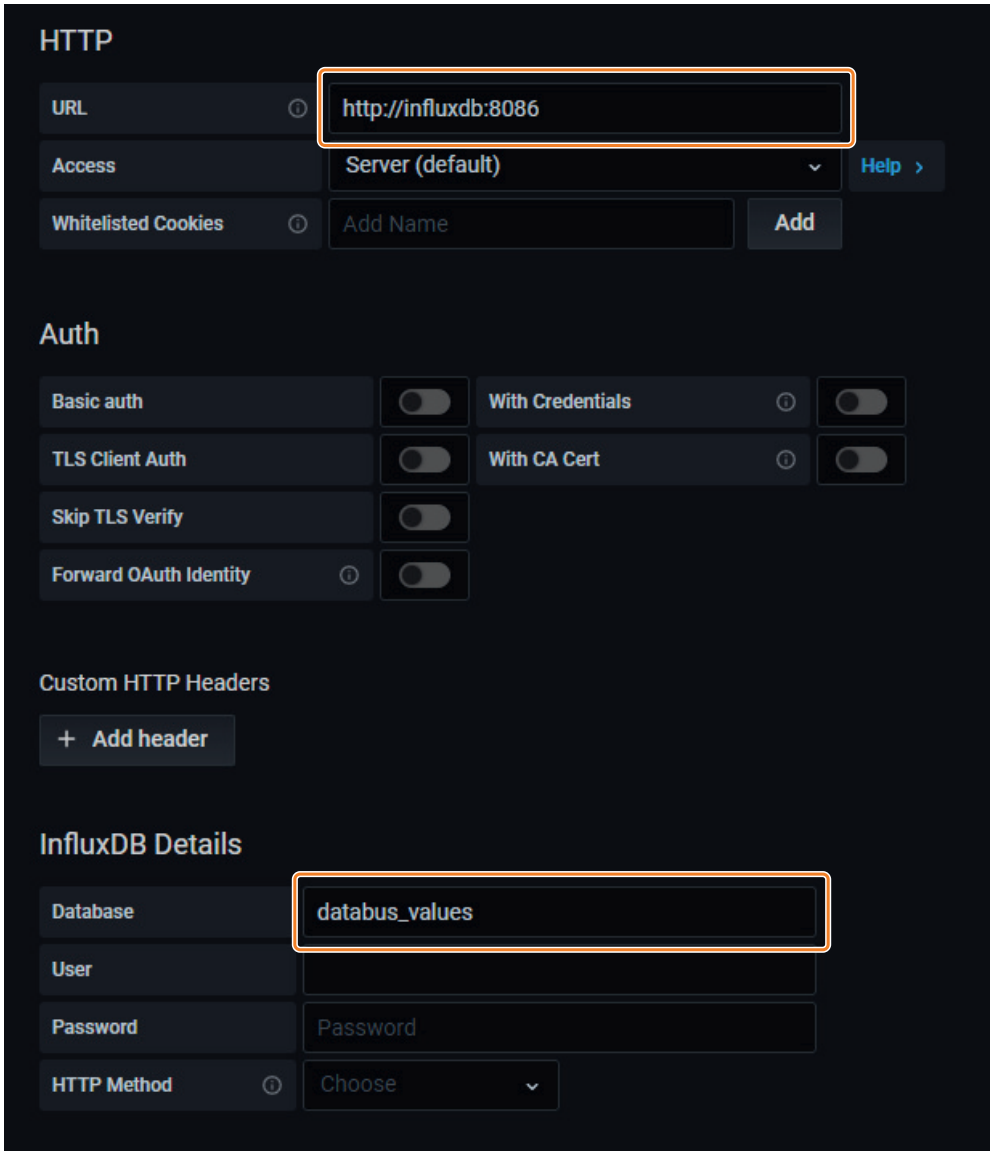
7. Add the new "InfluxDB" data source by entering "InfluxDB" in the search bar and selecting it.



   The data source is added.

