

Industrial Edge Management - Getting Started

Getting Started

Preface

Industrial security

1

Overview and setup

2

Installing the system apps

3

Working with the IEM

4




List of
abbreviations/acronyms

5

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.

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/de/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/de/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 Management - Release notes (<https://support.industry.siemens.com/cs/de/en/view/109780394>)" manual.

An overview with regard to security and requirements for running the Industrial Edge Management and its components are included in the "Industrial Edge Management - Security overview and requirements (<https://support.industry.siemens.com/cs/us/en/view/109781002>)" 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 and setup	9
2.1	Overview of Industrial Edge	9
2.2	Industrial Edge Hub	11
2.2.1	Signing up	11
2.2.2	Signing in	15
2.2.3	Home	17
2.2.4	Market.....	18
2.2.4.1	Purchasing an Edge App license	19
2.2.5	Library	19
2.2.5.1	Copying the app to the IEM catalog	20
2.2.5.2	Opening documentation	20
2.2.6	Licenses.....	21
2.2.7	IEM Instances	22
2.2.7.1	Managing IEM instances	23
2.2.8	Download Software	23
2.2.9	Documents	23
2.3	Setting up the IEM	24
2.3.1	Setup steps.....	24
2.3.2	Downloading the Industrial Edge Management OS	25
2.3.3	Creating IEM instance and downloading the configuration file.....	26
2.3.4	VMware Workstation.....	27
2.3.4.1	Creating the VM.....	27
2.3.4.2	Configuring the VM	32
2.3.4.3	Installing the Industrial Edge Management OS	41
2.3.5	Oracle VirtualBox	43
2.3.5.1	Creating the VM.....	43
2.3.5.2	Configuring the VM	46
2.3.5.3	Installing the Industrial Edge Management OS	56
2.3.6	Configuring the Industrial Edge Management OS	59
2.3.7	Installing the IEM	62
2.3.8	Setting up a proxy server	70
2.3.9	Installing the system configurators.....	73
2.3.10	Adding a relay server	76

3	Installing the system apps.....	81
3.1	Copying system apps to the IEM.....	81
3.2	Connecting an Edge Device.....	83
3.2.1	Creating the Edge Device configuration file	83
3.2.2	New Edge Device - Parameters	88
3.2.3	Connecting the Edge Device through an USB flash drive	90
3.2.4	Connecting the Edge Device through the IEM.....	91
3.2.5	LED status.....	94
3.2.6	Example logs	95
3.3	Installing system apps on Edge Devices	96
3.4	Launching system configurators.....	98
4	Working with the IEM	101
5	List of abbreviations/acronyms.....	105
	Glossary	107

Industrial security

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

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

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

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

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

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

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

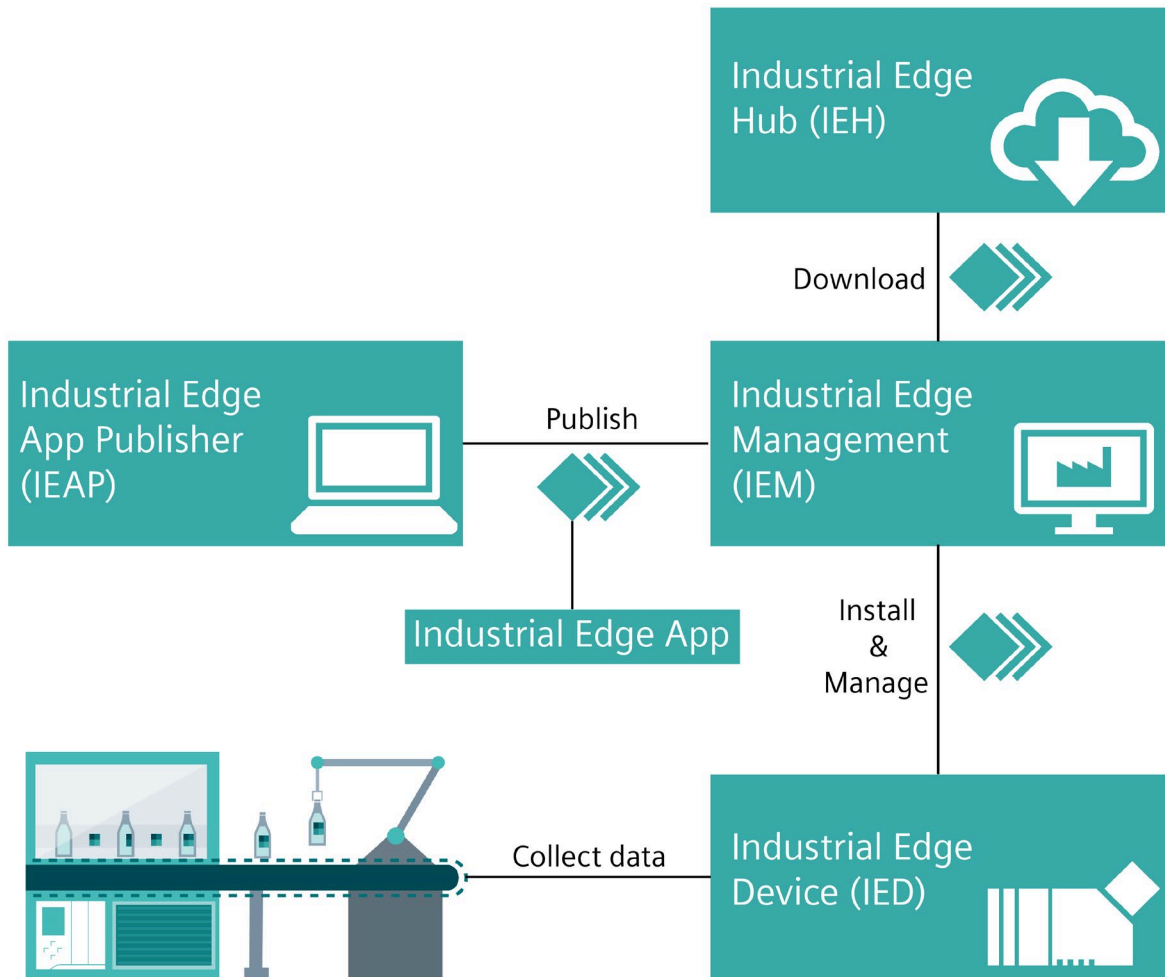
Overview and setup

2.1 Overview of Industrial Edge

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.

2.2 Industrial Edge Hub

2.2.1 Signing 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

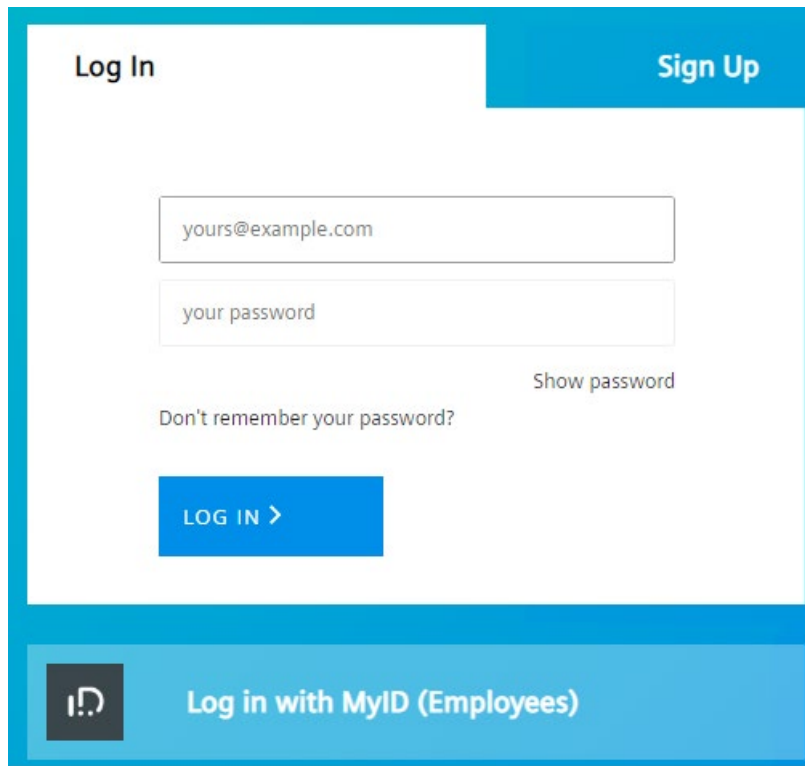
Receiving the welcome email

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 a minimum requirement of at least 8 characters, 1 upper- and lower-case letter, 1 special character and 1 number.

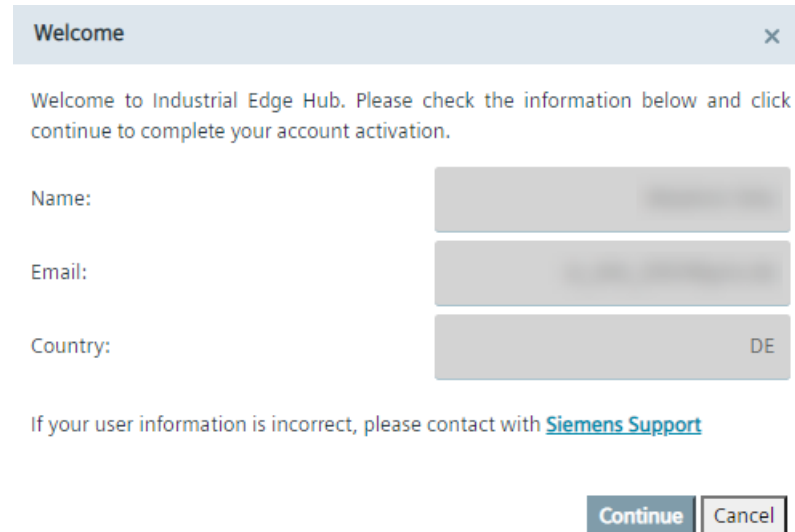
- First name: First name of the email user
- Last name: Last name of the email user

All input fields are mandatory.

4. Read and accept the terms of use.

5. Click "Sign Up".

The "Welcome" screen is displayed.



The screenshot shows a 'Welcome' dialog box with a close button (X) in the top right corner. The text inside reads: 'Welcome to Industrial Edge Hub. Please check the information below and click continue to complete your account activation.' Below this text are three input fields: 'Name:', 'Email:', and 'Country:'. The 'Country:' field has 'DE' entered. At the bottom of the dialog, there is a link for 'Siemens Support' and two buttons: 'Continue' and 'Cancel'.

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.

Confirmation of delivery address and Export Control Clause

Delivery Address

Email:

Country Code:

The user confirms that the download is executed on the displayed country.

Export regulations for DE

[export regulations \(en\)](#)

[export regulations \(de\)](#)

The export control clause for distribution contracts is accepted.

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.

2.2.2 Signing in

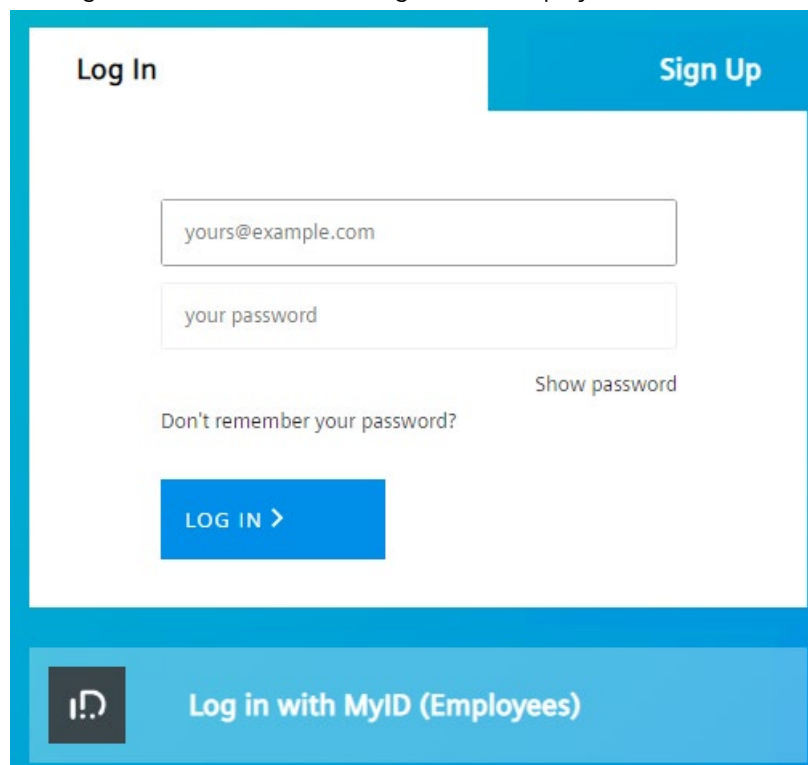
Requirement

- 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.

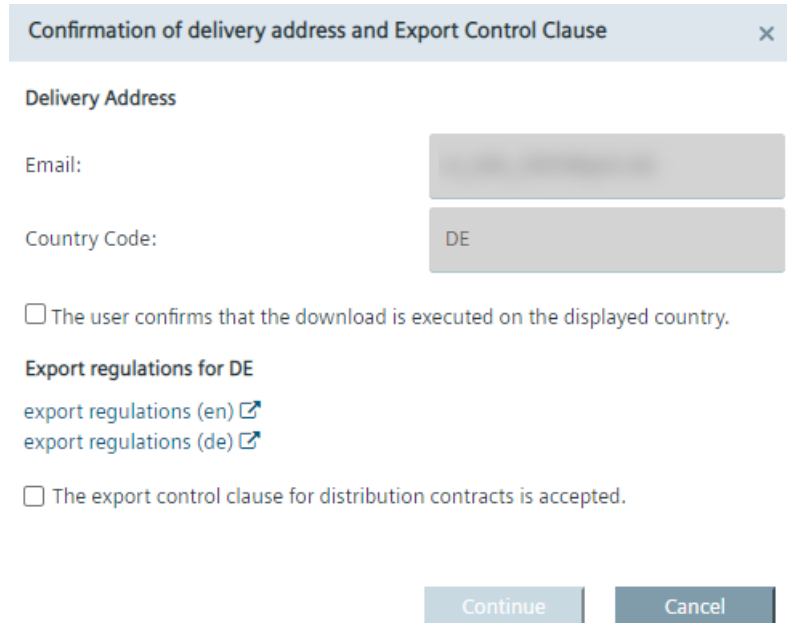


The screenshot shows the login interface for the Industrial Edge Hub. It features a blue header with 'Log In' and 'Sign Up' options. The main area contains two text input fields for email and password, a 'Show password' link, a 'Don't remember your password?' checkbox, and a blue 'LOG IN >' button. At the bottom, there is a blue bar with a MyID icon and the text 'Log in with MyID (Employees)'.

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.

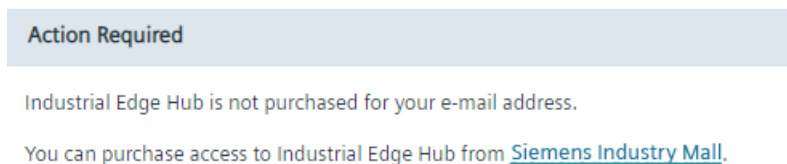
The acceptance will be logged in the IE Hub database along with the date of acceptance.

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:

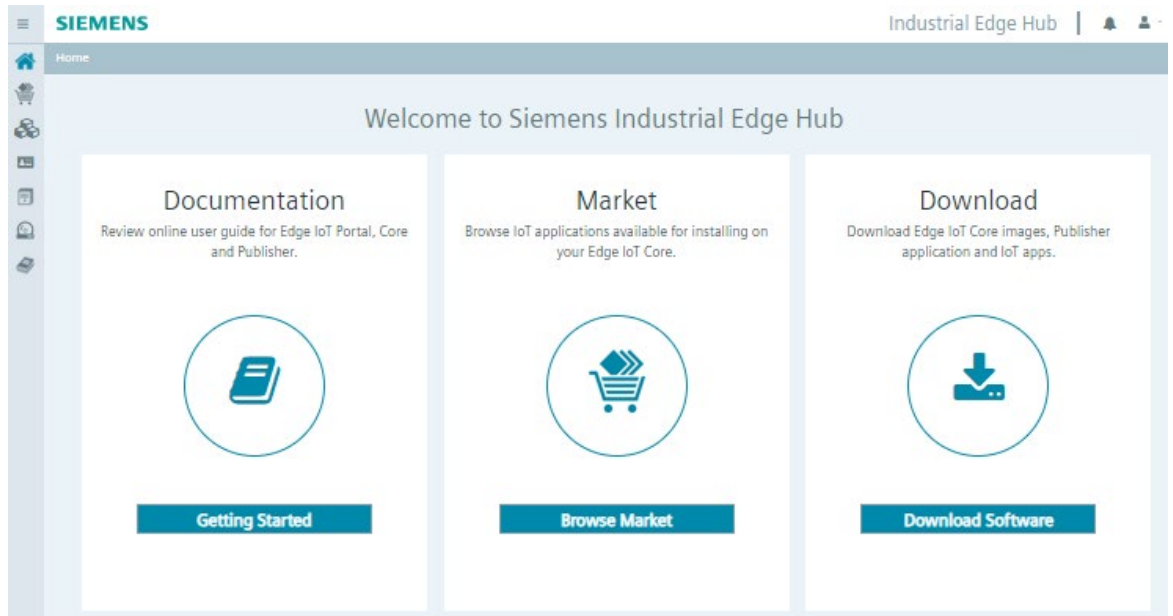


Purchase access to the Industrial Edge Hub in the Siemens Industry Mall by clicking the link.

2.2.3 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 Siemens logo anywhere in the IE Hub, you navigate to the home page. By clicking the button within the tiles, you navigate to the according menu entry.

The IE Hub provides the following menu:

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

Notifications

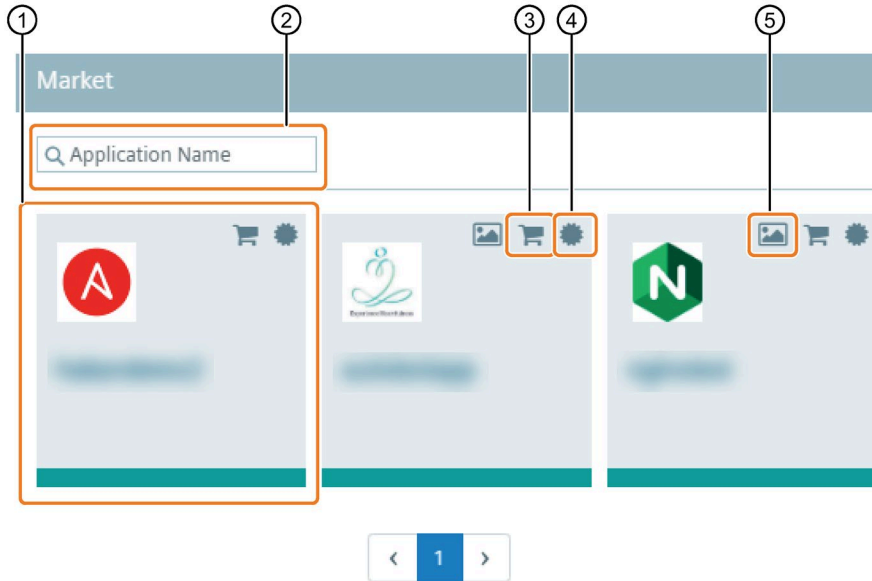
By clicking the  icon, the "Notifications" screen with all notifications referring to the IE Hub is displayed. Whenever 1 of the following events occur, the according notification is displayed in the "Notifications" screen:

- 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

2.2.4 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 Available Edge App
Only purchasable Edge Apps are listed.
- ② Filter the app catalog (only current page) based on the app name.
- ③ Purchasing the Edge App
- ④ Licensing status:
 - Gray: Edge App is not licensed
 - Green: Edge App is licensed
- ⑤ Screenshots
If screenshots are available for the Edge App, click on the icon to display the screenshots.

