SIEMENS

Industrial Edge Management - Operation 04/22

Operating Manual

04/2022

A5E50177922-AI

Legal information

Warning notice system

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

⚠DANGER

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

⚠WARNING

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

⚠CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠WARNING

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E50177922-AI
Ⓟ 04/2022 Subject to change

Preface

Purpose of this document

This documentation provides the basic information you need to operate the functions of the Industrial Edge Management.

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

Basic knowledge required

- Solid knowledge of personal computers is required.
- Solid knowledge of Linux-based operating systems is required.
- Solid knowledge of IP-based networks is required.
- Solid knowledge of Docker is required.
- Solid knowledge of creating Docker images 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 operating manual 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

Industrial security 1

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

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

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

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

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

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

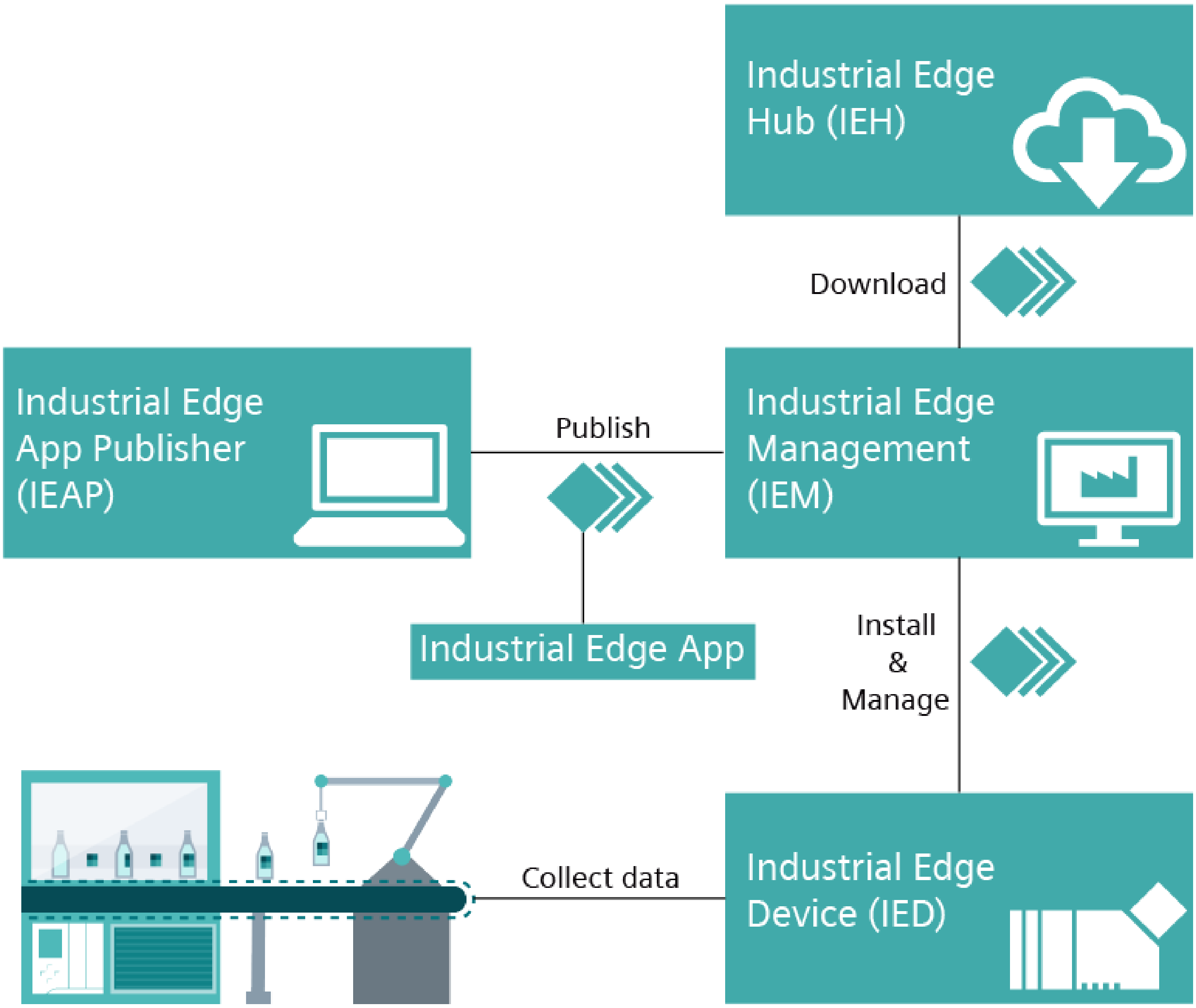
Follow the recommendations stated in this document. In addition, observe and follow the security statements, which are valid for this documentation, from the "Industrial Edge - Security Overview (https://support.industry.siemens.com/cs/us/en/view/109781002)" manual. Following these recommendations and security statements ensures that Siemens will provide correct response in case some vulnerabilities are found in the system.

Overview of Industrial Edge 2

Industrial Edge combines local engineering with Cloud engineering.

Industrial Edge provides you with the following options:

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


Industrial Edge Hub (IEH)
Download
Industrial Edge App Publisher (IEAP)
Publish
Industrial Edge Management (IEM)
Industrial Edge App
Install & Manage
Collect data
Industrial Edge Device (IED)

Industrial Edge consists of the following main components:

- Industrial Edge Hub (IEH):

  The Industrial Edge Hub (IEH) is placed in the cloud level and is the central starting point of Industrial Edge. 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 placed in the factory level and 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 Devices:

  Industrial Edge Devices (IEDs) are placed in the field level where the data generation and acquisition from automation systems take place. 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. Once provisioned and connected, the IEM activates the Edge Device through an Edge Device configuration file.