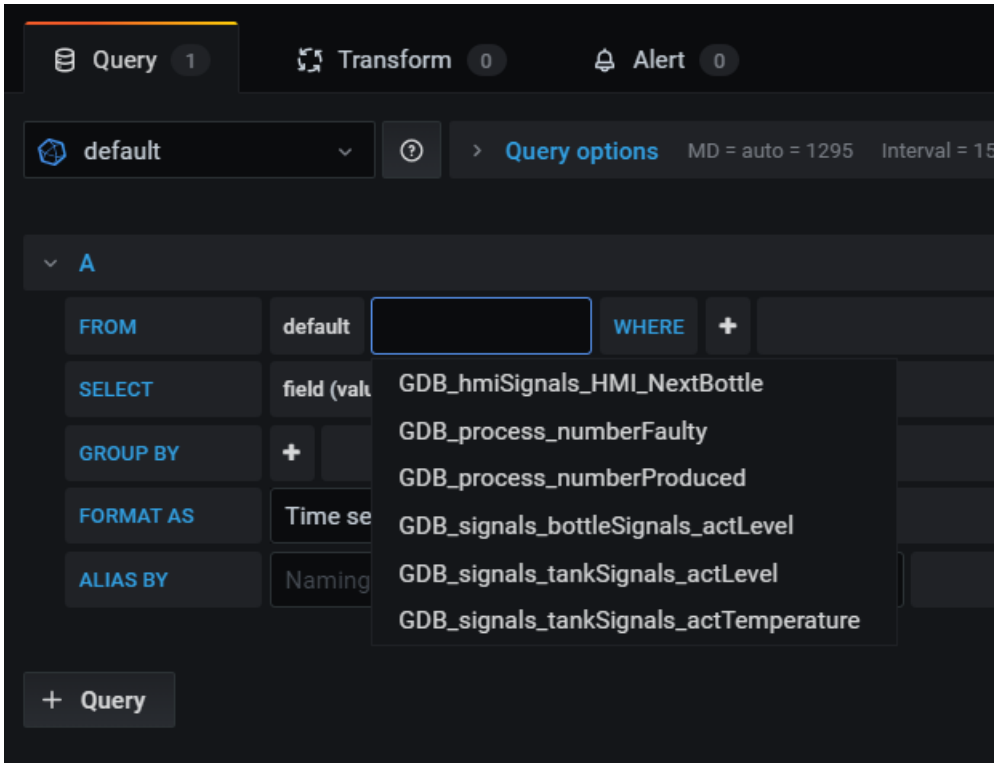
8. In the "URL" input field under the "HTTP" section, enter the "http://influxdb:8086" address.

9. In the "Database" input field under the "InfluxDB Details" section, enter the "databus_values" database name.



10. Click "Save & Test".
    You should receive a notification "Data source is working". If not, you might have selected a different name in the configuration file. In that case, check again the configuration file.

11. In the "Dashboard" section, add a new panel.
    You are able to select and configure your tags.



12. Select the values you want to plot.

13. Remove the "Group By" options and the "SELECT mean(value)" option.
    The tag values, and by that the bottle filling process, are displayed and monitored via the dashboard.

List of abbreviations/acronyms

8

Abbreviation	Description
IE	Industrial Edge
IED	Industrial Edge Device
IEH	Industrial Edge Hub
IEM	Industrial Edge Management
IERT	Industrial Edge Runtime
IEAP	Industrial Edge App Publisher
IED-OS	Industrial Edge Device Operating System
IEM-OS	Industrial Edge Management Operating System
VM	Virtual machine
UI	User Interface
CLI	Command Line Interface
SFC	SIMATIC Flow Creator
SAS	Shared Access Signature
SSH	Secure Shell
IoT	Internet of Things
DHCP	Dynamic Host Configuration Protocol
API	Application Programming Interface
TPM	Trusted Platform Module
LAN	Local Area Network
FQDN	Fully Qualified Domain Name
NTP	Network Time Protocol
L2	Layer 2
LLDP	Link Layer Discovery Protocol
CIDR	Classless Inter-Domain Routing
DR	Disaster Recovery
IE ACS	Industrial Edge Application Configuration Service
IEDK	Industrial Edge Device Kit

Glossary

3rd Party Industrial Edge App

3rd Party IE Apps are not provided by Siemens, but by 3rd party providers.