2.2.4.1 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

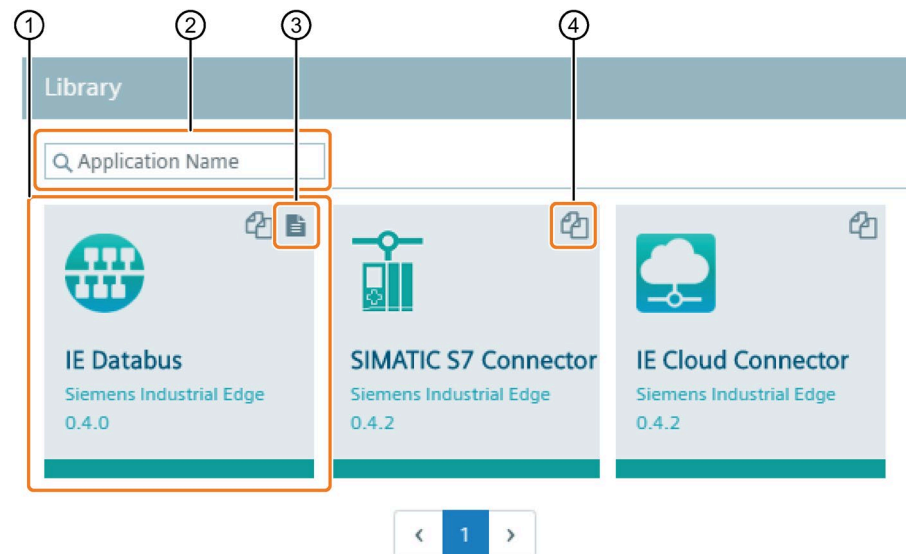
To use and connect Edge Devices in the IEM, you need according Edge Device licenses too. To purchase Edge Device licenses, you obtain a link from Siemens through which you purchase the according Edge Device licenses.

2.2.5 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 additionally. 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 Filter the apps (only current page) regarding the app name
- ③ Open documentation
- ④ Copy app to IEM catalog

2.2.5.1 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.

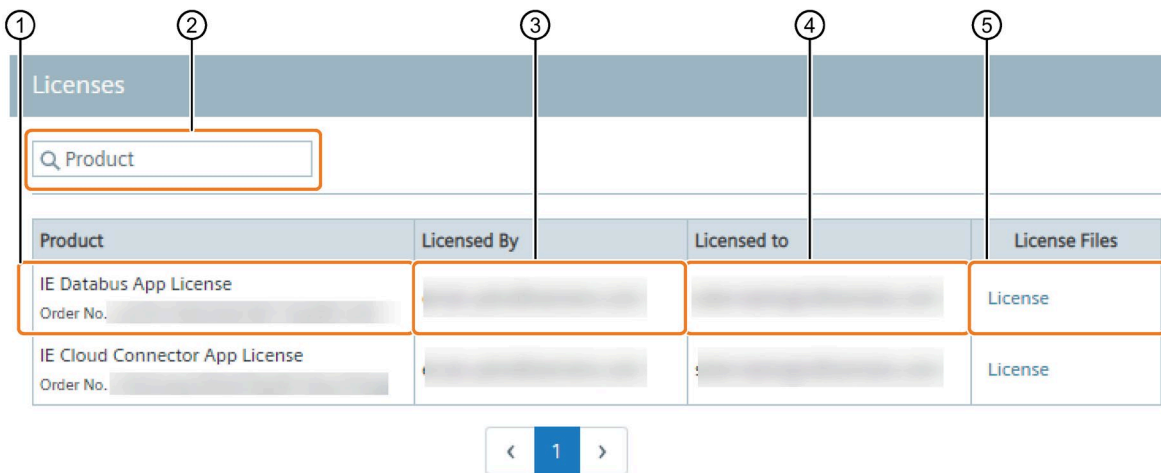
2.2.5.2 Opening documentation

If the app includes a documentation, the app tile contains the documentation icon. By clicking the icon, you will be redirected to the documentation page.

2.2.6 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 Download license file

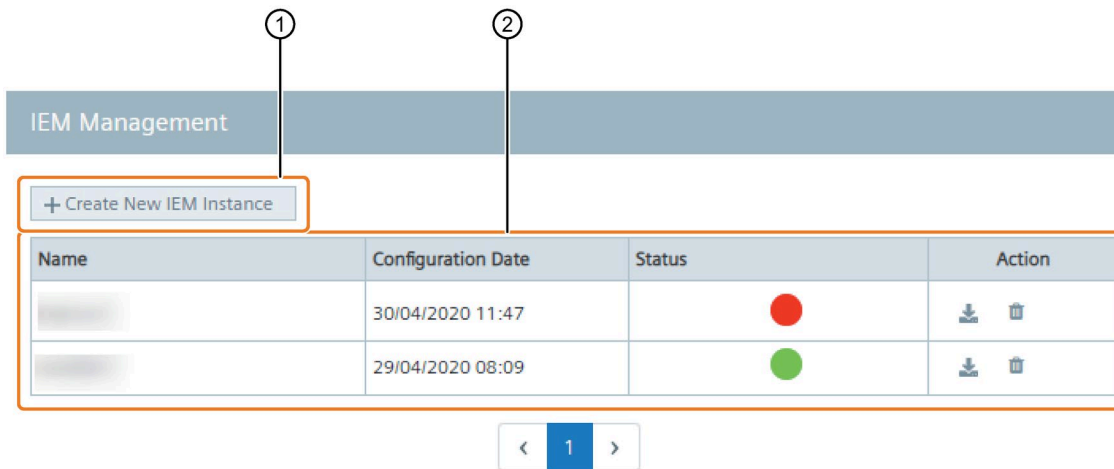
2.2.7 IEM Instances

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
- Action: Download configuration file and delete IEM instances

2.2.7.1 Managing IEM instances


Creating an IEM instance

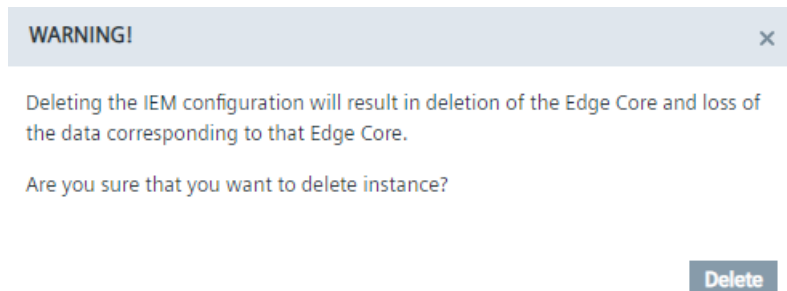
When you click on "Create New IEM Instance", you create a configuration file which you need for setting up your IEM. You find the detailed procedure to create an IEM instance in the "Creating IEM instance and downloading the configuration file (Page 26)" subsection.

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.

2.2.8 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 or Ubuntu version 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.

2.2.9 Documents

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

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

2.3 Setting up the IEM

2.3.1 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 enabling the IEM, you set up the IEM.

When you successfully set up 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.
- 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 set up encrypted
 - TPM is enabled for the VM

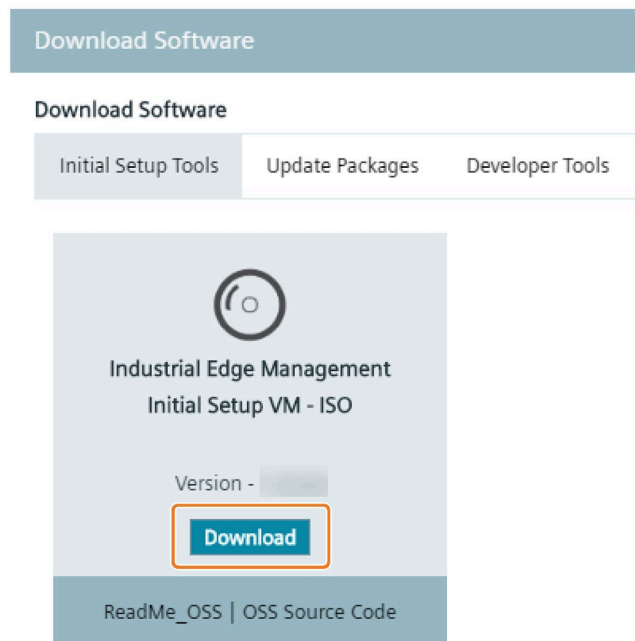
You find information on how to enable these settings in the documentation of the virtualization environment itself from the Internet.

2.3.2 Downloading the Industrial Edge Management OS

You download the Industrial Edge Management OS (IEM-OS) for the VM from the IE Hub. The VM including the Industrial Edge Management OS functions as a cluster and enables the IEM. In that cluster, you deploy your 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.

2.3.3 Creating IEM instance and downloading the configuration file

Procedure

1. In the navigation menu of the IE Hub, click "IE Management".
2. Click "Create New IEM Instance".

The "Create IEM Instance" screen is displayed.

Create IEM Instance

Name



3. In the "Name" input field, enter the name of the instance.

The name of the instance must be unique within your own account 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.

2.3.4 VMware Workstation

2.3.4.1 Creating the VM

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

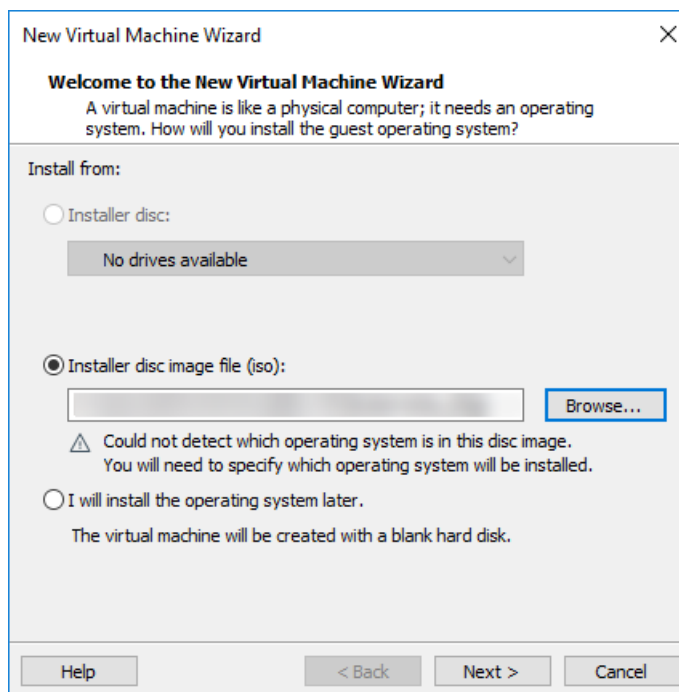
The following procedure describes the installation in the "VMware Workstation" virtualization environment.

Requirement

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

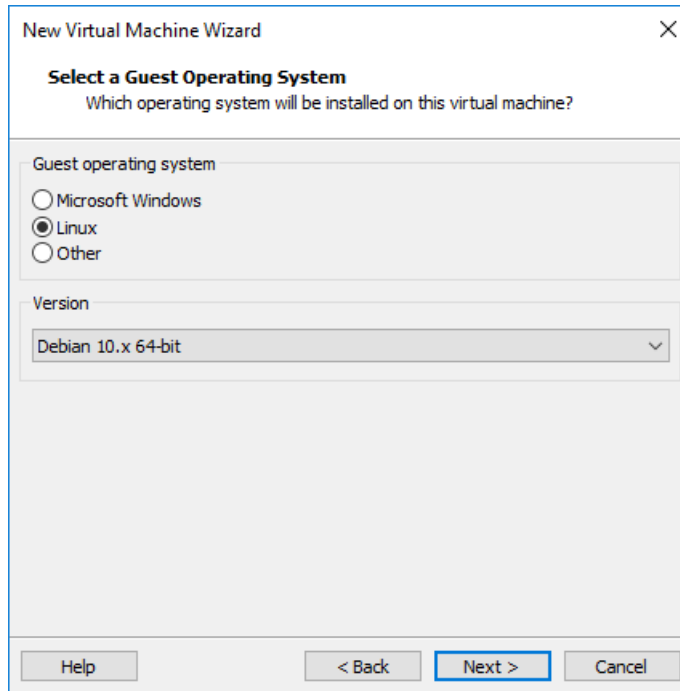
Procedure

1. Open "VMware Workstation".
2. On the right side, click "Create a New Virtual Machine".
The "New Virtual Machine Wizard" screen is displayed.
3. Select the "Installer disc image file (iso)" option.
4. Click "Browse" and select the extracted "industrial_edge_management.iso" file.

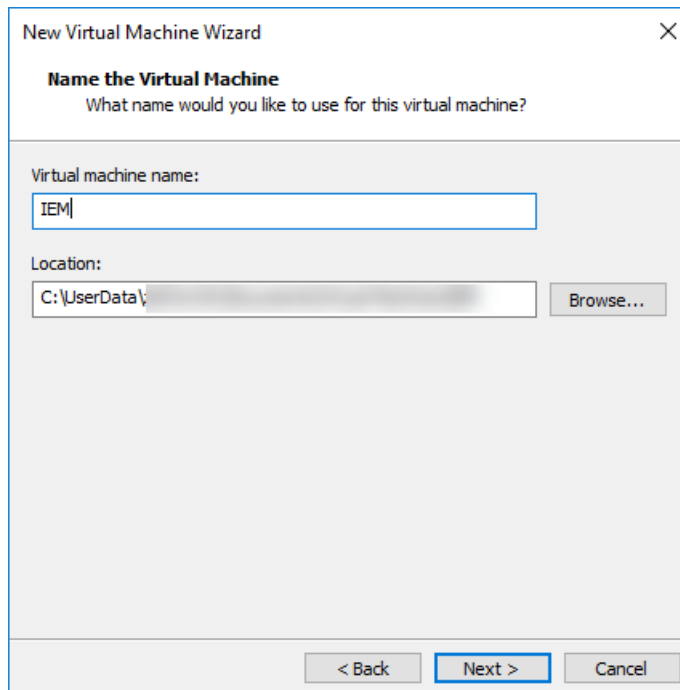


5. Click "Next".
6. From the "Guest operating system" options, select "Linux".

7. From the "Version" drop-down list, choose a 64-bit version of a Linux distribution, for example "Debian 10.x 64-bit".



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



11. Click "Next".

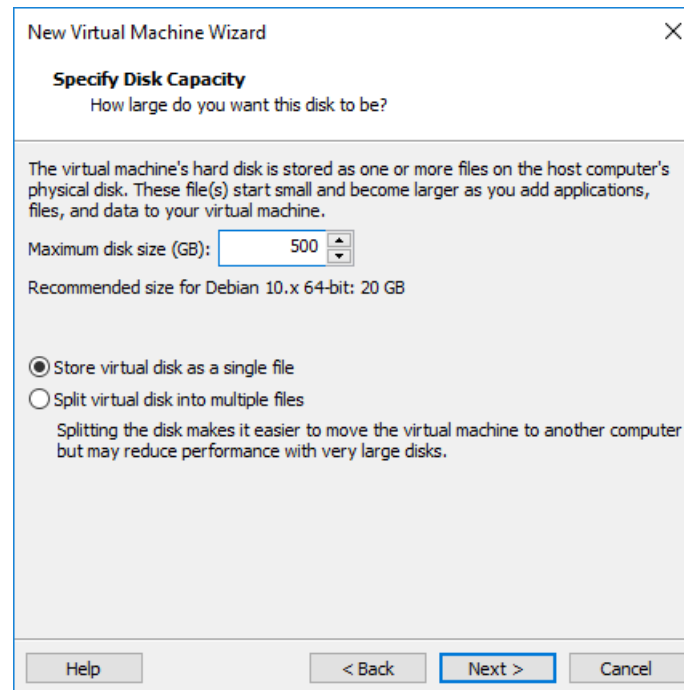
12. In the "Maximum disk size (GB)" input field, enter a maximum disk size for the VM on the host PC's physical disk.

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.

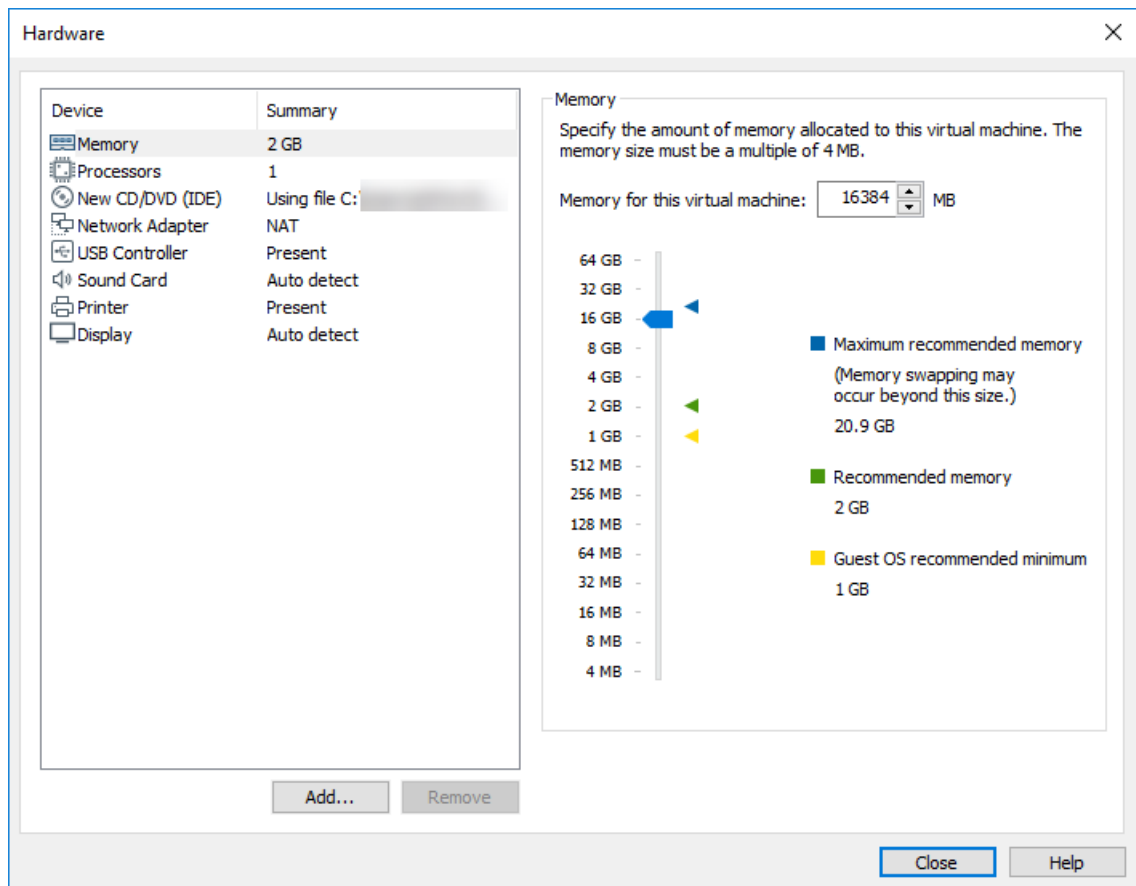
13. Select the "Store virtual disk as a single file" option.



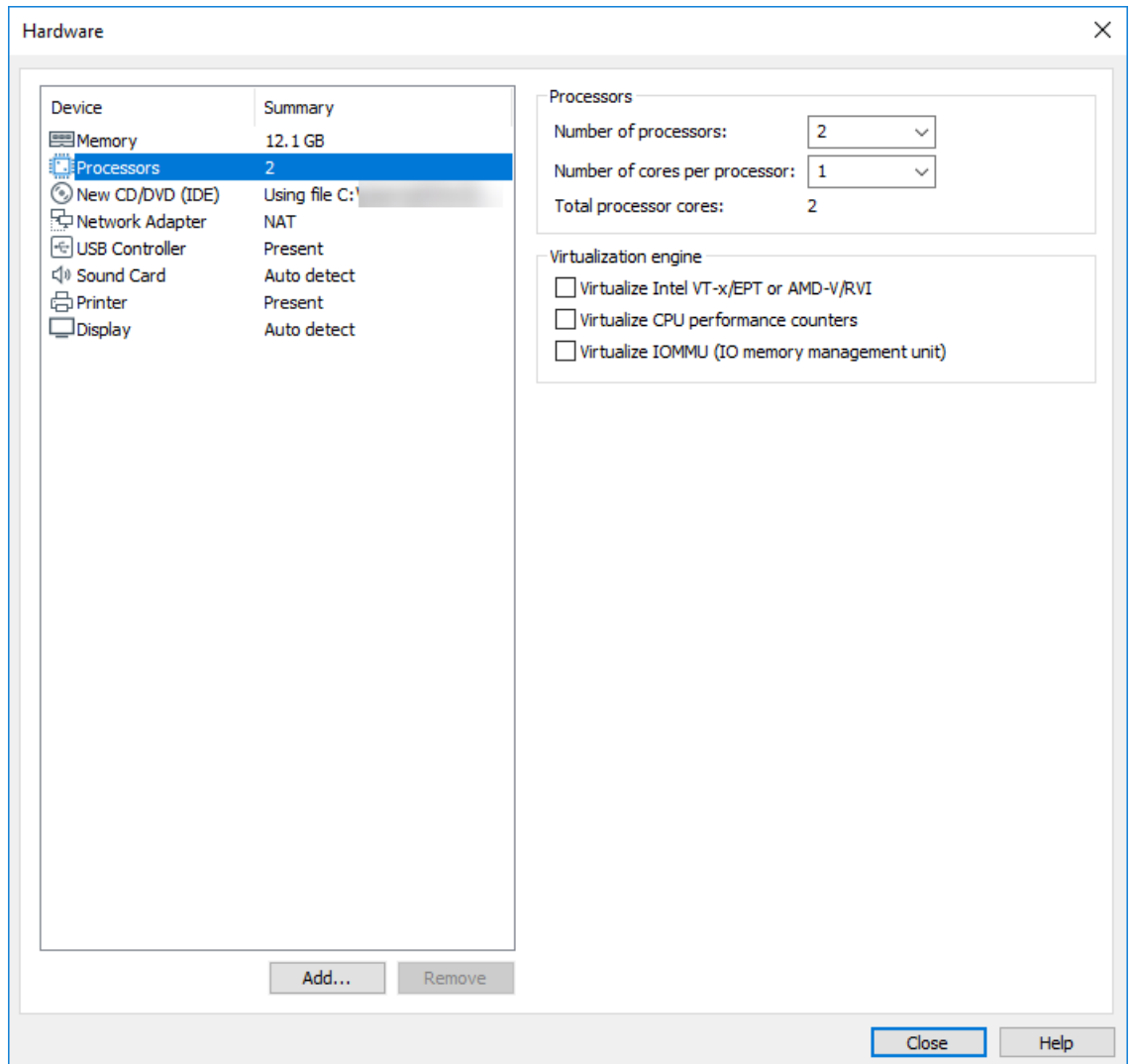
14. Click "Next".