- Industrial Edge Apps:

  Industrial Edge Apps are used for intelligent processing of automation data. Edge Apps are available from Siemens, business partners (App Partners), third-party vendors or from your own development. You use the IEM to configure, install and maintain these Docker containerized Edge Apps to targeted Edge Devices.

- Industrial Edge App Publisher (IEAP):

  The Industrial Edge App Publisher is a software application to package Docker images to Industrial Edge Apps and to publish these Industrial Edge Apps to your IEM. The Industrial Edge Apps can then be installed on Industrial Edge Devices. The IEAP is available for Windows and Linux operating systems.

Maintenance UI

3

The Maintenance UI is the UI in which you deploy the Industrial Edge Management App and in which you configure the system to your needs. From the Maintenance UI, you also deploy configurators and IEM Services.

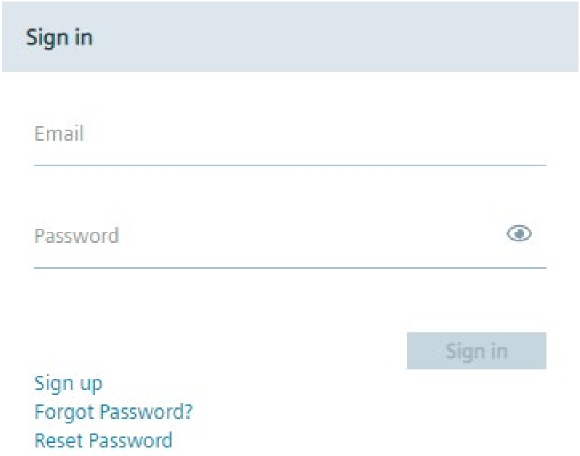
3.1 Sign up

Requirement

You have received an invitation code to sign up to the Maintenance UI.

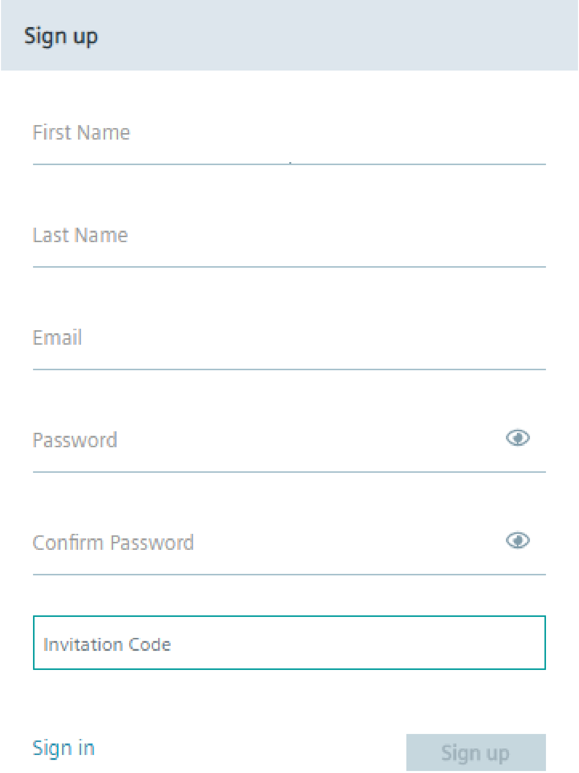
Procedure

1. Open the Maintenance UI by entering the IP address respectively domain of the Maintenance UI in the HTTPS protocol into an Internet browser.
2. Accept the privacy warning and proceed to the "Sign in" screen.



3. Click "Sign up".

   The "Sign up" screen is displayed.



Sign up

First Name

Last Name

Email

Password

Confirm Password

Invitation Code

4. Enter the required information.

   In the "Invitation code" input field, enter the received invitation code.

   The password must meet the following criteria:

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

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

5. Click "Sign Up".

   If the invitation code is valid and correct, you will be redirected to the "Sign in" screen.

   The admin of the IEM-OS must now approve your request.

6. Contact the admin of the IEM-OS for approval of your user account.

7. Wait until the admin has approved your user account.

   The approval takes some time. After the admin has approved your user account, you successfully signed up to the Maintenance UI. The admin must now contact you and inform you that you are able to log into the Maintenance UI.

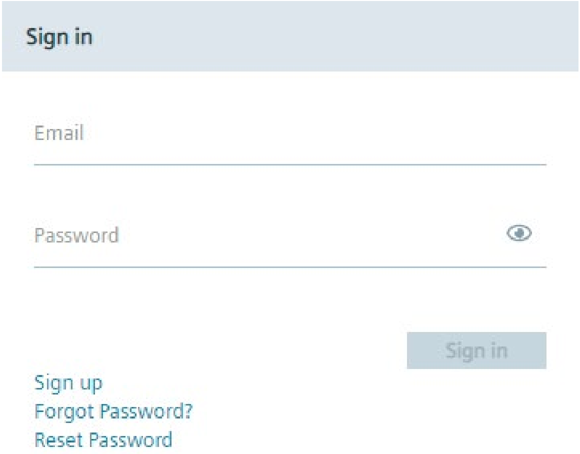
3.2 Log in

Requirement

You successfully signed up to the Maintenance UI.

Procedure

1. Open the Maintenance UI by entering the IP address respectively domain of the Maintenance UI in the HTTPS protocol into an Internet browser.
2. Accept the privacy warning and proceed to the "Sign in" screen.