Centrally-managed Edge

Edge Device and Edge App management is done centrally in the Industrial Edge Management.

Device-managed Edge

Edge Device and Edge App management is done on the Edge Device itself, for example HMI Unified Comfort Panels.

Industrial Edge Access

Offer that is available in the Siemens Industry Mall. The offer includes access to the Industrial Edge Hub.

Industrial Edge App Publisher (IEAP)

Software application that enables packaging and publishing of Industrial Edge Apps. The IEAP is available as Linux and Windows application.

Industrial Edge Cloud Connector

System app for data distribution to data services of cloud providers.

Industrial Edge Cloud Connector Configurator

System Configurator for the IE Cloud Connector. In contrast to the IE Cloud Connector, the IE Cloud Connector Configurator is executed in the IEM and not on the Edge Device.

Industrial Edge Databus

System app for data distribution in Industrial Edge.

Industrial Edge Databus Configurator

System Configurator for the IE Databus. In contrast to the IE Databus, the IE Databus Configurator is executed in the IEM and not on the Edge Device.

Industrial Edge Device License

License (subscription) which customers purchase from Siemens. The Edge Device license includes the annual fee for each Industrial Edge Device that is centrally managed through an IEM.

Industrial Edge Device OS (IED-OS)

Software (Operating System) that is running on an Edge Device. The IED-OS enables hardware to be managed as Edge Device. The IED-OS file also includes versioning and device family flavor in the scheme "IED-OS-".

Industrial Edge Ecosystem

Ecosystem which will be built around Industrial Edge. This includes Edge Devices, their publishers, as well as app and solution partners.

Industrial Edge Management On-Premises

IEM On-Premises describes the installation and use of IEM on computers at the premises of the organization using the software, not at a remote facility. IEM is operated by the customer.

Industrial Edge Management OS (IEM-OS)

Software (Operating System) that is running in a VM to enable the IEM.

Industrial Edge Runtime (IERT)

Software component that is running within the IEM-OS and IED-OS.

Industrial Edge System Apps

Application that is provided with the IEM. A system app provides basic functionality, such as connectivity to the shop floor. System apps are the entry point for a variety of customer tasks. System apps include SIMATIC S7 Connector, Industrial Edge Databus, and Industrial Edge Cloud Connector.

In comparison to Edge Apps, system apps are shipped with the IEM by default and are given special rights because they provide essential functionality for the IEM.

Industrial Edge App

Self-contained entity which contains functionality that creates value for the customer. It can consist of 1 or more Docker containers.

Industrial Edge Device (IED)

A standalone hardware device (inclusive firmware) with the purpose of providing Industrial Edge functionality.

Industrial Edge Hub (IEH)

The Industrial Edge Hub (IEH) is the entry point for Siemens customers into Industrial Edge and the central starting point for downloading and configuring the Industrial Edge Management (IEM). In the IEH, you download all necessary software for running the IEM and manage licenses of purchased Edge Apps and Edge Devices. Also, the IEH provides a global catalog from which you download Edge Apps and distribute to the Industrial Edge Management.

Industrial Edge Management (IEM)

Central user interface of Industrial Edge. The IEM provides Edge App and Edge Device management, as well as system-internal configurations, such as the settings for connections to controllers. The IEM is enabled by the IEM-OS that is running in a VM.

Secrets

Secrets are sensitive data that generally must be protected.

Side loading

Functionality that allows Edge Apps to be loaded onto an IEM without interaction with the IE Hub.

Siemens Industrial Edge App

Edge App that is developed by an app partner of Siemens.

SIMATIC S7 Connector

System app that provides connectivity to the plant network.

SIMATIC S7 Connector Configurator

System Configurator for the SIMATIC S7 Connector. In contrast to the SIMATIC S7 Connector, the SIMATIC S7 Connector Configurator is executed in the IEM and not on the Edge Device.

Topic

A topic is a permanently defined access area. Measured data can be sent to a specific topic or access area. Only users who have access to the area are allowed to use the data. The access area is defined by the name of the topic.