15. Click "Customize Hardware".

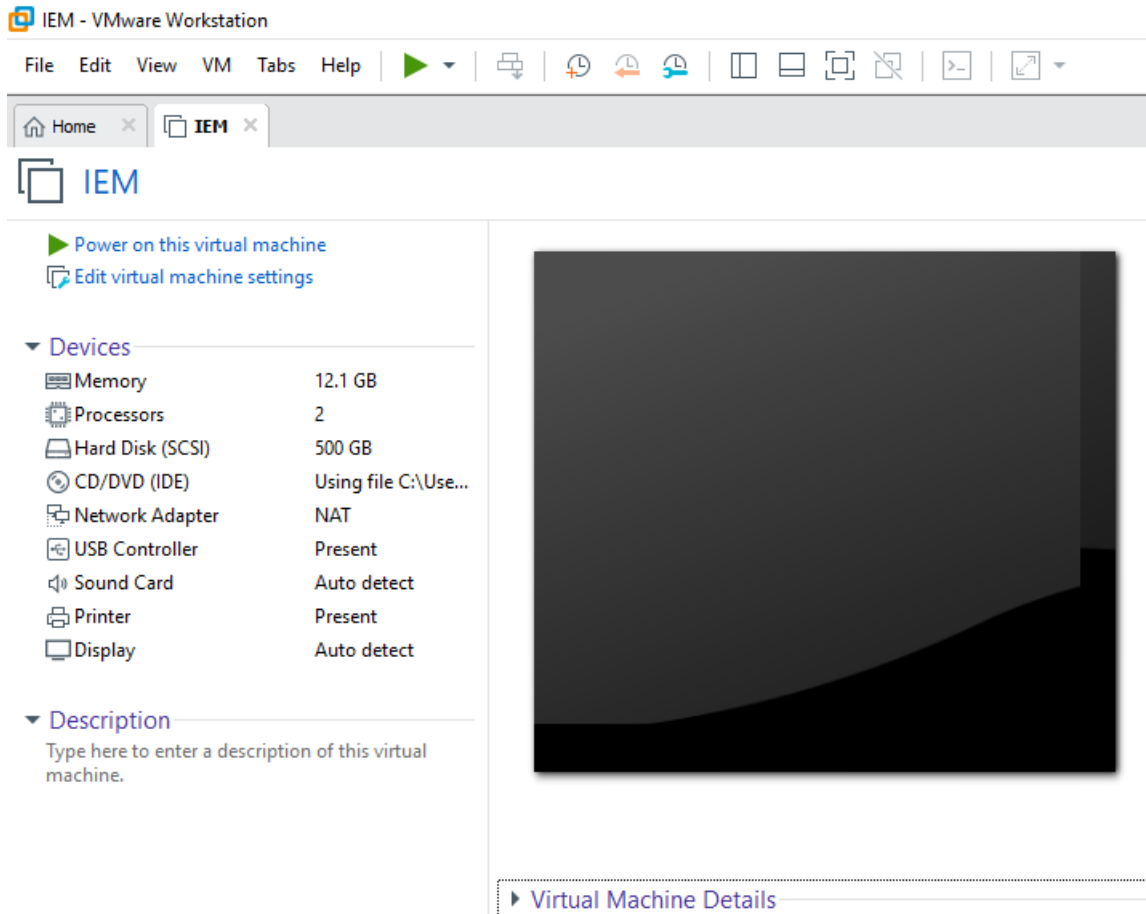
16. For the memory amount allocated to the VM, choose a minimum of 16 GB.



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



- 18. Click "Close".
 - 19. Click "Finish".
- The VM is created.



2.3.4.2 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.

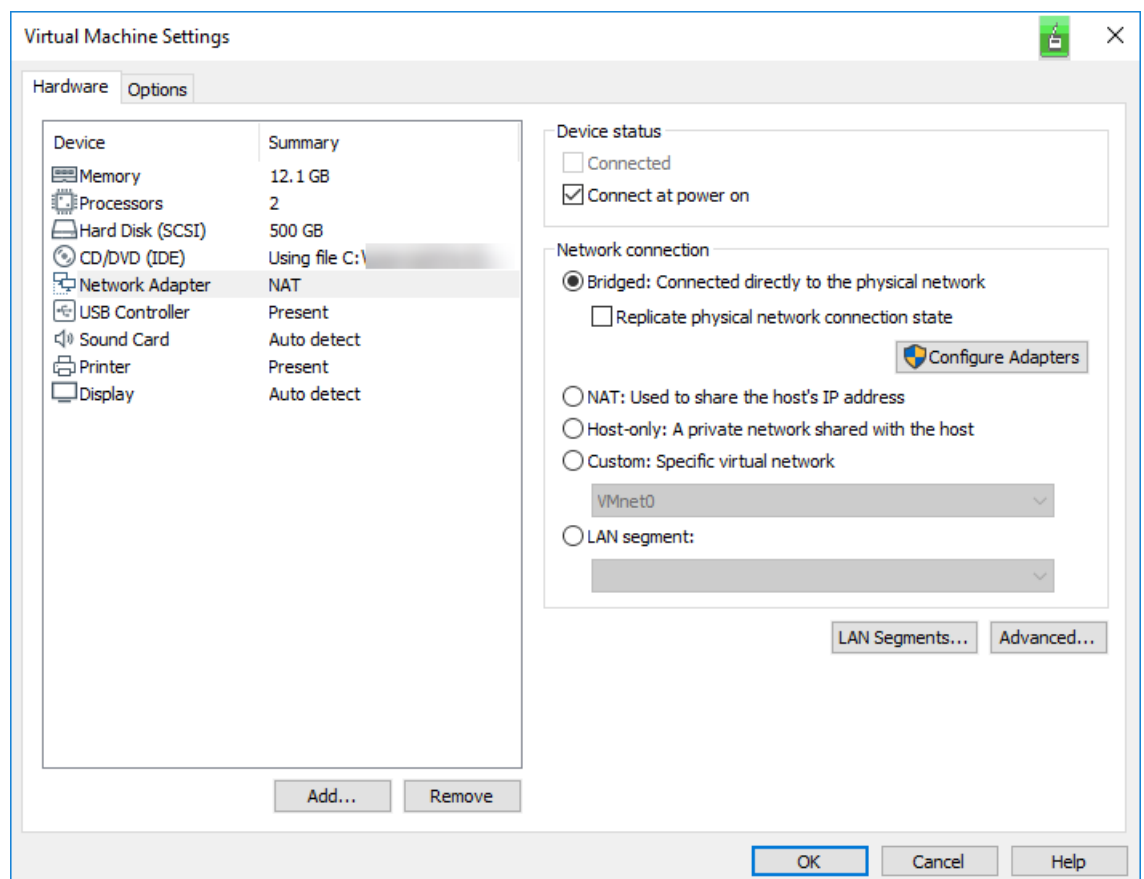
Procedure

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.

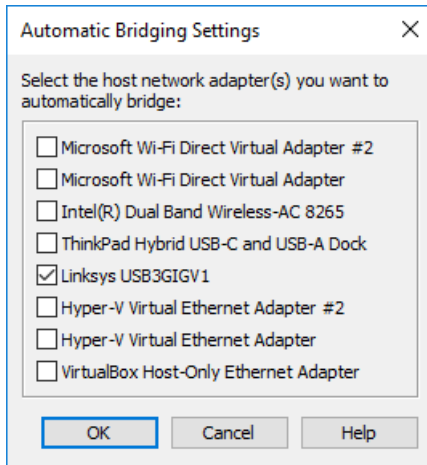
If you use a "NAT" network connection for your VM, go to step 11.

4. On the right side under "Network connection", select "Bridged: Connected directly to the physical network".



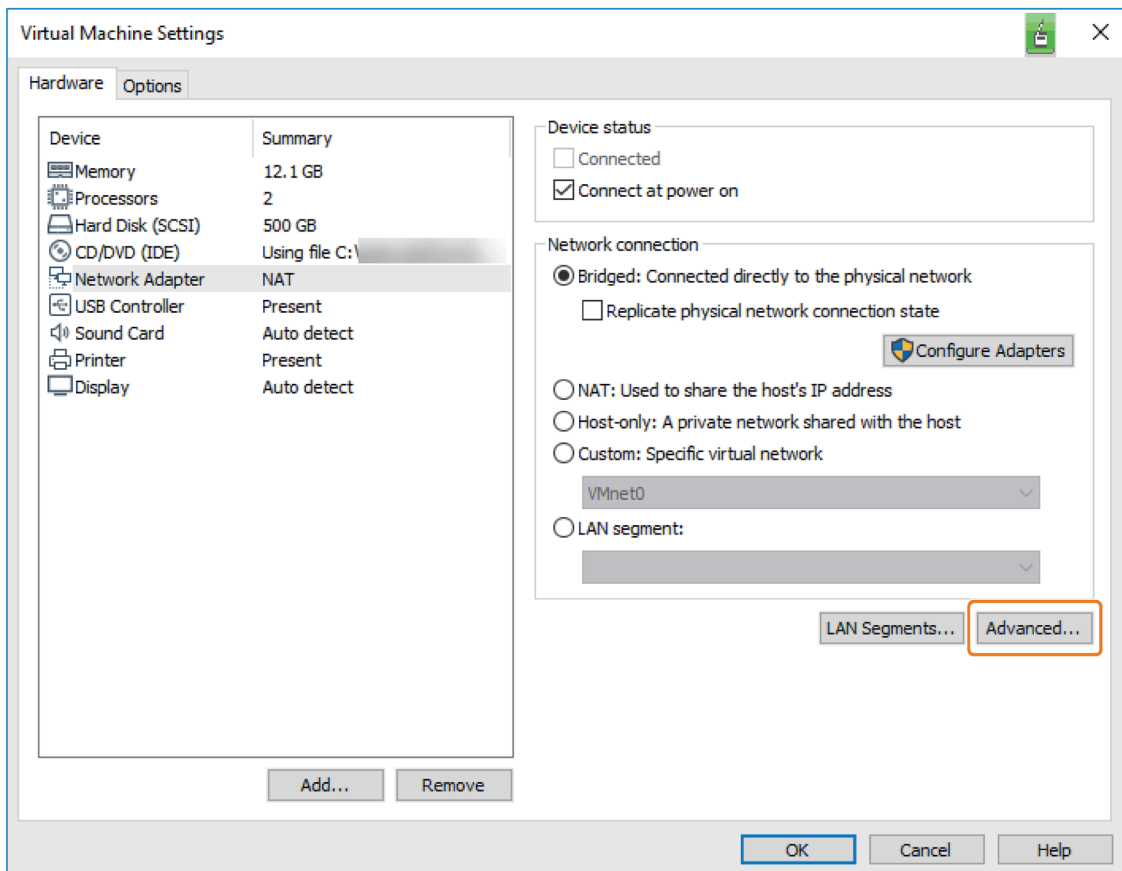
5. Click "Configure Adapters".
- The "Automatic Bridging Settings" screen is displayed.

6. Activate only your connected USB network adapter.



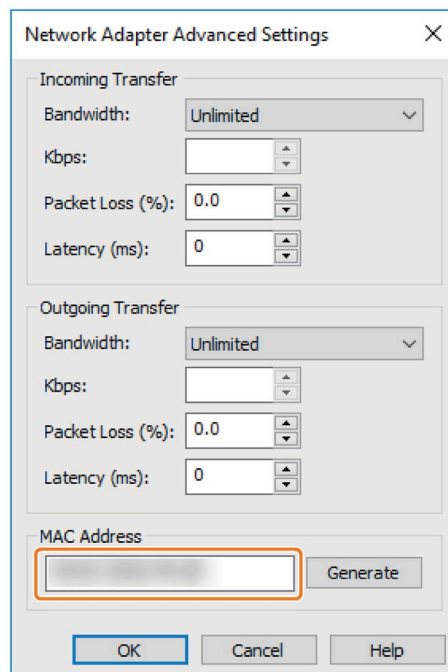
7. Click "Ok".

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



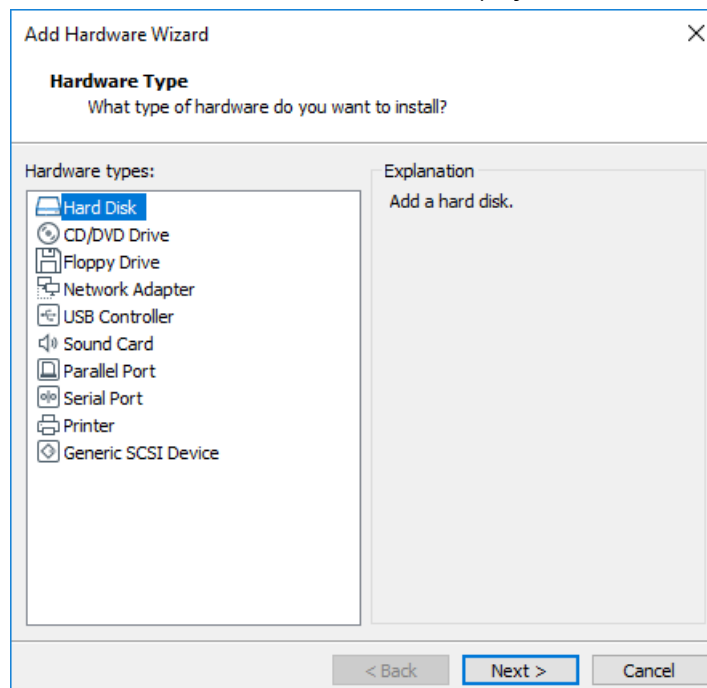
The "Network Adapter Advanced Settings" screen is displayed.

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



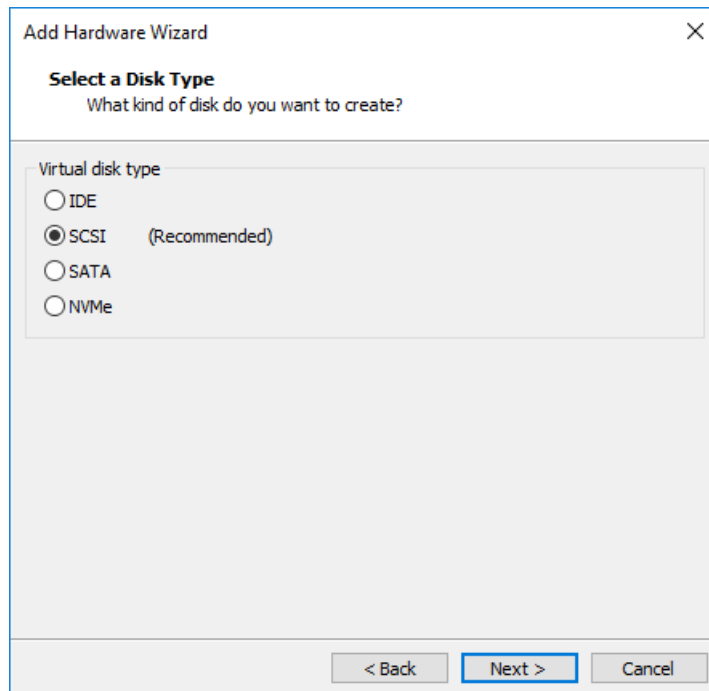
10. Click "OK".
11. Below the left navigation, click "Add".

The "Add Hardware Wizard" screen is displayed.

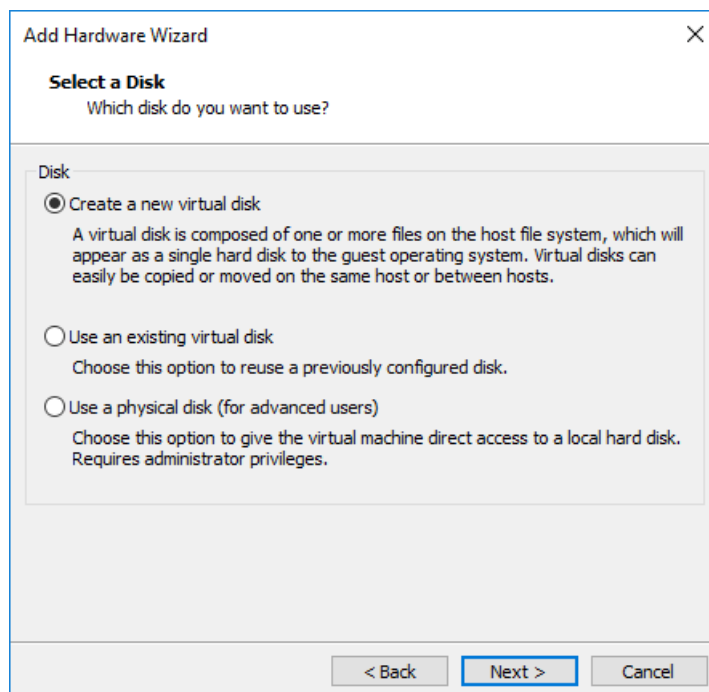


12. Select "Hard Disk" and click "Next".

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



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

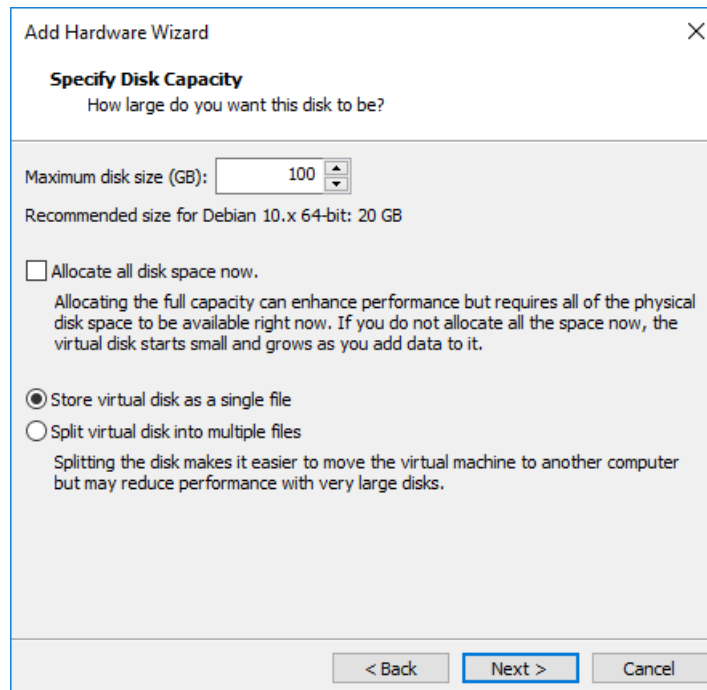


15. In the "Maximum disk size (GB)" input field, enter a maximum disk size that is lower than the disk size that you configured before.

The second hard disk is for the apps data storage.

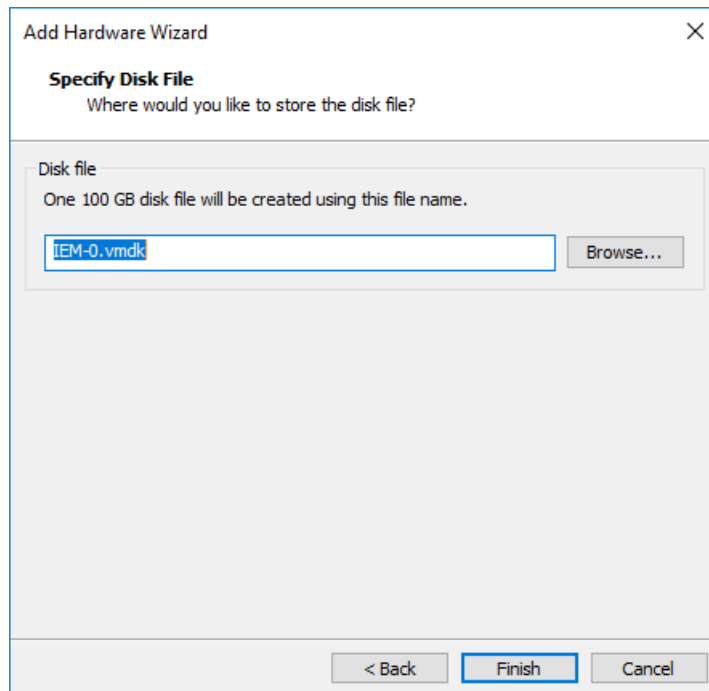
Siemens recommends a maximum disk size of 100 GB for the second disk. A minimum of 50 GB is mandatory.