3. Sign in with the credentials that you have entered during the sign up process. If you are the admin of the IEM-OS, sign in with the credentials that you have defined when you created the IEM-OS.

   After signing in, the "Home" screen is displayed.

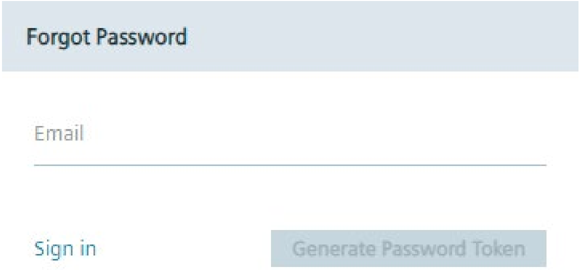
3.3 Reset password

If you have forgotten your password, you can set a new password through generating a temporarily password token.

Procedure

1. In the "Sign in" screen, click "Forgot Password".

   The "Forgot Password" screen is displayed.

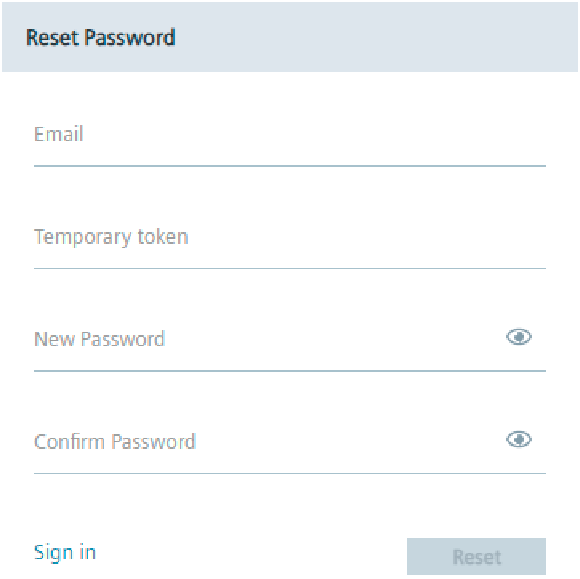


2. In the "Email" input field, enter your email address.
3. Click "Generate Password Token".

   A password token is generated which the admin can check under "Registered Users" in the Admin UI of the IEM.

   If the admin has configured an email server, you will automatically receive an email containing the password token. If the admin has not configured an email server, the admin must share the password token manually with you.

   The "Reset Password" screen will be opened.

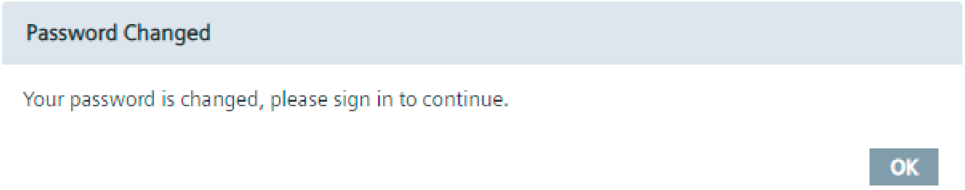


4. In case that an email server is not configured, contact the admin to receive the password token.

5. When you have received the password token, enter the following in the "Reset Password" screen:
   - Email: Your email address
   - Temporary token: Generated password token
   - New Password: New user password
   - Confirm Password: Confirm new user password

   The new password must meet again the password criteria.
6. Click "Reset".

   If the password token was valid, you successfully changed your password.



Password Changed

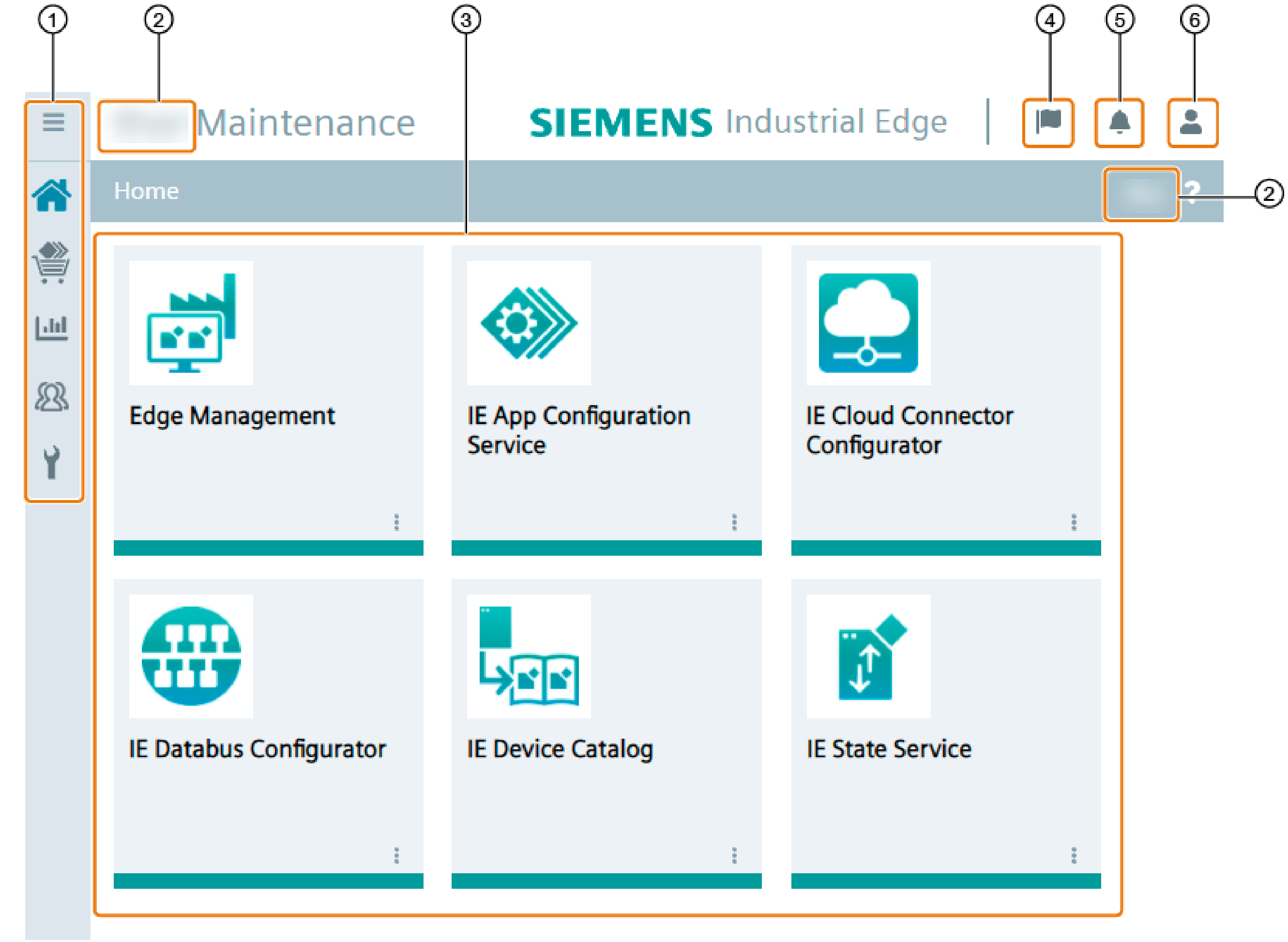
Your password is changed, please sign in to continue.