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



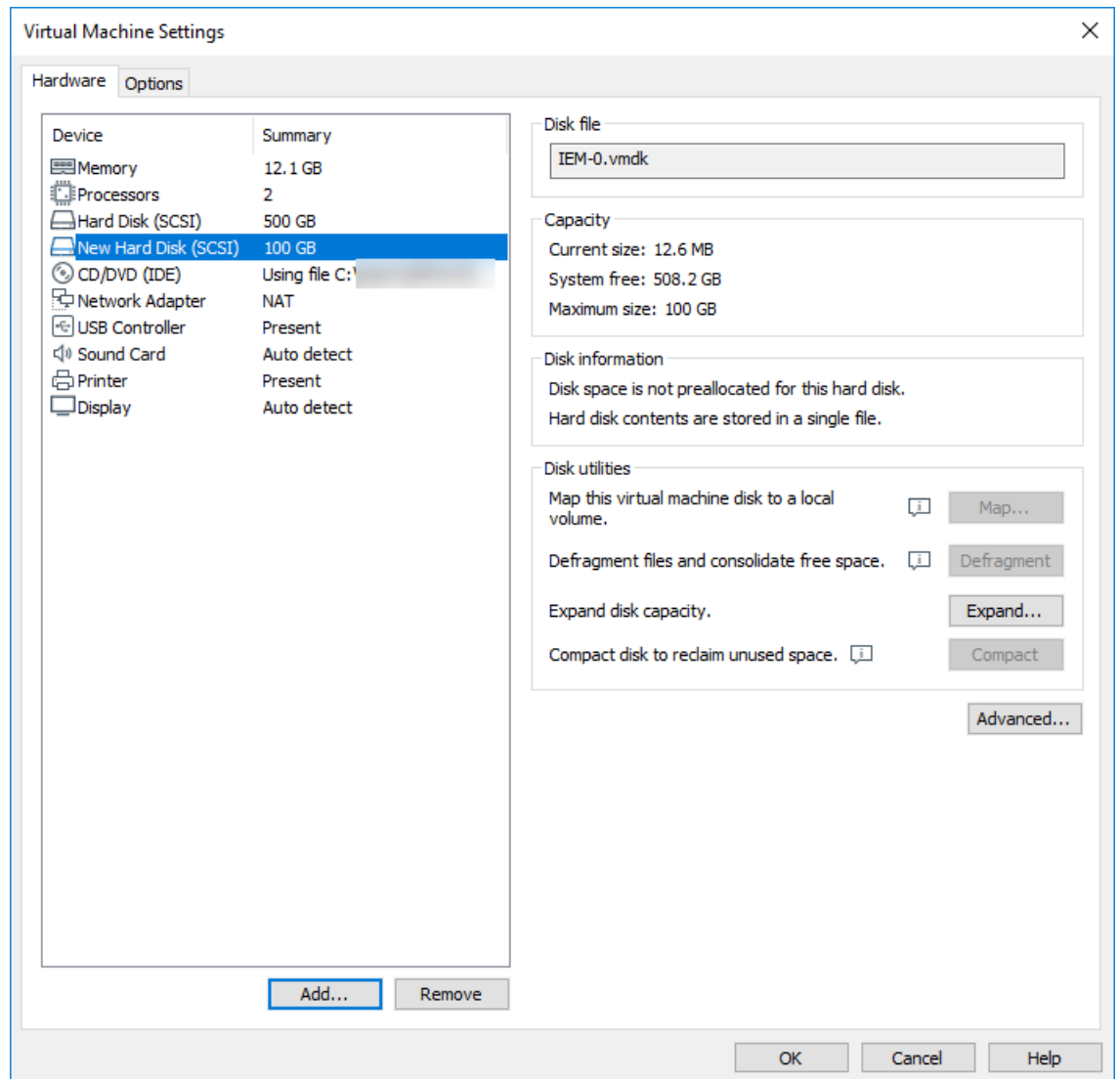
The screenshot shows a dialog box titled "Add Hardware Wizard" with a close button (X) in the top right corner. The main heading is "Specify Disk Capacity" with the subtitle "How large do you want this disk to be?". Below this, there is a text label "Maximum disk size (GB):" followed by a text input field containing the number "100" and a small spinner control. Underneath, it says "Recommended size for Debian 10.x 64-bit: 20 GB". There are two radio button options: the first is "Allocate all disk space now." with a description: "Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it." The second option is "Store virtual disk as a single file" which is selected with a radio button. Below it is another option: "Split virtual disk into multiple files" with a description: "Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks." At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

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



18. Click "Finish".

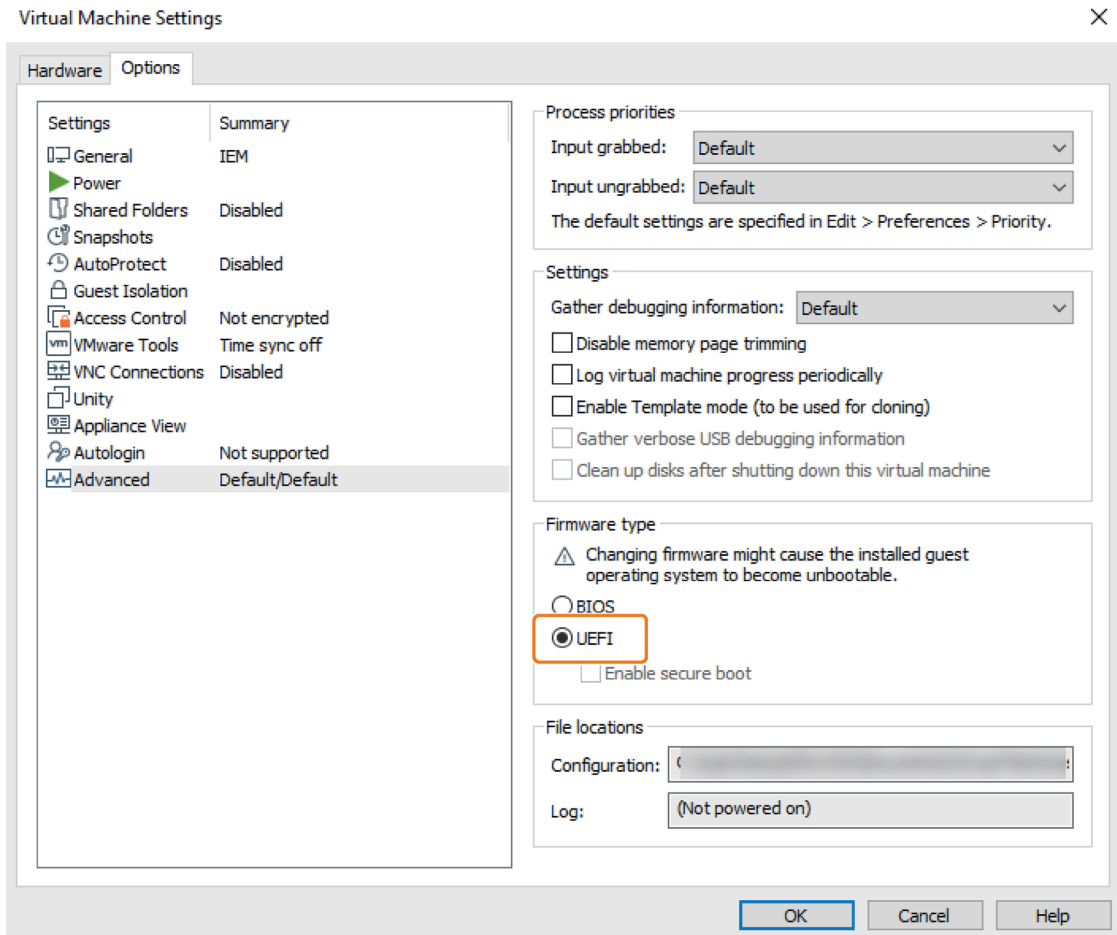
The second hard disk is added to the hardware list in the left navigation.



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*
```


2.3.4.3 Installing the Industrial Edge Management OS

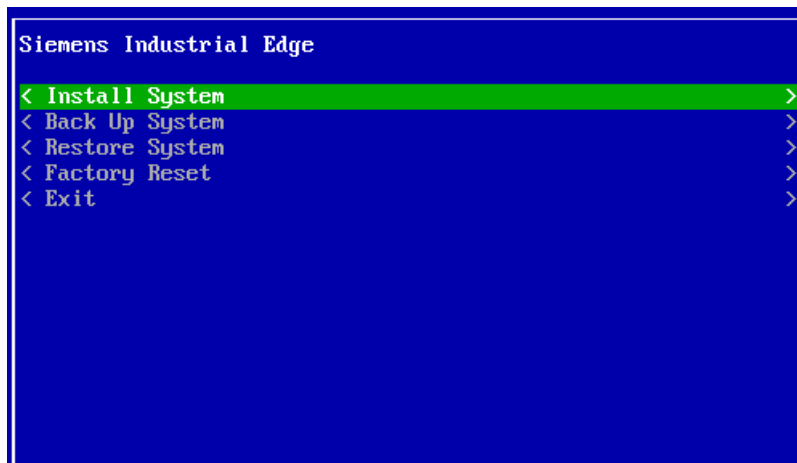
Requirement

UEFI Boot is enabled in the VM settings.

Procedure

1. Start the VM.

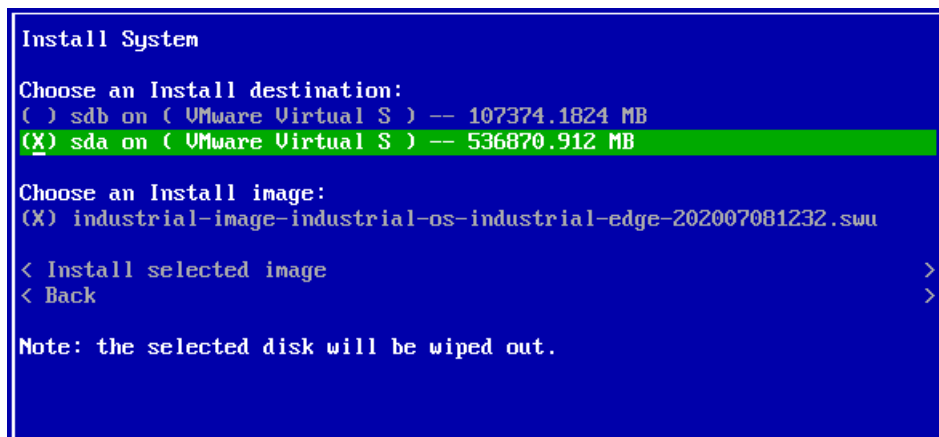
The "Siemens Industrial Edge" screen is displayed.



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".

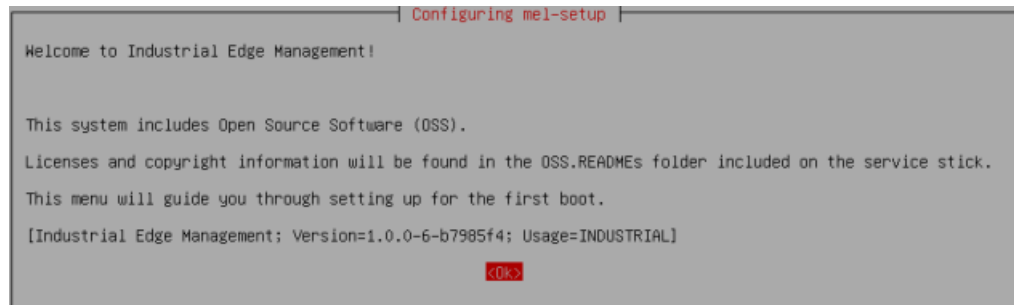
The VM is getting rebooted.

Note

Changing boot order

When the "Siemens Industrial Edge" screen is displayed again after the reboot, you must change the boot order in the BIOS settings. Open the BIOS 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 59)" subsection describes how to configure the IEM-OS.

2.3.5 Oracle VirtualBox

2.3.5.1 Creating the VM

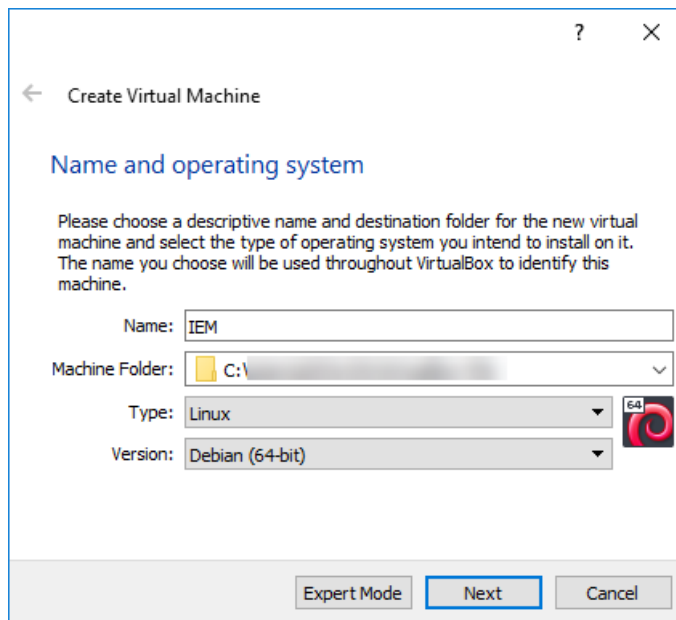
The following procedure describes the installation in the "Oracle VirtualBox" virtualization environment.

Requirement

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

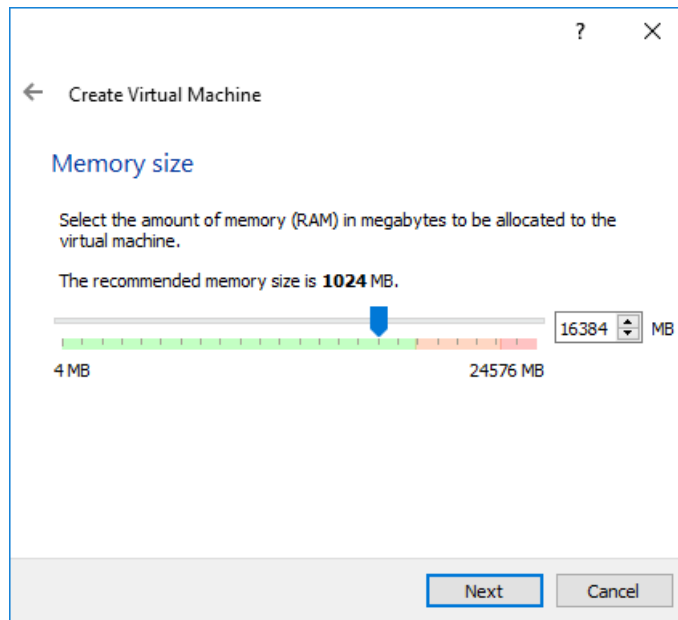
Procedure

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)".



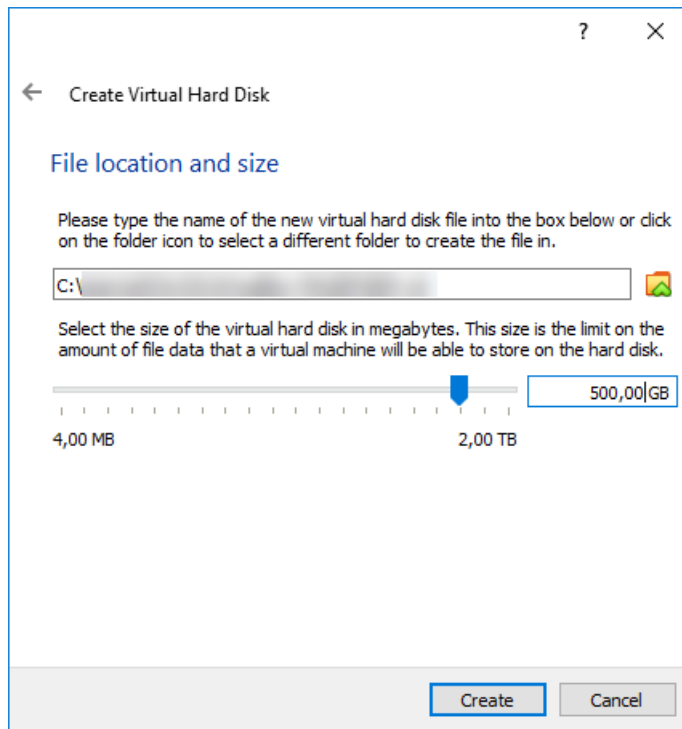
6. Click "Next".

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.

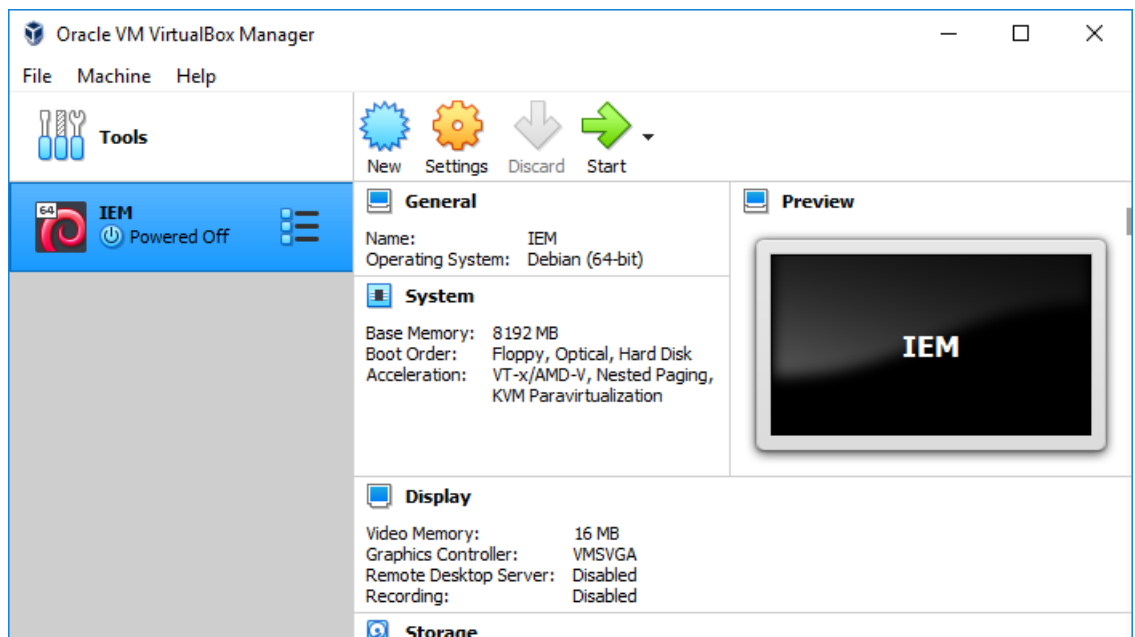
12. For the hard disk size, set a maximum disk size for the VM on the host PC's physical disk.



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.



2.3.5.2 Configuring the VM

Requirement

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

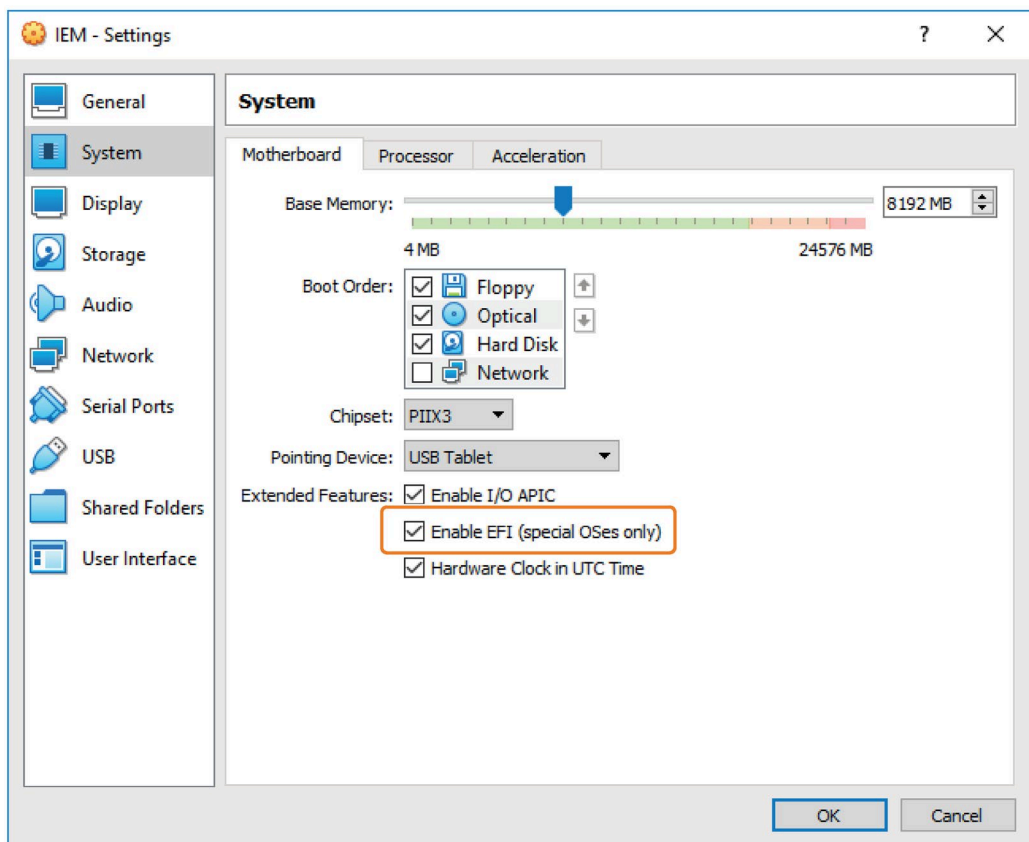
Note

USB network adapter

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

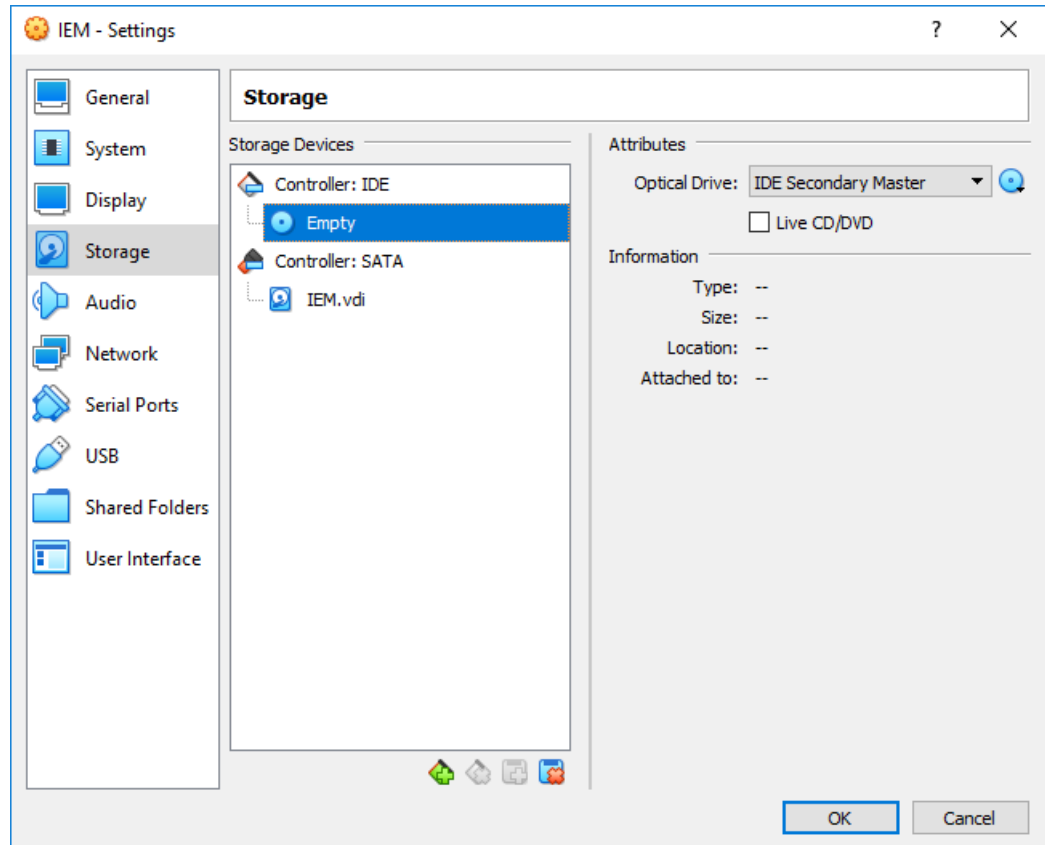
Procedure


1. Select the created VM.
2. Click "Settings".
3. In the navigation on the left side, click "System".
4. Select the "Enable EFI (special OSes only)" check box.



5. Click the "Processor" tab.

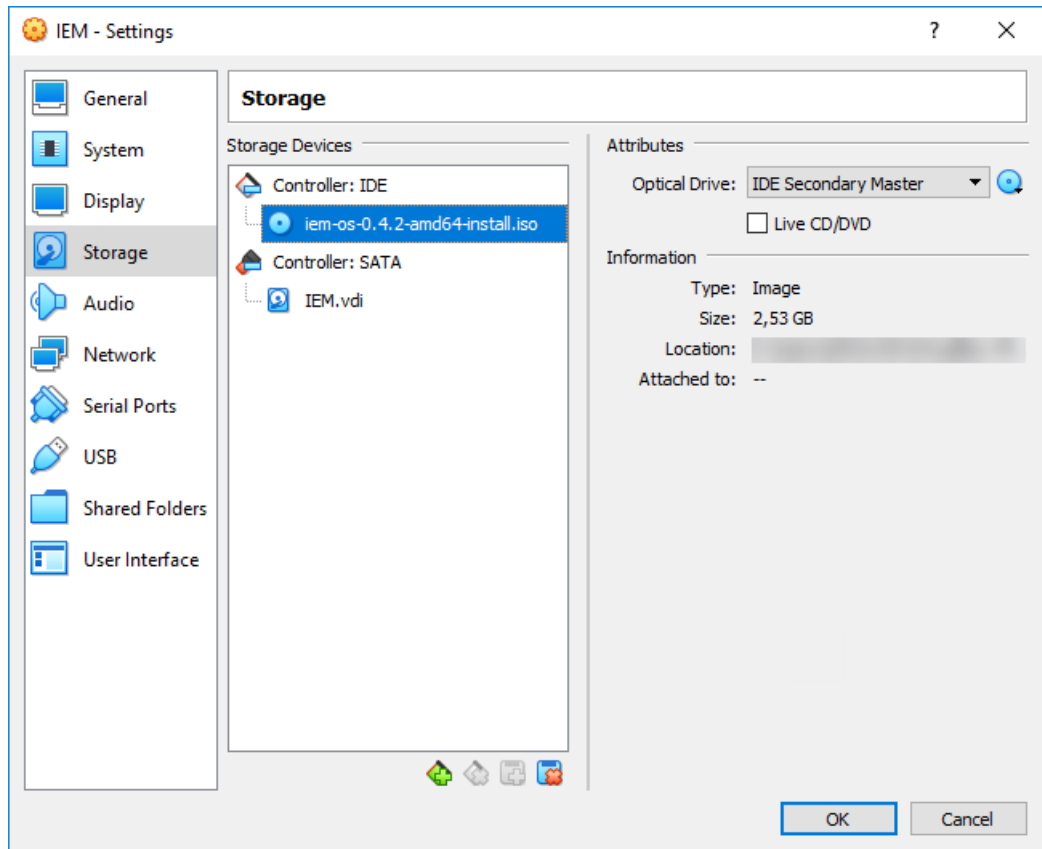
6. For the number of processors, choose minimum 2 processor cores for the VM.
7. In the navigation on the left side, click "Storage".
8. Under "Controller: IDE", click "Empty".




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

12. Click "Choose".

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

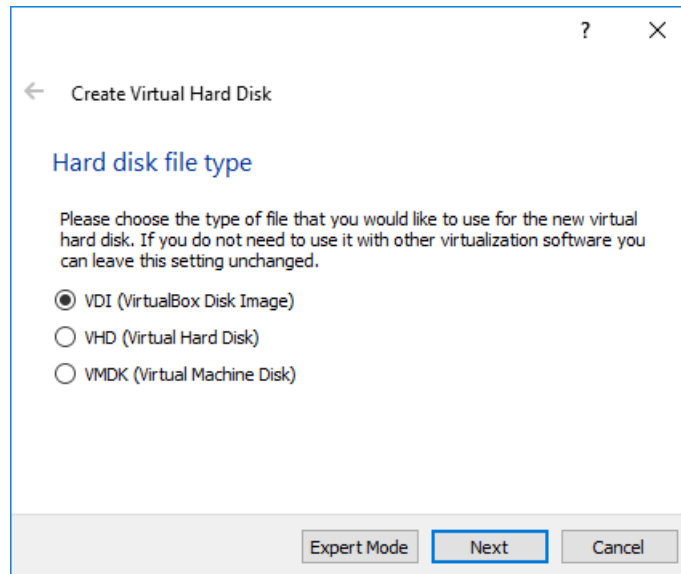


13. To add the second hard disk, select "Controller: SATA" and click the  icon.

The "Hard Disk Selector" screen is displayed.

14. Click "Create".

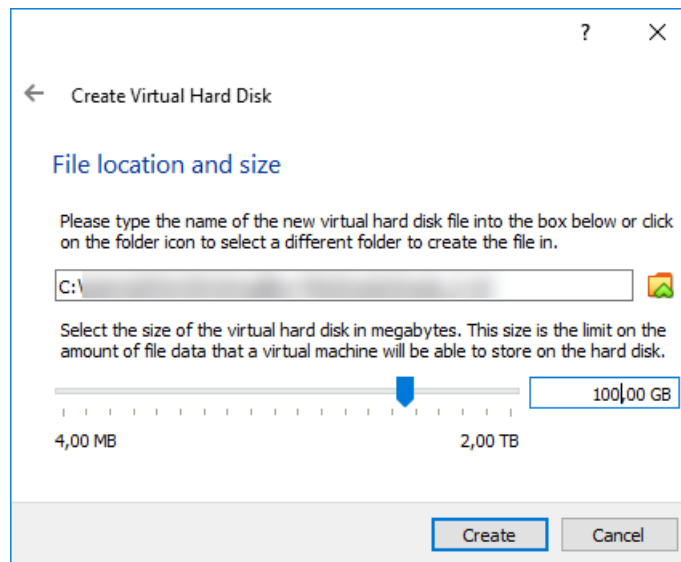
The "Create Virtual Hard Disk" screen is displayed.



15. Select the "VDI (VirtualBox Disk Image)" check box and click "Next".

16. Select the "Dynamically allocated" check box and click "Next".

17. Select a maximum disk size that is lower than the disk size that you configured before.



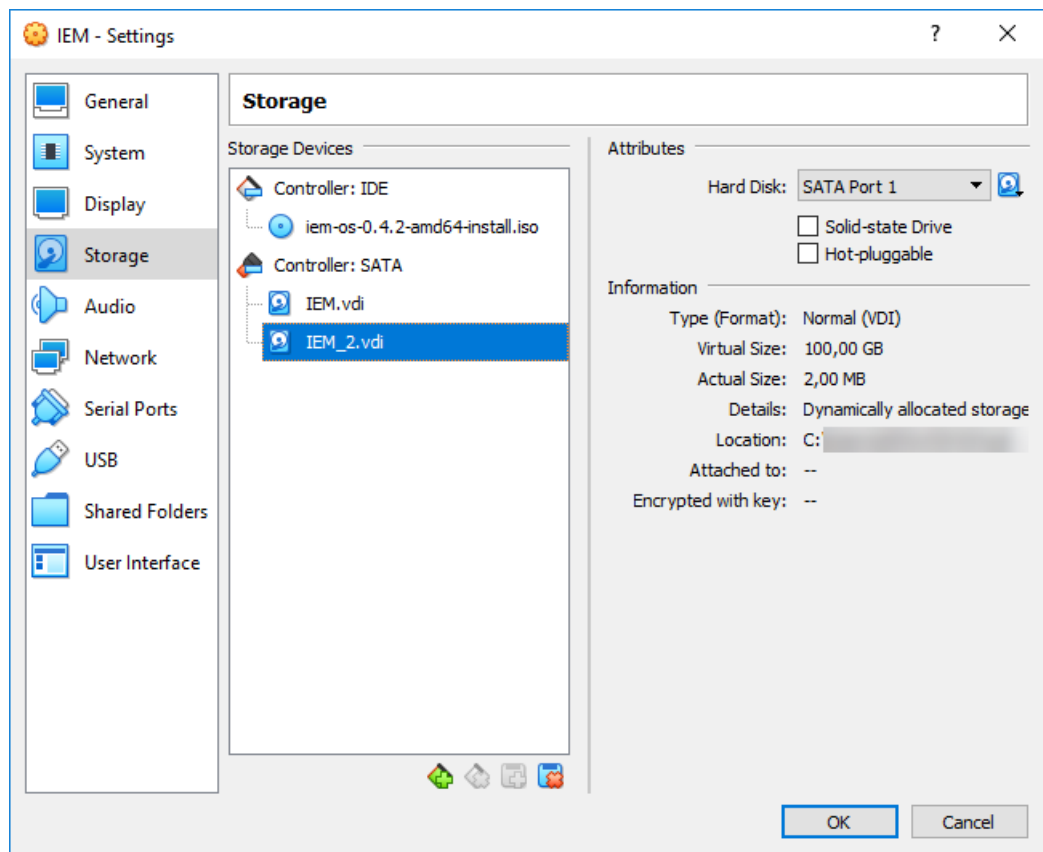
The second hard disk is for the apps data storage.

Siemens recommends a maximum disk size of 100 GB for the second disk. A minimum of 50 GB is mandatory.

18. Click "Create".

19. Click "Choose".

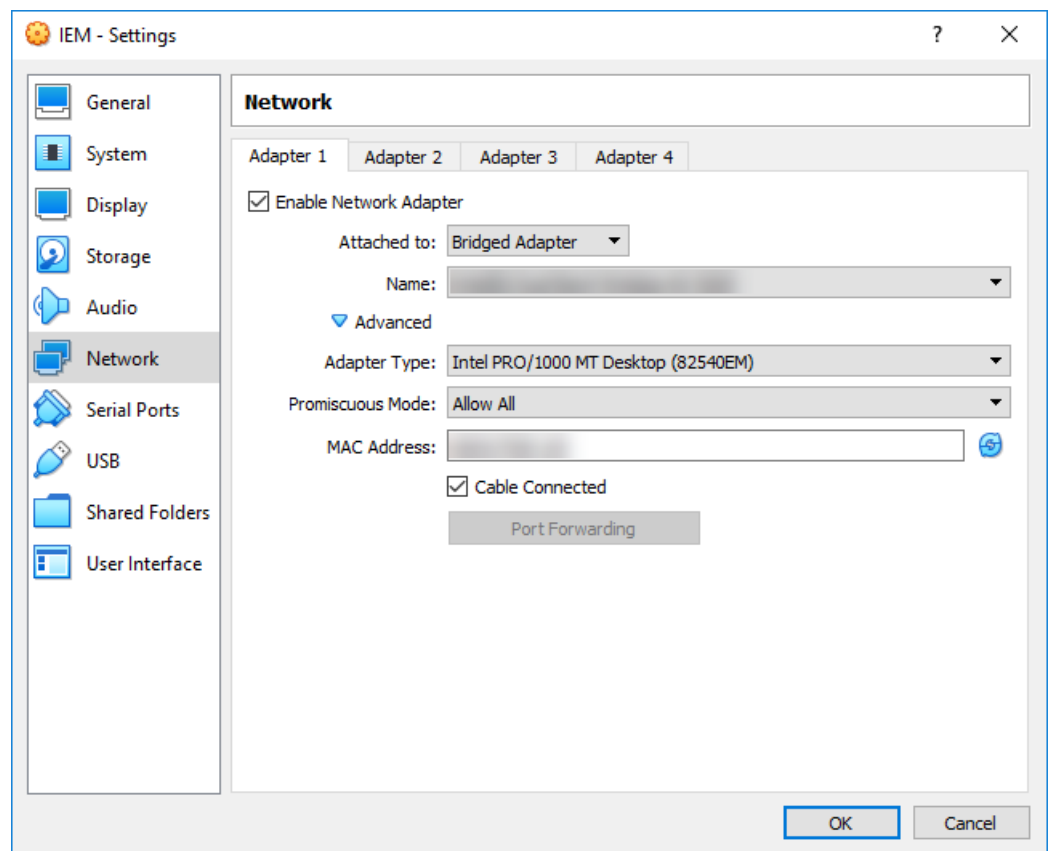
The second hard disk is added under "Controller: SATA".



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

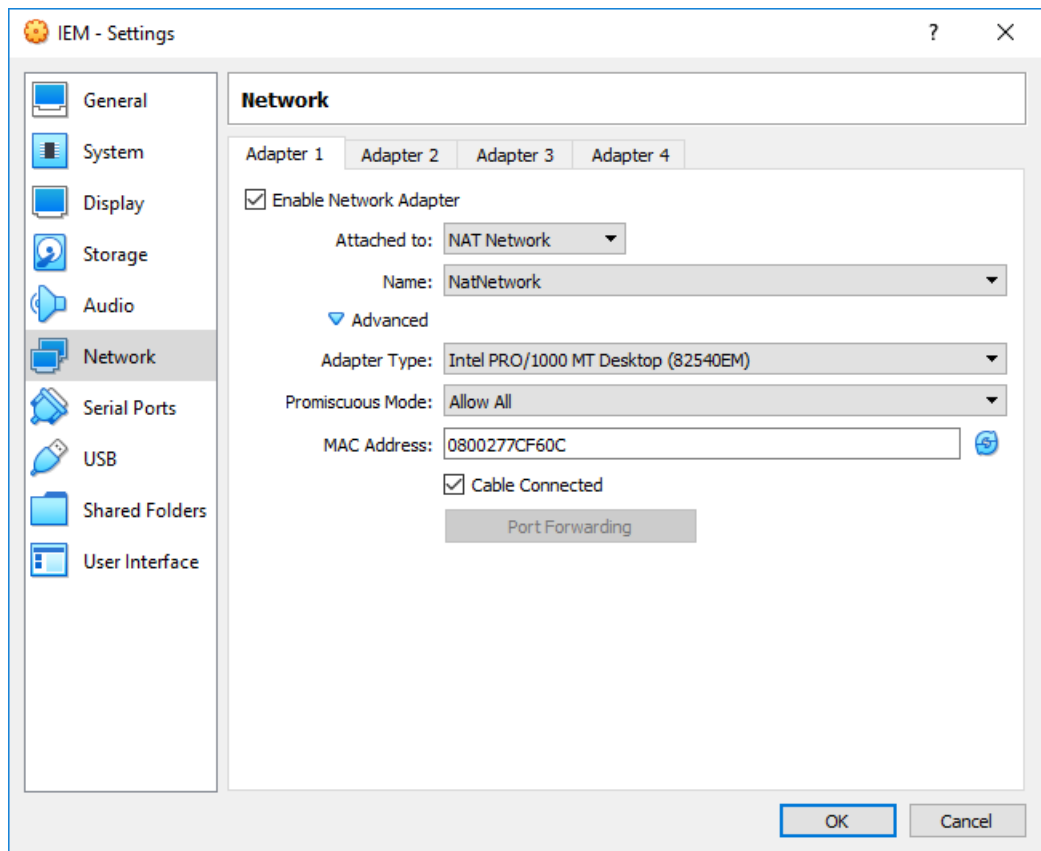
21. If you use a bridged network connection, the following settings must be configured under the "Adapter 1" tab:

- Checkbox "Enable Network Adapter" selected
- Attached to: "Bridged Adapter"
- Name: Name of the additional network interface
- Adapter type: Intel PRO/1000 MT Desktop (82540EM)
- Promiscuous Mode: Allow All
- MAC Address: MAC address of the additional network interface
- Checkbox "Cable Connected" selected



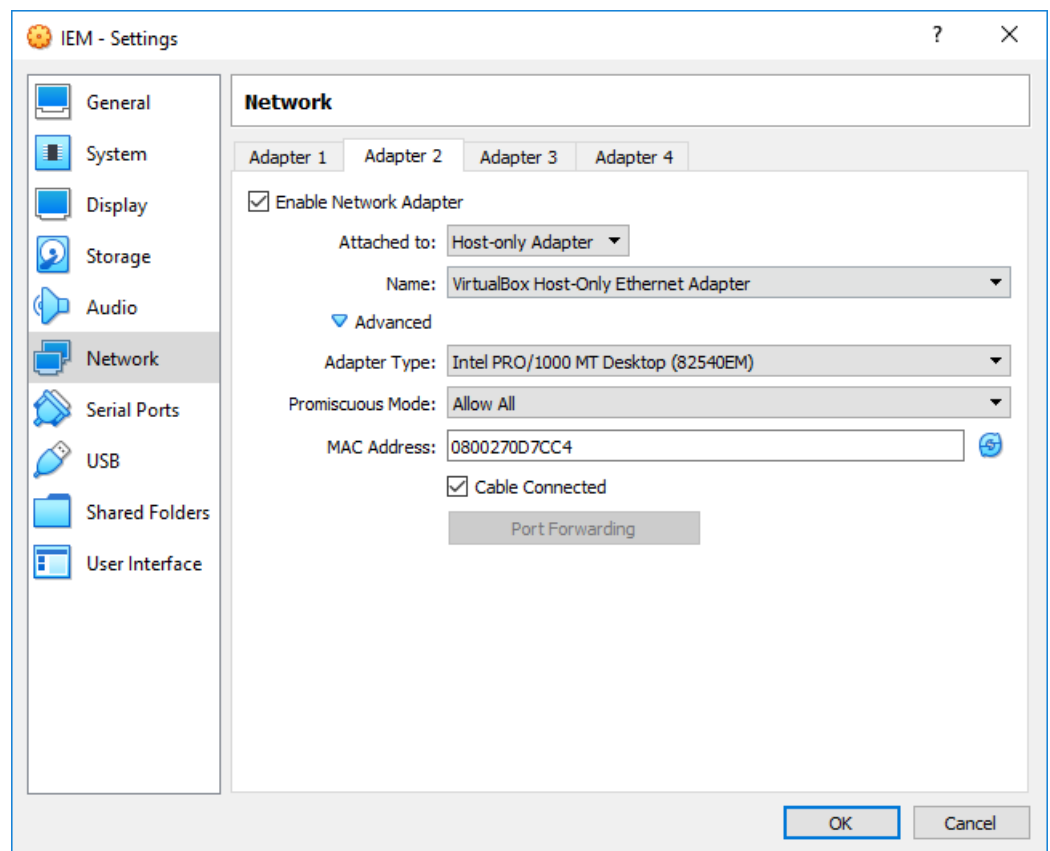
22.If you use a NAT network connection, the following settings must be configured under the "Adapter 1" tab:

- Checkbox "Enable Network Adapter" selected
- Attached to: "NAT Network"
- Name: Name of the NAT network
- Adapter type: Intel PRO/1000 MT Desktop (82540EM)
- 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 (82540EM)
- Promiscuous Mode: Allow All
- MAC Address: Random MAC address for the VM
- Checkbox "Cable Connected" selected



23. 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:

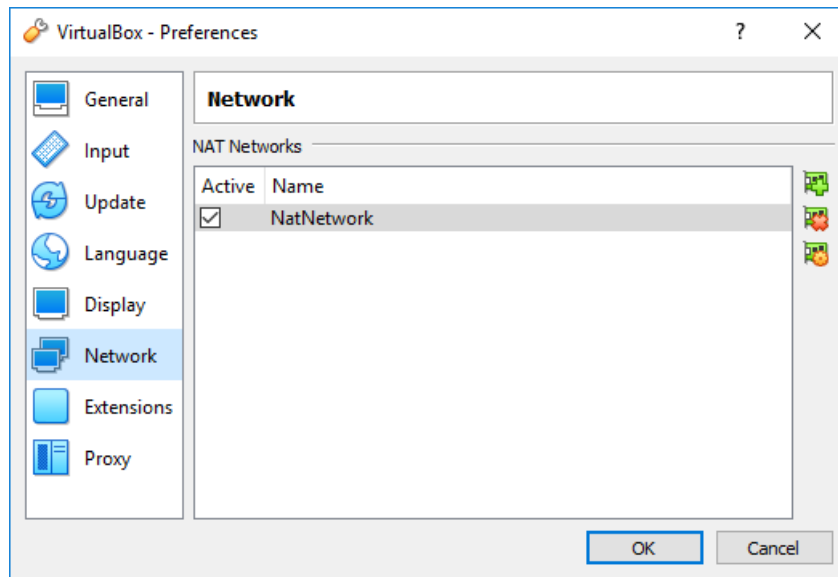
1. Click the "File > Preferences" command in the "Oracle VM VirtualBox Manager" screen.

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".

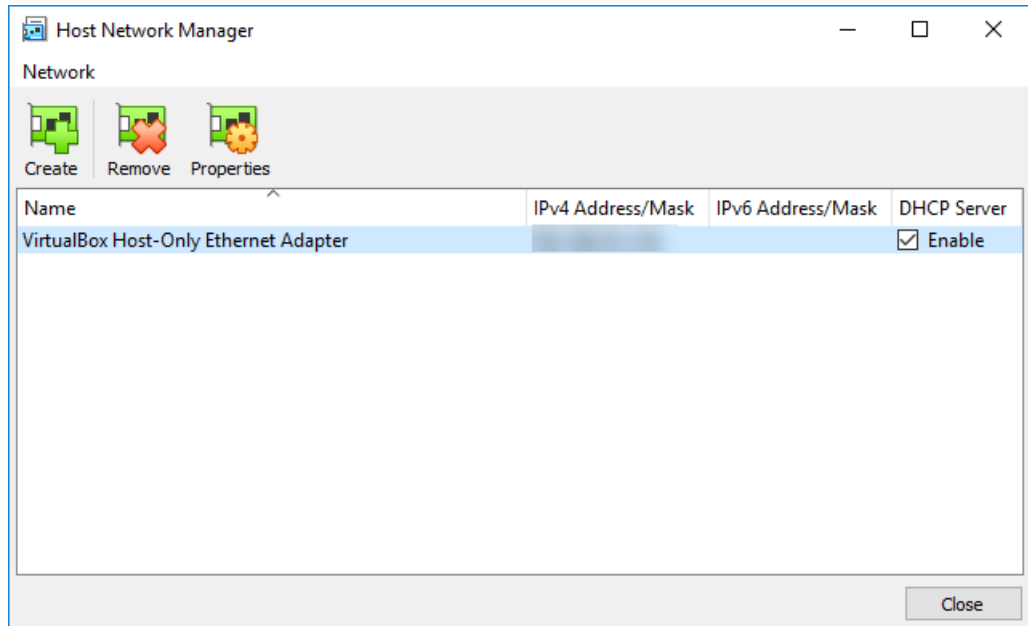
5. Click the "File > Host Network Manager" command in the "Oracle VM VirtualBox Manager" screen.

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".

2.3.5.3 Installing the Industrial Edge Management OS

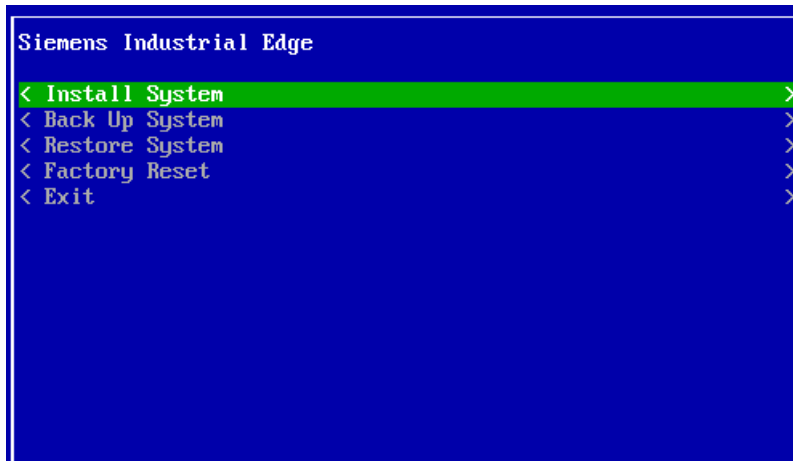
Requirement

UEFI Boot is enabled in the VM settings.

Procedure

1. Start the VM.

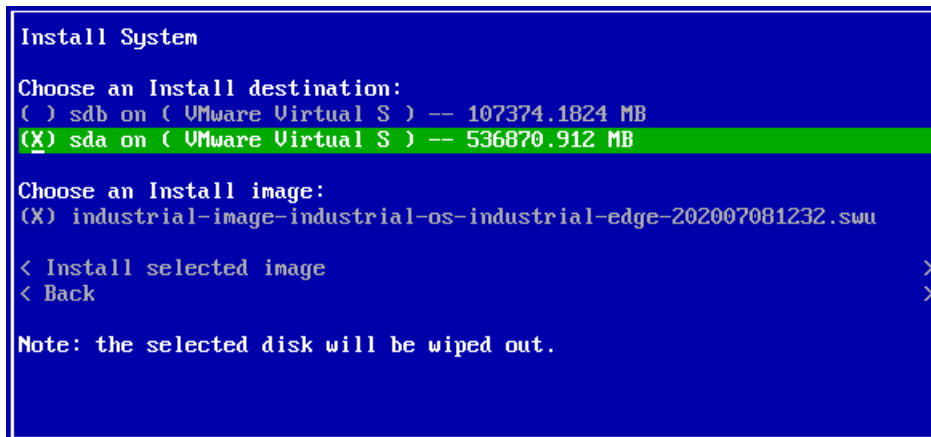
The "Siemens Industrial Edge" screen is displayed.



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.

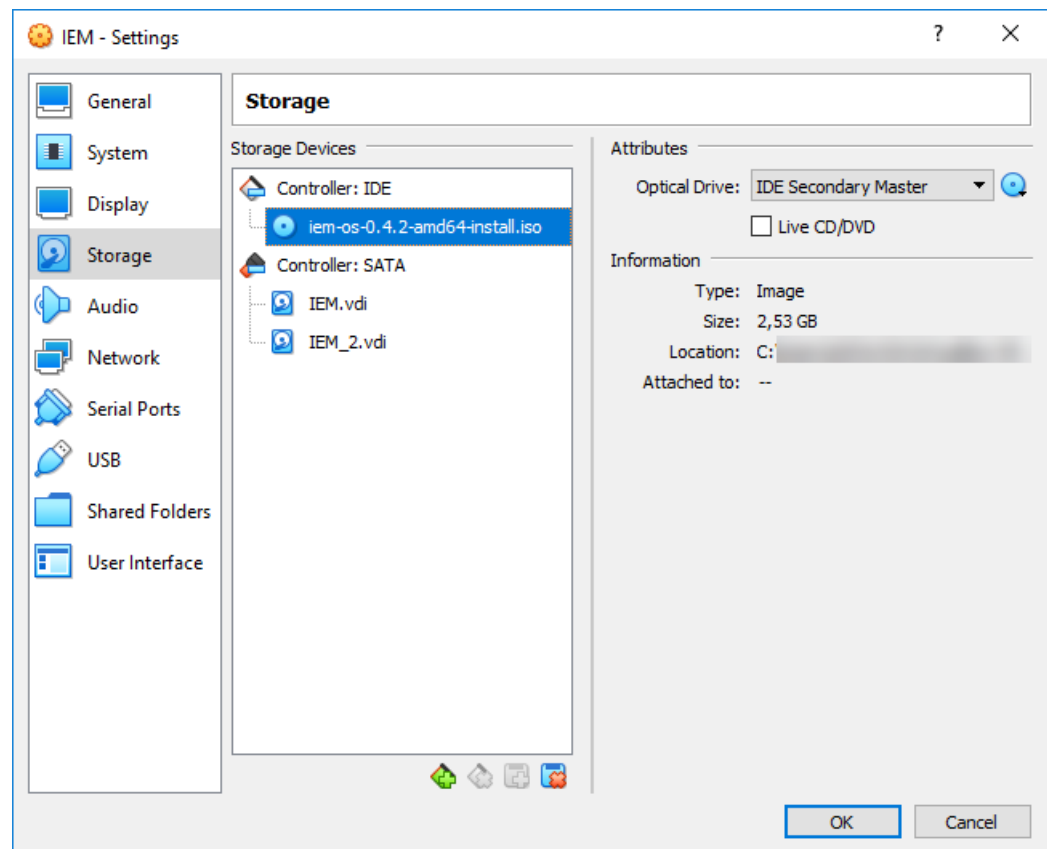
The installation of the Industrial Edge Management OS is starting.


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

The VM is getting rebooted.

When the VM is rebooted, the "Siemens Industrial Edge" screen is displayed again.

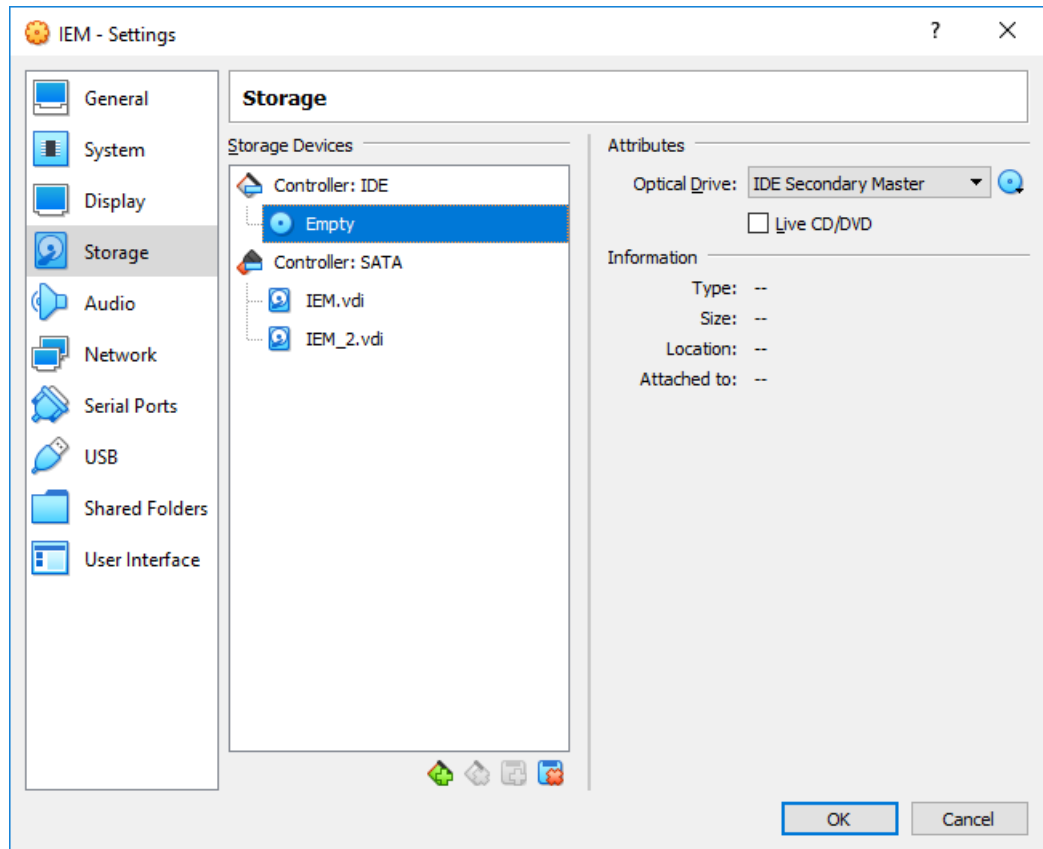
8. Close and power off the VM.
9. After the VM is powered off, select the VM and click "Settings".
10. In the navigation on the left side, click "Storage".
11. Under "Controller: IDE", select the ISO image.



12. On the right side, click the  icon.

13. Click the "Remove Disk from Virtual Drive" command.

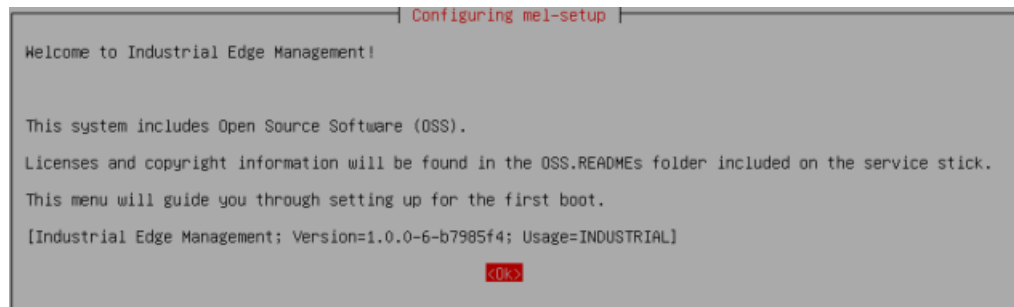
Under "Controller: IDE", "Empty" is displayed again.



14. Click "OK".

15. Start the VM.

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



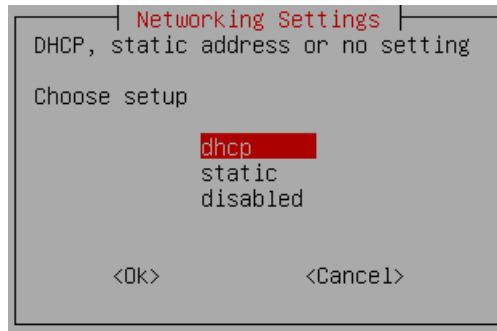
The "Configuring the Industrial Edge Management OS (Page 59)" subsection describes how to configure the IEM-OS.

2.3.6 Configuring the Industrial Edge Management OS

Procedure

1. In the welcome screen, select "Ok".
2. Select "Ok".

The "Network Settings" screen is displayed.



3. Select your network settings as required.

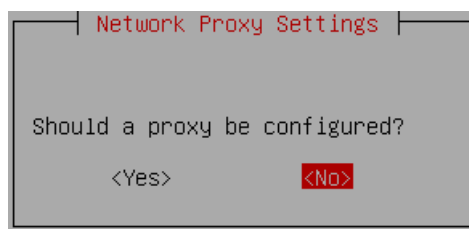
To select a network connection through DHCP, select "dhcp".

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

4. Select "No" for the proxy settings.



To use a proxy server, you can set a proxy server in the Industrial Edge Management UI.

5. After the proxy settings, select the default "English: en_US.UTF-8" localization setting.
6. Select the default keyboard model.
7. Select the default keyboard layout.
8. Select the default keyboard variant.

You must select the default keyboard model, layout and variant. Otherwise you cannot install the IEM.

9. For the "Keyboard Settings", select "No".



10. Select the "UTC" timezone.

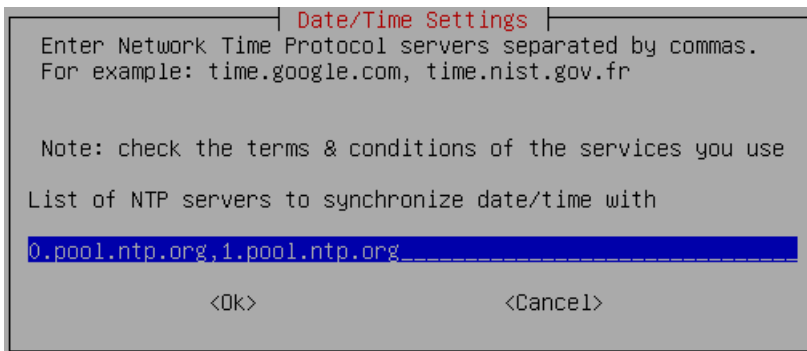
You must select the "UTC" timezone. Otherwise you cannot install the IEM.



11. Select "Ok".

12. Use a NTP server by selecting "Yes" and 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, a NTP server is mandatory.

13. To lock the settings, select "Disable". To allow reconfiguration of the settings by attaching an Industrial Edge service USB flash drive, select "Enable".

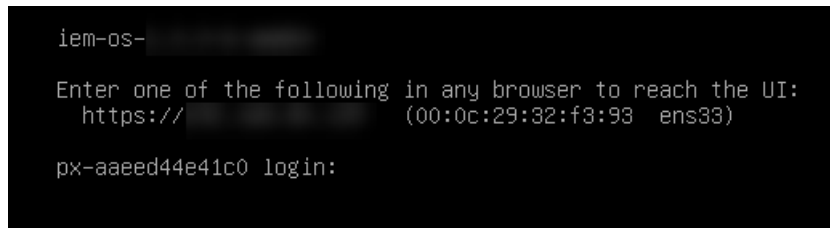
The setup is being performed.

When the setup is completed, the following screen is displayed.



14. 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.

2.3.7 Installing the IEM

To 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 cluster 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.



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

- Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

ADVANCED

Back to safety

2. Click "Advanced".

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 cluster by entering the email address and password of the admin user.

The password must meet the following criteria:

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

6. If you want the admin user for the cluster 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 cluster and for the IEM is mandatory.

8. If you need to use a proxy server, click "Settings".

The "Settings" screen is displayed. You find the procedure on how to set up a proxy server in the "Setting up a proxy server (Page 70)" subsection.

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 DNS server locally. Before you create the cluster, add the DNS server addresses to the network settings by clicking "Settings" and then clicking the edit icon under the "LAN" tab.

9. If you do not need a proxy server or after you have set up a proxy server, click "Next".
The "Certificate" tab is displayed.