7. Click "Ok".

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

3.4 Home

The following figure shows the "Home" screen of the Maintenance UI as an example:



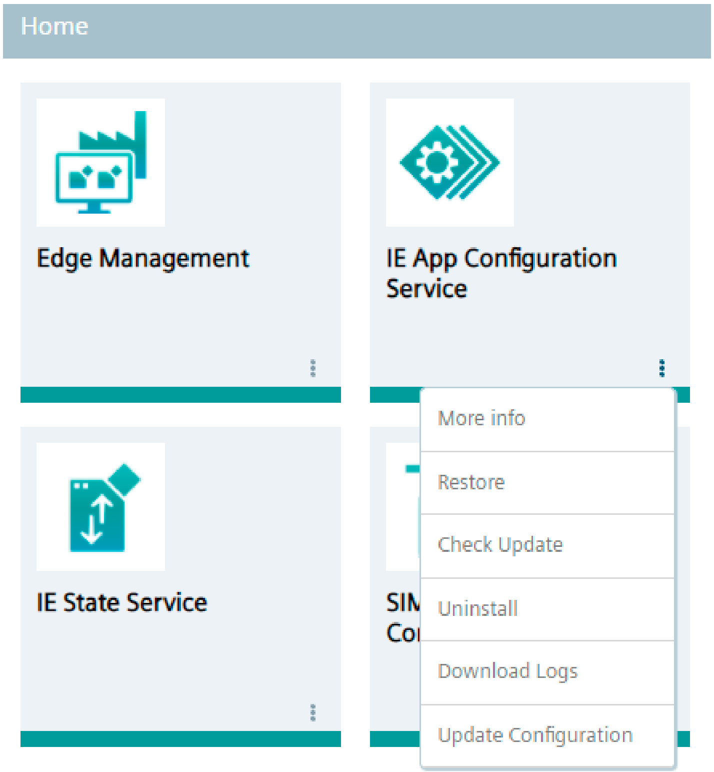
① Navigation menu
② IEM-OS name
③ Installed apps in the Maintenance UI
④ Display and close IEM-OS jobs
⑤ Display and close notifications
⑥ Sign out and edit user profile

The "Home" screen lists all apps that are installed in your IEM-OS. When you successfully create the IEM-OS, the IEM is automatically installed as "Edge Management" app in your Maintenance UI.

Before opening the IEM, ensure that all configurators are installed. You install the configurators from the catalog.

App commands

When you click the ⋮ icon in the lower part of the app tile, the following drop-down list opens for example:



The shown drop-down list has the following commands:

- More Info: Opening app details
- Restore: If a backup version of the app is available, restore the app to a saved version

Note

Disabled backup and restore feature

Since Industrial Edge Management V1.1, the "Restore" command is disabled.

- Check Update: Checking, if an app update is available
- Uninstall: Uninstalling the app
- Download Logs: Downloading the app logs as "*.tar" file
- Update Configuration: Updating the app configuration

The available app commands, and in general functionalities and operations within the IEM-OS, depend on the role respectively permissions that are assigned to the group that you have joined to access the IEM-OS. The available roles and permissions are listed in the "Roles (Page 30)" subsection.

Note

Updating the Industrial Edge Management

You find the procedure and additional information on how to update the Industrial Edge Management, the Industrial Edge Management App and other components in the "Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/10979534)" manual.

3.4.1 User profile

To open your user profile, click the user icon in the top-right corner and click "Profile". To close the user profile and return to the Maintenance UI, click "Home" below the header.

In the user profile, you have the possibility to edit the following settings:

- Profile: Editing your user profile
- Change Password: Changing your password
- Profile Picture: Setting a profile picture

Editing your profile

In the "Profile" section, you edit the following profile parameters:

Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
Email	Email address of the user

After you have updated your profile parameters, click "Update" to save your changes.

Changing password

1. In the "Current Password" input field, enter your current password.
2. In the "New Password" input field, enter your new password.

   The password must meet the following criteria:

   – At least 8 characters

   – At least 1 upper case letter

   – At least 1 special character

   – At least 1 number

   The following characters are recognized as special characters: ! @ # $ % ^ & * . ( ) _ +
3. In the "Confirm Password" input field, confirm your new password.
4. To save your new password, click "Change".

Setting a profile picture

1. To upload a profile picture, click the ✎ icon.
2. Select a profile picture.
3. To save your profile picture, click "Save".

3.4.2 Storage manager service

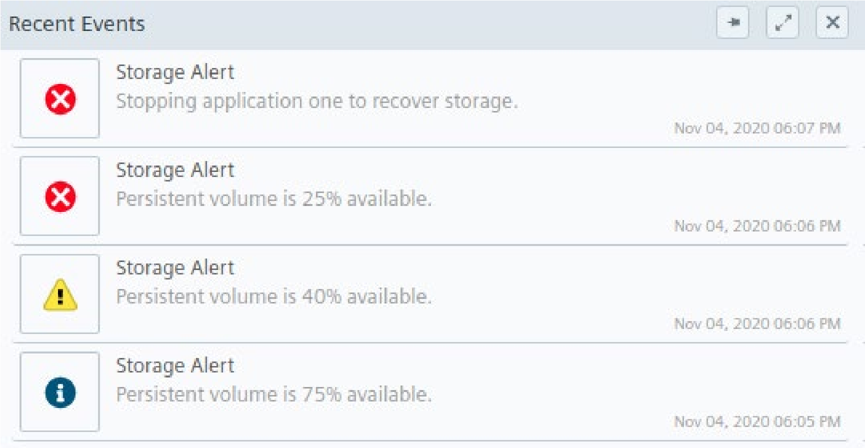
The Storage Manager Service monitors the persistent storage of the IED-OS of each Edge Device and the IEM-OS. The storage status will be notified by the service in the Edge Device UI, the Management UI and the Maintenance UI. The IED-OS storage is notified in the respective Edge Device UI and in the Management UI, the IEM-OS storage is notified in the Maintenance UI. When a storage status notification appears, you display the notification in the "Recent Events" screen respectively in the "Alerts" screen in the Management UI by clicking the 🔔 icon.

The following 3 notification types are possible:

- Information: When the used storage is lower than 55%
- Warning: When the used storage is greater than 55% and less than 70%
- Error: When the used storage is greater than 70%

In case of an error notification type, the service will clean up the storage.

The storage status notifications are displayed as follows for example:



Recent Events

Storage Alert
Stopping application one to recover storage.
Nov 04, 2020 06:07 PM

Storage Alert
Persistent volume is 25% available.
Nov 04, 2020 06:06 PM

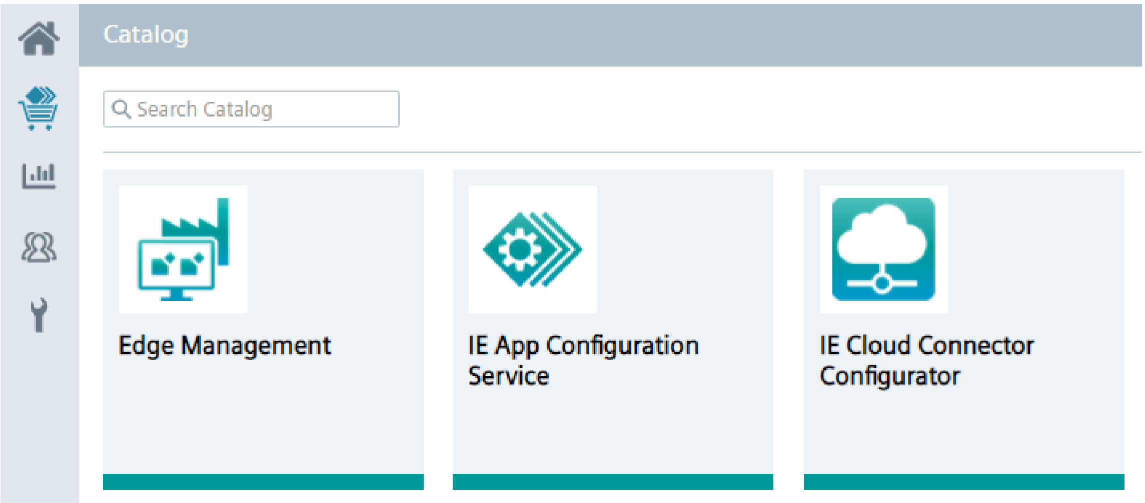
Storage Alert
Persistent volume is 40% available.
Nov 04, 2020 06:06 PM

Storage Alert
Persistent volume is 75% available.
Nov 04, 2020 06:05 PM

3.5 Catalog

The catalog provides all the available apps that you can install in the IEM-OS, for example the configurators.