The screenshot shows a web interface titled "Activate IEM Instance". At the top, there are two tabs: "1 Onboarding" and "2 Certificate", with "2 Certificate" being the active tab. Below the tabs is a "Details" section containing several input fields: "Common Name", "Organization Unit", "Organization", "Street Address", "Locality", "State / Province", and "Country". The "Country" field is a dropdown menu currently showing "United States". At the bottom of the form, there is a "Settings" link on the left, and "Back" and "Activate" buttons on the right.

10. In the "Common Name" input field, enter the Fully Qualified Domain Name (FQDN).

The FQDN is the characteristic value within a distinguished name. Typically, the FQDN is composed of the host domain name.

The "Common Name" input field is mandatory, the other input fields are optional.

11. Click "Activate".

When the activation of the IEM instance was successful, an according screen is displayed.

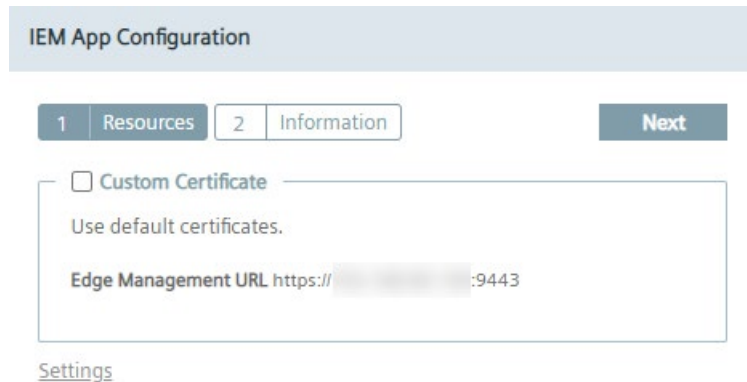
The screenshot shows a confirmation screen titled "Activate IEM Instance". Below the title, the message "IEM Instance activated successfully." is displayed. At the bottom right, there is a blue "OK" button.

12. Click "OK".

You will be redirected to the "Sign in" screen.

13. Sign in with the admin user for the cluster that you created during the setup.

The "IEM App Configuration" screen is displayed.



Note

Edge Management URL

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

Note

Settings

By clicking "Settings", the "Settings" screen is displayed in which you can configure LAN and proxy settings and download system logs.

-
14. To use the certificates from the IEM itself, disable the "Custom Certificate" check box and go to step 22.

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 due to domain name allocated certificates.

-
15. 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.

16. In the "Edge Management SSL Key" field, click "Browse" and select your private key for the IEM.

17. In the "Edge Management SSL Certificate" field, click "Browse" and select your private 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 1 of the certificates for both the IEM and the Registry server.

18. 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

Multiple DNS servers

If you are using multiple DNS servers, ensure to resolve the URL of the IEM in each DNS server. Otherwise, errors occur when you upload app versions to the IEM in the "*.app" file format.

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.

19. In the "Registry SSL Key" field, click "Browse" and select your private key for the Registry server.

20. 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.

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 used.

21. 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.

22.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.

23.If the certificates are not public trusted, deselect the "Public Trusted" check box.

In that case, you must import and accept these certificates for each other component in Industrial Edge.

24.Click "Next".

The "Information" tab is displayed.

IEM App Configuration

1 Resources
2 Information

Back
Create Cluster

IEM Cluster Network

Service Network	
IP address	Range
67.67.0.0	12
Pod Network	
IP address	Range
77.32.0.0	12

Configuration

CPU	1
Cores	2
Memory	11.83 GB
OS Disks	0
NICs	1

Network

Name	Boot Protocol	IP address
ens33	DHCP	[Redacted]

Storage

• /dev/sdb

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

25.If needed, edit the "Service Network" and the "POD Network" sections.

These network ranges must not overlap the LAN network in which the IEM is installed and both network ranges must not overlap each other.

Note

IEM Cluster Network settings

Siemens recommends to not change these settings.

26.Click "Create Cluster".

You will be redirected to the URL of the cluster.

The cluster is being created automatically. The "Create cluster" screen is displayed.



This process takes approximately 10 minutes.

27.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 cluster automatically downloads 3 images of approximately 1.5 GB. Depending on the Internet speed, the download of these images takes approximately 10 minutes.

2.3.8 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.

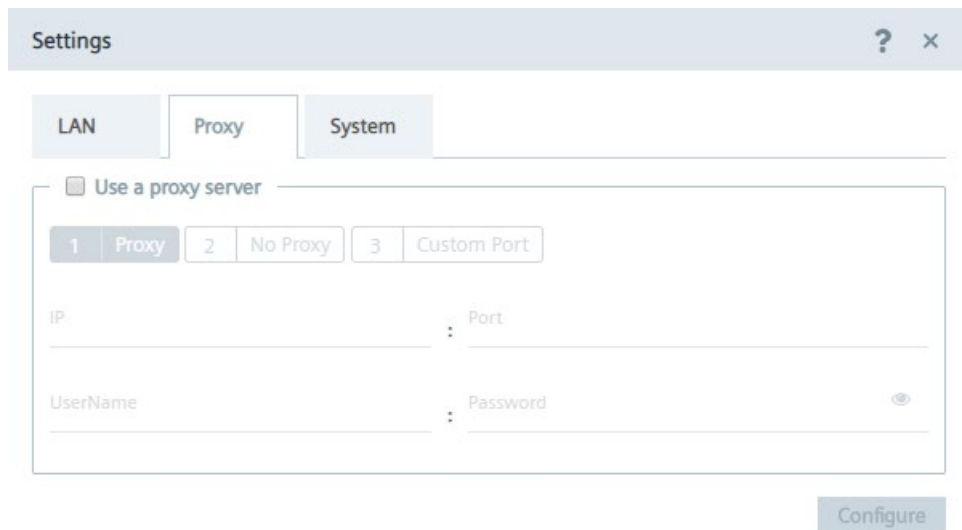
App developers do not need to implement their own proxy settings. The in this procedure described proxy settings apply for all IEM components.

Procedure

1. In the "Activate IEM Instance" screen, click "Settings".

The "Settings" screen is displayed.

2. Click the "Proxy" tab.



The screenshot shows the "Settings" interface with the "Proxy" tab selected. At the top, there are three tabs: "LAN", "Proxy", and "System". Below the tabs, there is a checkbox labeled "Use a proxy server". Underneath the checkbox, there are three radio buttons: "1 Proxy", "2 No Proxy", and "3 Custom Port". The "1 Proxy" radio button is selected. Below the radio buttons, there are four input fields: "IP", "Port", "UserName", and "Password". The "IP" and "Port" fields are on the top line, and "UserName" and "Password" are on the bottom line. There is a small eye icon next to the "Password" field. At the bottom right of the form, there is a "Configure" button.

3. To use a proxy server, click the "Use a proxy server" check box.

The input fields for the proxy server settings are enabled.

4. Enter the IP address and the corresponding port of the proxy server in the according input fields.
5. 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.

6. Click "Next".

The "No Proxy" tab is displayed.


The screenshot shows the IEM Settings window with the 'Proxy' tab selected. The 'No Proxy' sub-tab is active. A checkbox labeled 'Use a proxy server' is checked. Below it are three sub-tabs: '1 Proxy', '2 No Proxy', and '3 Custom Port'. The 'No Proxy' sub-tab is selected. An 'IP' input field with a '+' icon is present. Below it is a table with the following data:

IP address	Action
0.0.0.0/8	—
10.0.0.0/8	—
127.0.0.0/8	—
169.254.0.0/16	—
172.16.0.0/12	—
192.168.0.0/16	—
224.0.0.0/4	—
240.0.0.0/4	—

At the bottom of the window are 'Back' and 'Next' buttons.

In the "No Proxy" tab, add all the no proxy addresses that you need to run the IEM.

By default, several no proxy addresses are listed which are required by the IEM.

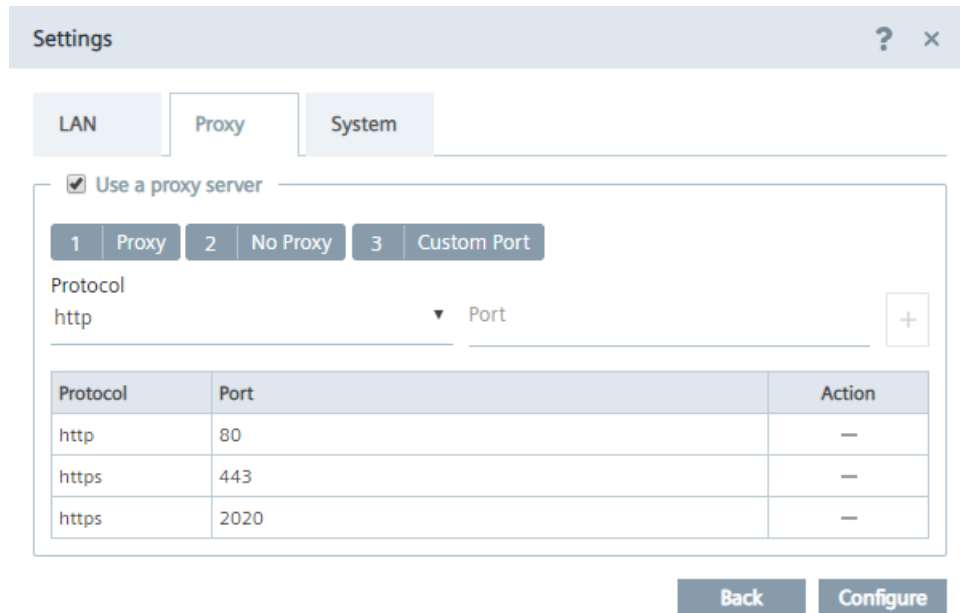
7. If you want to add a no proxy address, enter the IP or domain of the no proxy address in the "IP" input field and click the  icon.

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.

- 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.

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

The proxy settings are saved. The "Activate IEM Instance" screen is displayed to continue the IEM setup.

Note

Setting up a proxy server after IEM installation

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

2.3.9 Installing the 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 cluster.

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

Note

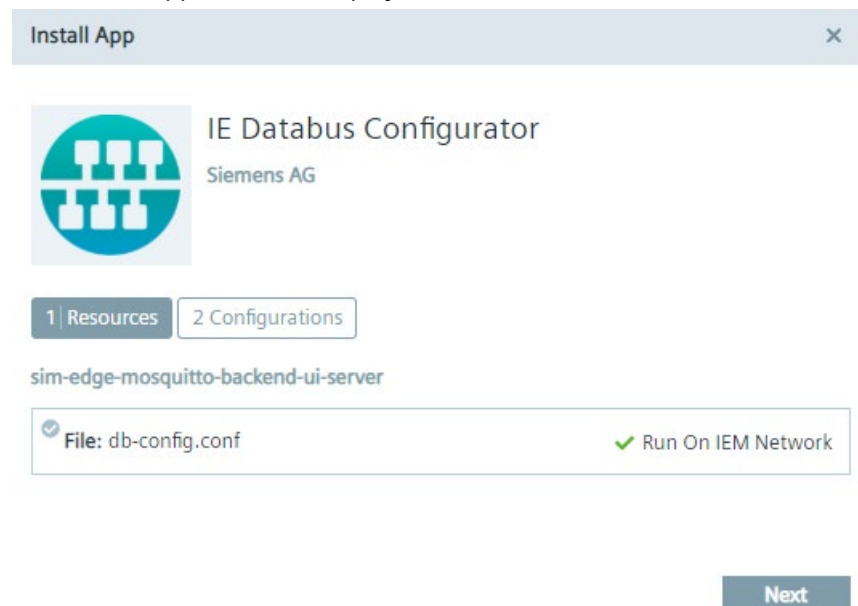
System configurators documentation

You find more information on the functionalities and the operation of the system configurators in the "System Configurators" section in the "Industrial Edge Management - Operation" manual.

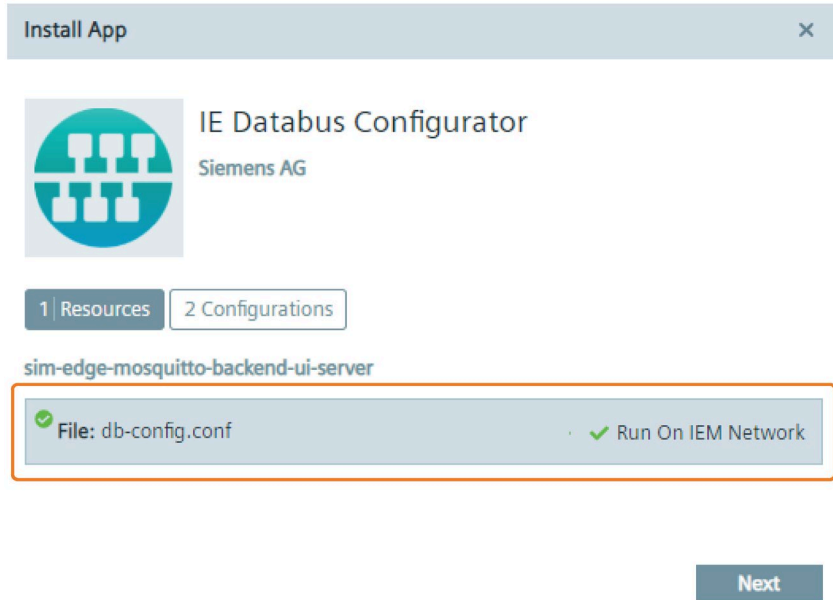
Procedure

1. In the navigation menu of the cluster, click "Catalog".
2. Click the "IE Databus Configurator" app.

The "Install App" screen is displayed.



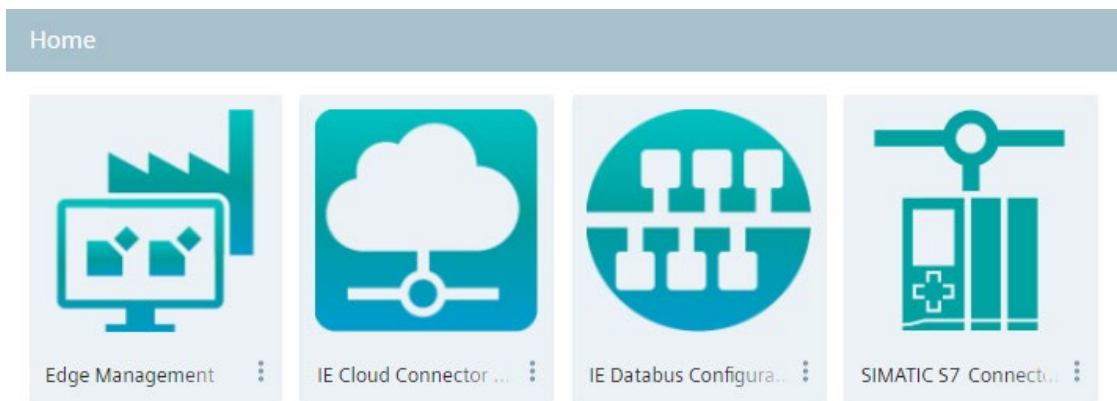
3. In the "Resources" tab, click respectively activate the available resource file.



4. Click "Next".
5. 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.
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 cluster.



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 the system apps (Page 81)" subsection.

2.3.10 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 Edge Devices in the plant network establish the connection to the relay server. This relay server allows you to access the Edge Devices from the control plane network.

Procedure

1. When the "Edge Management" app and the system configurators are installed, open the IEM by clicking on the "Edge Management" app.

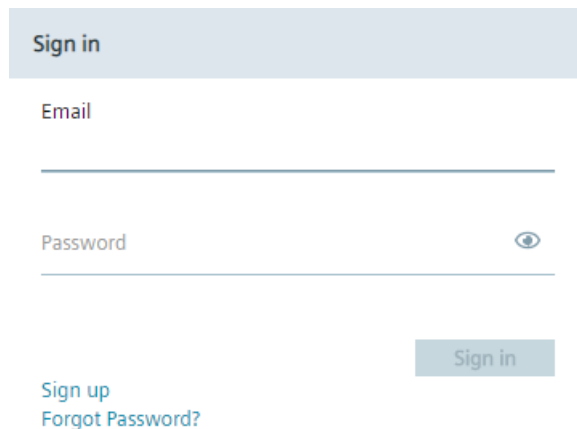
Alternatively, you open the IEM by entering the URL of the IEM, that you entered during the setup of the cluster, into an Internet browser, for example "iem.my.domain.name.com".

The login screen of the IEM is displayed.



2. Click "Sign in".

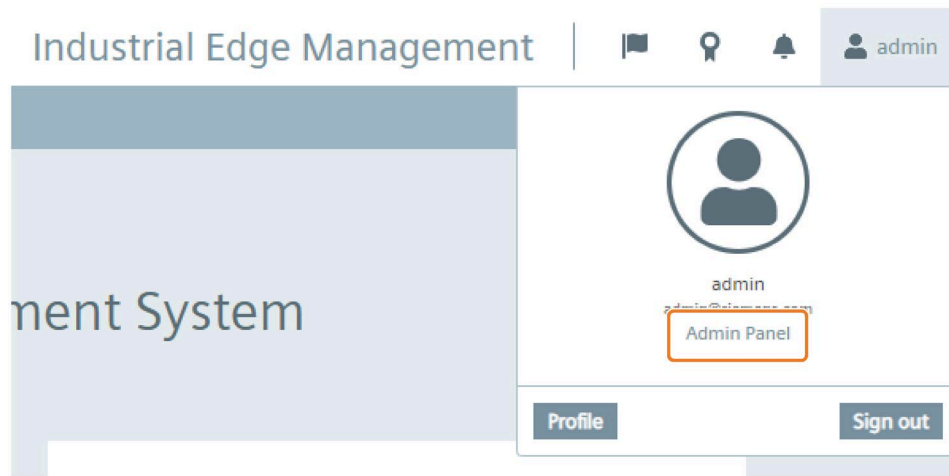
The "Sign in" screen is displayed.



3. Access the admin user by signing in with the credentials that you configured during the setup of the cluster.

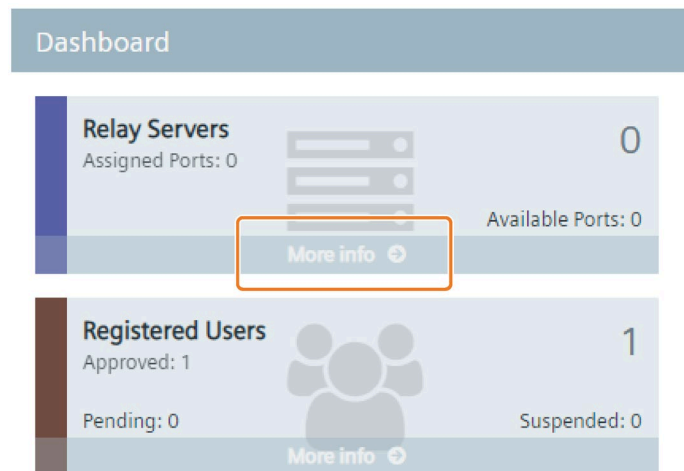
The home page of the IEM is displayed.

4. In the top-right corner, click the username.
5. Click "Admin Panel".



The "Dashboard" screen 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 cluster respectively your VM in the "IP Address" input field.

Add Relay Server ✕

Domain Name

IP Address _____ Admin Port 32500

Usable Ports

Start Range	End Range
32501	32700

Status
Enabled ▼

Label
Relay

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 the system apps

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

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

3.1 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.

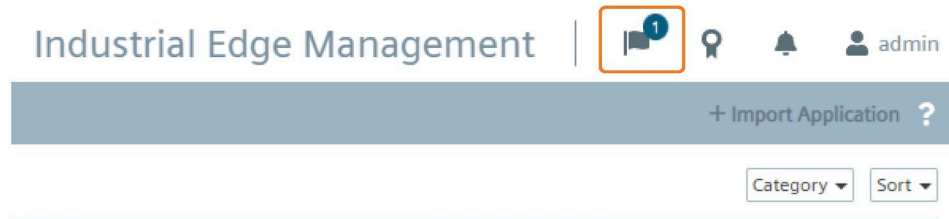


The "Copy Application to IEM catalog" screen is displayed.

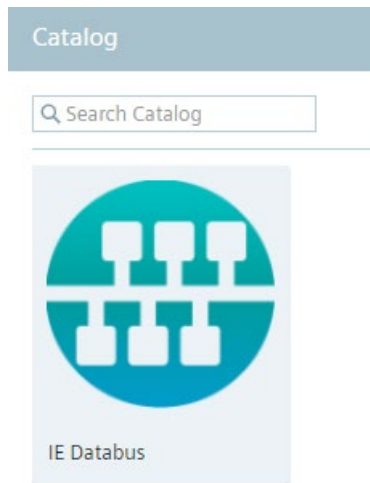
3.1 Copying system apps to the IEM

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.

3.2 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.

3.2.1 Creating the Edge Device configuration file

Procedure

1. Click "New Edge Core".



The "New Edge Core" screen is displayed.

2. In the "Core" tab, enter all the required information according to the "New Edge Device - Parameters (Page 88)" subsection.

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

New Edge Core [X]

1 Core 2 Network Interface 3 Proxy **Next**

Edge Core ID
kasan

Edge Core Name
kasan

Edge Core Username (Email)
[Redacted]

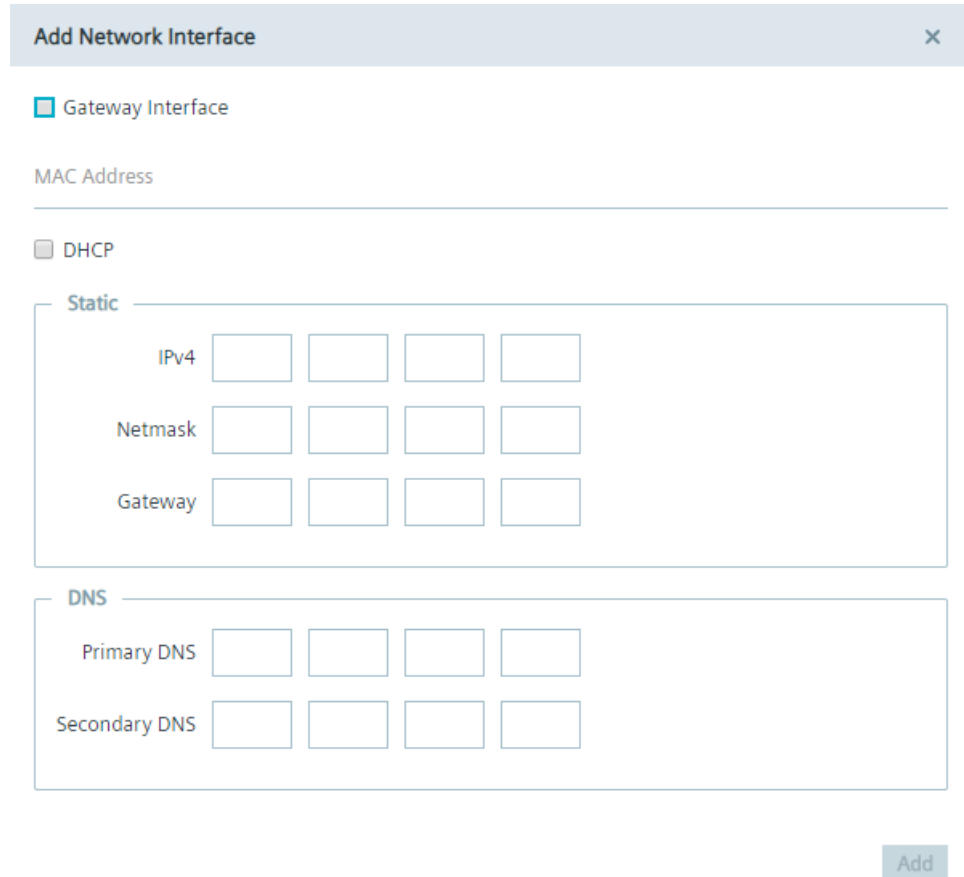
Edge Core Password
•••••• [Eye icon]

Strong

Edge Core Confirm Password
•••••• [Eye icon]

- In the "Network Interface" tab, click the  icon under the "Network Interface" section to enter the network properties of the Edge Device.

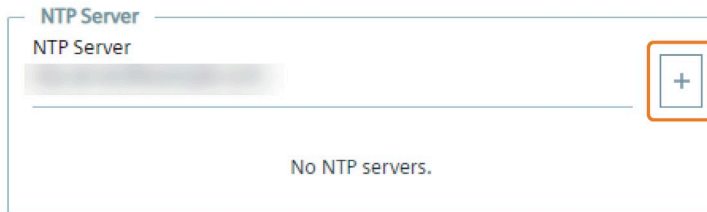
The "Add Network Interface" screen is displayed.



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

- Enter the network properties of the Edge Device according to the "New Edge Device - Parameters (Page 88)" subsection.
- Click "Add".
The network settings are added to the network interface.
- To add a Network Time Protocol (NTP) server, enter the DNS of the server in the "NTP Server" input field.

8. Click the plus icon.



The NTP server is being added.

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, a 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.

9. Click "Next".

10. In the "Proxy" tab, enter, if needed, all required proxy information according to the "New Edge Device - Parameters (Page 88)" subsection.

The screenshot shows a web interface for configuring a new edge device. The title bar reads "New Edge Core" with a close button (X). Below the title bar are three tabs: "1 Core", "2 Network Interface", and "3 Proxy", with the "Proxy" tab selected. To the right of the tabs are "Back" and "Create" buttons. The form contains the following fields and sections:

- Host:** A text input field.
- Protocol:** A dropdown menu currently set to "https".
- User:** A text input field.
- Password:** A text input field with a toggle icon (eye) to the right.
- No Proxy (Optional):** A checkbox that is currently unchecked. Below it is a text area with the instruction: "Add more IP address / domain ',' separated."
- Custom Ports:** A section with a title "Custom Ports" and a "Port" input field. To the right of the input field is a "+" button. Below the input field, it says "No custom ports."

11. Click "Create".

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

3.2.2 New Edge Device - Parameters

Device

Parameter	Description
Edge Core ID	<ul style="list-style-type: none"> • Unique domain wide ID of the Edge Device • 3 - 15 lower case letters or alphanumeric characters
Edge Core Name	<ul style="list-style-type: none"> • Unique domain wide name of the Edge Device • 3 - 15 lower case letters or alphanumeric characters
Edge Core Username	Valid email address of the user for signing into the Edge Device
Edge Core Password	Password for signing into the Edge Device

Network Interface

Parameter	Description
Gateway Interface	<ul style="list-style-type: none"> • Set the network interface as the connection interface to the IEM • If this check box is selected, you connect to the IEM through this interface • Only 1 interface can but must be selected as the "Gateway Interface"
MAC Address	<ul style="list-style-type: none"> • MAC address of the network interface of the Edge Device • Interface "X1 P1" of your Edge Device • Use colons as separations • Input of the MAC address is mandatory
DHCP	<ul style="list-style-type: none"> • Enable or disable network connection through DHCP • If this check box is selected, the network connection through DHCP is used • When the network connection through DHCP is disabled, the network connection through static IP address is used
IPv4	<ul style="list-style-type: none"> • IP address of the Edge Device in the network • Is enabled with a network connection through static IP address • Input of the IP address is mandatory for a network connection through static IP address
Netmask	<ul style="list-style-type: none"> • Is enabled with a network connection through static IP address • Input of the subnet mask is mandatory for a network connection through static IP address
Gateway	<ul style="list-style-type: none"> • IP address of the gateway • Is enabled with a network connection through static IP address • Input of the IP address is mandatory for a network connection through static IP address

Parameter	Description
Primary DNS	<ul style="list-style-type: none">Primary DNS server addressInput of the DNS server address is optional
Secondary DNS	<ul style="list-style-type: none">Secondary DNS server addressInput of the DNS server address is optional

Proxy

Parameter	Description
Host	<ul style="list-style-type: none">IP address and port of the proxyInput in the format "<IP>:<PORT>"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)	<ul style="list-style-type: none">Enable and enter no proxy addressesSeparate multiple no proxy addresses by a commaInput of no proxy address is optional
Custom Ports	<ul style="list-style-type: none">Ports that are needed for using apps on the Edge DeviceAdd further ports by clicking the plus buttonInput of custom ports is optional

3.2.3 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 IP address of the Edge Device is displayed in the IEM 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://162.235.34.23".

Note

Log file "usb-conf.log"

During the connecting process, the log file "usb-conf.log" is created in the USB flash drive. In case of any error, access the error logs from the log file to check the logs in case the connecting process has failed.

3.2.4 Connecting the Edge Device through the IEM

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://192.251.26.176".

A certificate warning is displayed.



Your connection is not private

Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

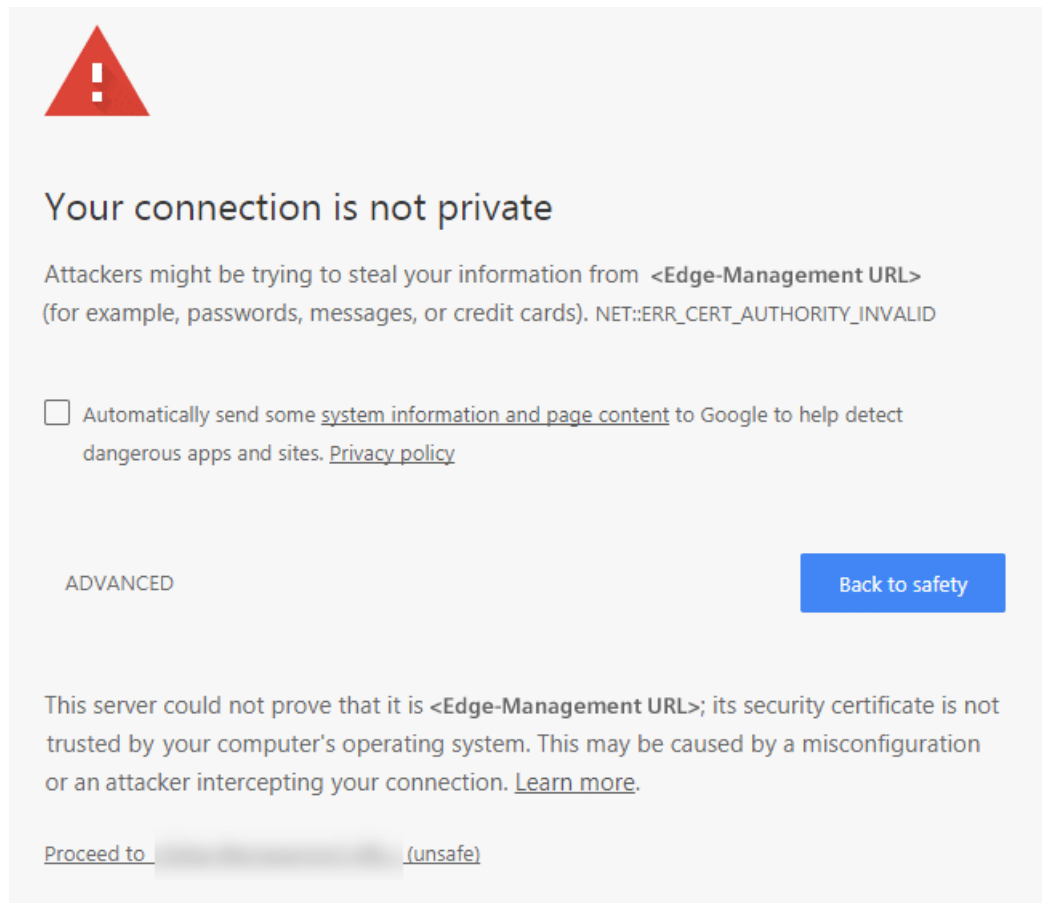
- Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

ADVANCED

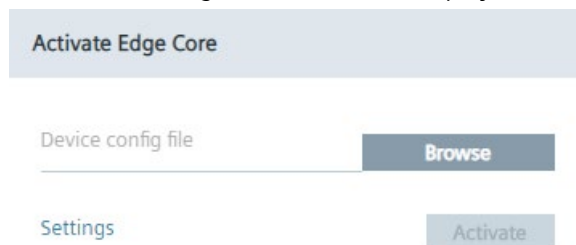
Back to safety

2. Click "Advanced".

3. Click "Proceed to [IP address]".



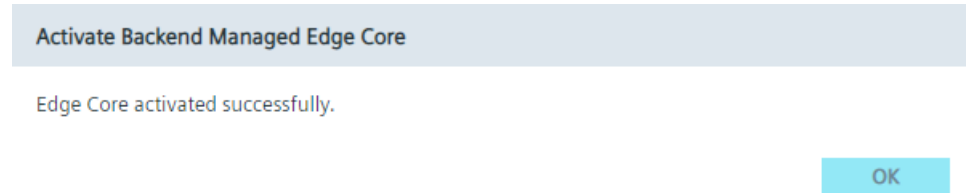
The "Activate Edge Core" screen is displayed.



4. Click "Browse" and select the created Edge Device configuration file.
5. If necessary, add and configure a proxy server under "Settings".

6. 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 IP address of the Edge Device is displayed in the IEM under the name of the Edge Device.

8. Sign in with your email address and password that you have entered in the "New Edge Core" screen.

The home page of the Edge Device UI is displayed.

3.2.5 LED status

The SIMATIC IPC227E has 4 LEDs which represent the following status:



- ① Power
- ② Run
- ③ Error
- ④ Maintenance

The following table lists all LED status changes of the Edge Device during the connecting process to the IEM and of general updating processes:

Process	Description	Power	Run	Error	Maintenance
Not connected to the IEM	When the Edge Device is not connected to the IEM, the "Run" LED flashes green.	Green	Green flashing	Off	Off
IEM-OS updates	When IEM-OS updates are in progress, the "Maintenance" LED flashes yellow.	Green	Off	Off	Yellow flashing
Connecting to the IEM	When the Edge Device is connecting to the IEM (after the USB flash drive is inserted), the "Run" LED flashes green and the "Maintenance" LED flashes yellow.	Green	Green flashing	Off	Yellow flashing
Connection to the IEM was successful	When the Edge Device is connected successfully to the IEM, the "Run" LED lights up green.	Green	Green	Off	Off
Connection to the IEM failed	When the connection to the IEM has failed, the "Error" LED flashes red.	Green	Off	Red flashing	Off

3.2.6 Example logs

The following are examples of the output of the "usb-conf.log" 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'
```