The "Catalog" screen is displayed as follows for example:

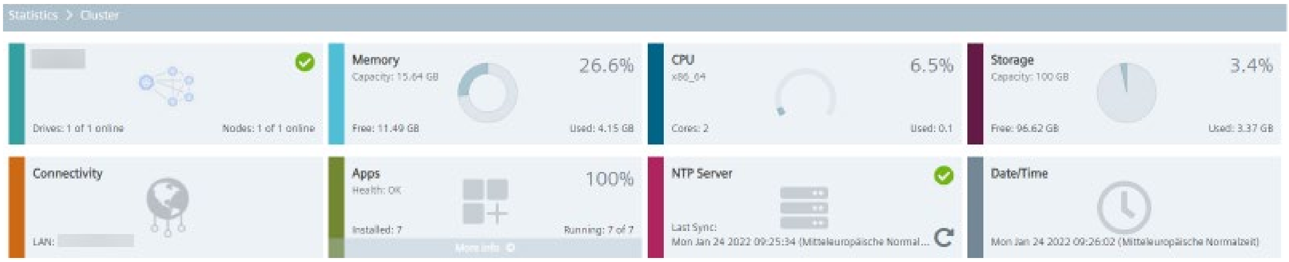


By clicking the tile of an app, you can install the app. If the app is already installed and if a new version of the app is available, you can also update the installed app from here by clicking the app tile. In this case, instead of the "Install App", the "Update Application" screen is displayed.

To use the configurators in the IEM, you must install them from the catalog in the Maintencane UI. You find more information on installing configurators in the "Installing Configurators" subsection in the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)" manual.

3.6 Statistics

In the "Statistics" screen of the Maintenance UI, you get an overview about the system properties of the IEM-OS.



Statistics > Cluster

[redacted]
Drives: 1 of 1 online
Nodes: 1 of 1 online

Memory
Capacity: 15.64 GB
26.6%
Free: 11.49 GB
Used: 4.15 GB

CPU
x86_64
6.5%
Cores: 2
Used: 0.1

Storage
Capacity: 100 GB
3.4%
Free: 96.62 GB
Used: 3.37 GB

Connectivity
LAN: [redacted]

Apps
Health: OK
100%
Installed: 7
Running: 7 of 7
More info

NTP Server
Last Sync:
Mon Jan 24 2022 09:25:34 (Mitteleuropäische Normal...

Date/Time
Mon Jan 24 2022 09:26:02 (Mitteleuropäische Normalzeit)

The "NTP Server" tile displays the status of the NTP server. The NTP server status is monitored by default every hour. You can edit the time interval under "Settings > Configuration > NTP Health Status Timers". Any changes of the NTP server status will be displayed in the "Recent Events" screen. By clicking the ↻ icon within the "NTP Server" tile, NTP services are getting restarted. Restarting NTP services may result in a time jump.

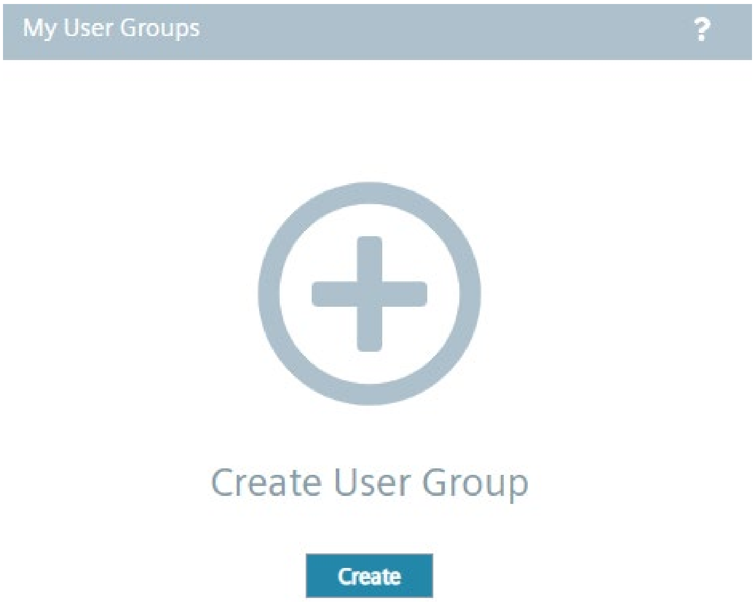
3.7 My User Groups

3.7.1 Overview

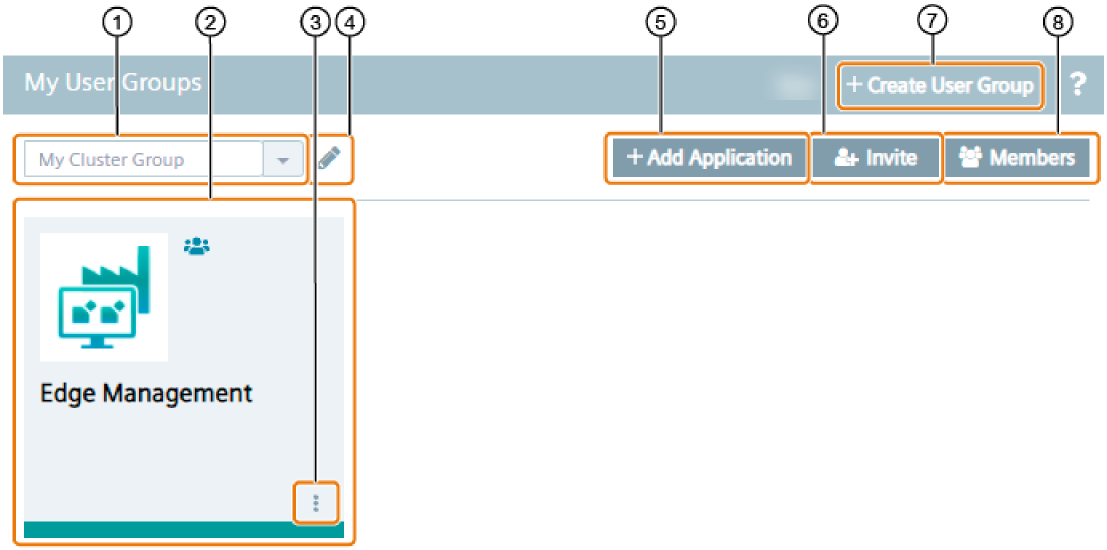
User groups enable access to apps. In the "My User Groups" screen you create your own user groups, assign apps to these user groups and add new users to the groups. In that way, you share specific apps with members of an user group. Depending on the permissions you give other group members, the members are, for example, just allowed to start apps on the IEM-OS or update apps.