3.3 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.

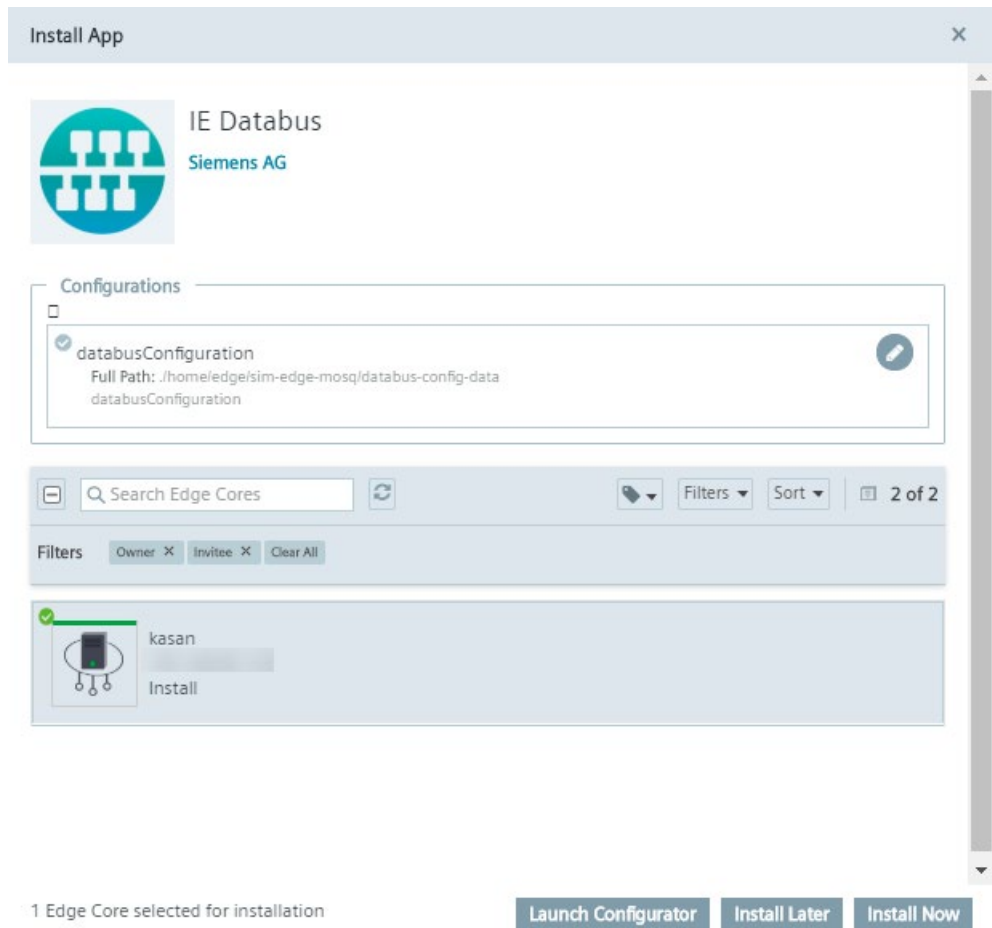
Procedure

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.
3. Click "Install".



The "Install App" screen is displayed.

- Without selecting a configuration, select the Edge Devices on which you want to install the system app.



The system configurators are only available for the Edge Devices on which the specific system apps are installed.

- Click either "Install Later" or "Install Now".

"Install Now" installs the app immediately. When you click "Install Later", select an installation time.

- To install the app, click "Allow".

You can check the installation status by clicking the tasks icon in the UI of the specific Edge Device.

3.4 Launching system configurators

Requirement

The system app has been installed on Edge Devices.

Procedure

1. In the IEM, navigate to "My Installed Apps".
All apps that are installed on any of the Edge Devices are displayed.
2. Click the tile of the "IE Databus" app.
The app details are displayed.

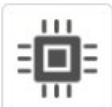
My Installed Apps > IE Databus Details ?

 **IE Databus**
Siemens AG Other
Installed on 1 Edge Core

Description
IE Databus

Events Update Configuration Delete Configuration Uninstall Start Restart Stop

Additional Information

 x86-64
V 0.4.0
231.25 MB

3. Click "Update Configuration".
The "Update Configuration" screen is displayed.

4. Without selecting a configuration, select 1 of the Edge Devices on which the system app is installed.

Note

Multiple Edge Devices

Selecting more than 1 Edge Device is not valid and results in an error when you open the system configurator. Only 1 Edge Device can be selected at each time.

5. Click "Launch Configurator".

The Databus configurator is displayed in a new screen with the configurations for the selected Edge Device.


Working with the IEM

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.

SIMATIC S7 Connector

Configure Data Source for kasan 

✔ Start operation successful.

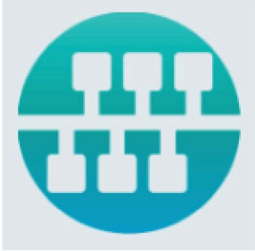
<input type="checkbox"/>	Name	Comments	Address	Data Type	Acquisition Cycle	Acquisition Mode	Actions
<input type="checkbox"/>							
<input type="checkbox"/>	▶ S7-1500 						   
<input type="checkbox"/>	▶ S7-1200 						   

You find information on connecting controllers with your Edge Devices in the "System Configurators" section in the "Industrial Edge Management - Operation" manual.

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" module to install your own app, or the "Catalog" module to install public Edge Apps from the IE Hub, on your Edge Devices.

Catalog > IE Databus Details ?

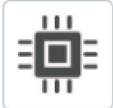


IE Databus
Siemens AG Other

Install

Description
IE Databus

Additional Information



x86-64
V 0.4.0
231.25 MB

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" manual.

- 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.

The screenshot shows the 'IE Databus' configuration interface for 'kasan'. It features 'Import' and 'Export' buttons. Below are 'User View' and 'Topic View' tabs. The 'User View' shows a search for 'edge'. The 'Topic View' shows a table of topics and their access rights.

Topic	Access Rights
<input type="checkbox"/> simatic/tags/#	Publish and Subscribe
<input type="checkbox"/> simatic/alarms/#	Publish and Subscribe

You find information on access rights for the IE Databus data in the "System Configurators" section in the "Industrial Edge Management - Operation" manual.

- Use the "My Installed Apps" entry to start your app in the app details.
- Use the data of your app for your tasks.
- If you want to send data to the cloud, use the IE Cloud Connector Configurator.

The screenshot shows the 'IE Cloud Connector Configurator' interface. It has three main sections: 'Bus Adaptor', 'Connecting Routes', and 'Cloud Connector Clients'. Each section has a table of configurations.

Topic Name	Name	Name	Type
<input checked="" type="checkbox"/> Edge	Route_Edge	<input checked="" type="checkbox"/> Edge_device	azure
		<input type="checkbox"/> Local	local_lake

You find information on sending data to the cloud in the "System Configurators" section in the "Industrial Edge Management - Operation" manual.

List of abbreviations/acronyms

Abbrevia- tion	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

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 runs locally in a VM based cluster.

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.