The layout of the "My User Groups" screen varies depending on whether or not you have already created an user group.

If you have created no groups yet, the "My User Groups" screen is displayed as follows:



Once you have created an user group and added apps to the user group, the "Create User Group" button is displayed on the right of the title bar of the "My User Groups" screen and the "Add Application" button is enabled. The following screen shows an example:



① Drop-down list of existing user groups
② Assigned apps to the user group
③ Removing apps from the user group
④ Editing the in ① selected user group
⑤ Assign an app to the user group
⑥ Invite new members to the user group
⑦ Create a new user group
⑧ Display joined and pending users of the user group

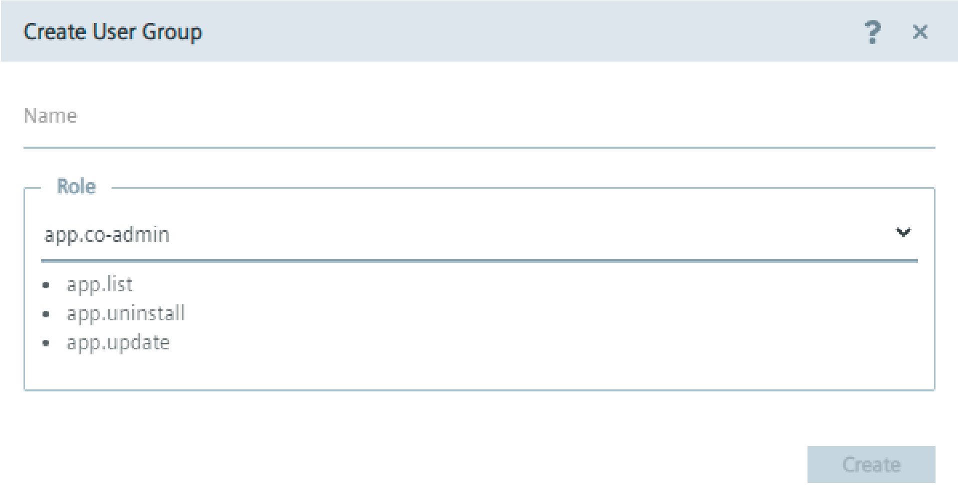
By clicking the tile of an app, the UI of the app opens, if available.

3.7.2 Creating and editing an user group

Creating a user group

1. Click "Create User Group".

   The "Create User Group" screen is displayed.



Create User Group

Name

Role

app.co-admin

- app.list
- app.uninstall
- app.update

2. In the "Name" input field, enter the name of the user group.
3. From the "Role" drop-down list, select the role respectively permissions for all members of the user group.

   You get an overview of all available roles and their permissions in the "Roles (Page 30)" subsection.
4. Click "Create".

   The user group is added to the user group drop-down list.

Editing a user group

1. From the user group drop-down list, select the user group you want to edit.
2. Click the ✎ icon next to the drop-down list.

   The "Edit User Group" screen is displayed.
3. Edit name of the user group and roles for the members.
4. To save the changes, click "Update".
5. If you want to delete a user group, click "Delete".

3.7.3 Roles

The following are the available roles:

Role	Permissions
App.co-admin	Apps: • List • Uninstall • Update
App.user	List apps
Device.co-admin	• Apps: – Create app backups – Delete app backups – Display app backups – Display app configurations – Manage app configurations – Download app logs – Display apps – Uninstall apps – Update apps • IEM-OS: – Display alerts – Manage apps – Manage IEM-OS – Download IEM-OS logs – Access job manager – Access network settings – Update NTP settings – Update proxy settings – Reboot – Update IEM-OS settings – Display catalog – Shutdown – Display IEM-OS statistics – Manage users

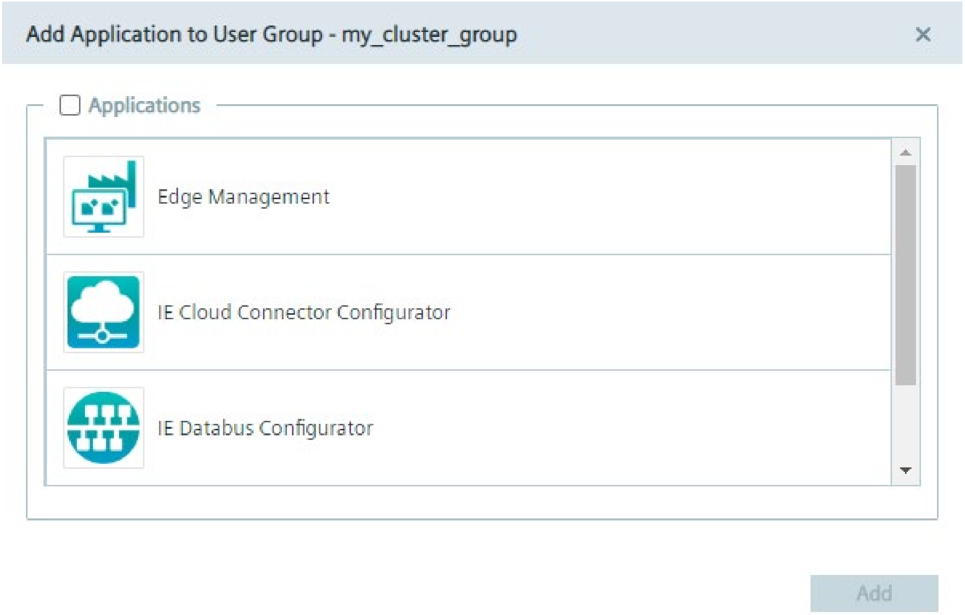
3.7.4 Adding apps

After creating an user group, you specify which apps you want to add to the user group.

Procedure

1. From the drop-down list, select the user group for which you want to add apps.
2. Click "Add Application".

   The "Add Application to User Group" screen is displayed.



Add Application to User Group - my_cluster_group

3. Select the apps you want to add to the user group.

   You add all available apps to the user group by clicking the "Applications" check box.
4. Click "Add".

   The apps are added to the user group.

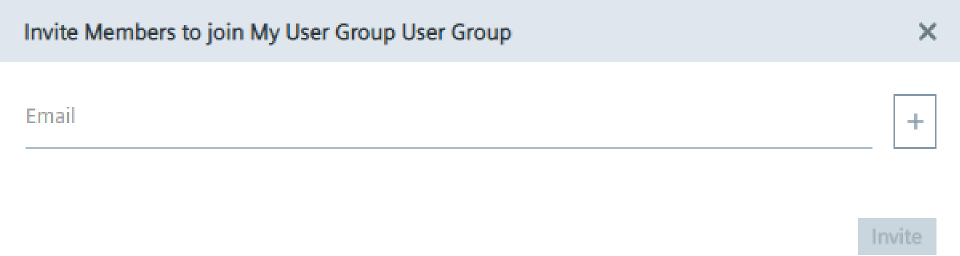
3.7.5 Inviting members

After assigning an app to an user group, you invite new users to the user group and manage the list of invited users.

Procedure

1. From the drop-down list, select the user group for which you want to invite a new user.
2. Click "Invite".

   The "Invite to User Group" screen is displayed.



3. In the "Email" input field, enter the email address of the user you want to add to the user group.
4. If you want to add more users to the user group, click the + icon.

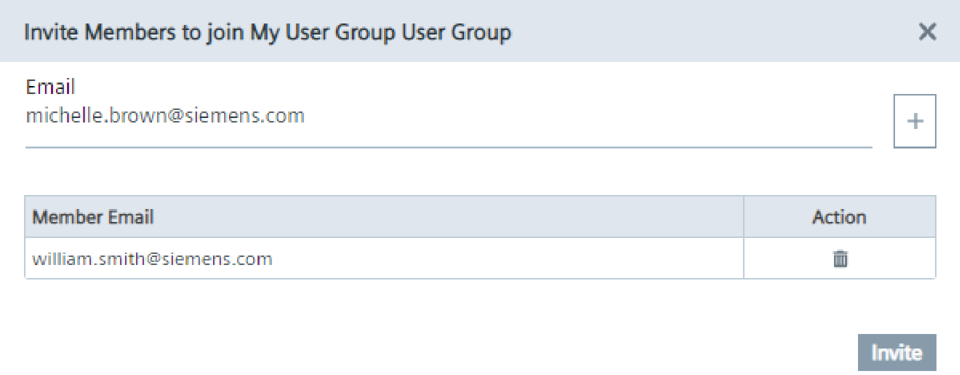
   The previously entered user is listed in the "Member Email" table.

Note

Deleting users

If you want to delete a user from the user group, click the 🗑 icon for the required user.

5. In the "Email" input field, enter the email address of the next user you want to add to the user group.



Email
michelle.brown@siemens.com

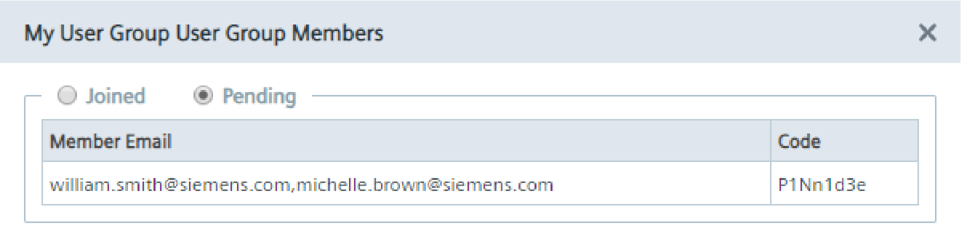
Member Email	Action
william.smith@siemens.com	🗑

6. To add the listed users to the user group, click "Invite".

   An invitation code is generated which you must send manually to the added users. The invited users then enter the invitation code in the "Invitation code" input field during signing up to the Maintenance UI. After signing up to the Maintenance UI and approving the user by the admin of the IEM-OS, the "Home" screen is displayed for the invited users with an overview of all apps that are shared within the user group. In the "Home" screen, invited users can join more user groups to the same IEM-OS by clicking "Accept Invitation".

Invited members

When you click "Members", all joined and still pending members are displayed. To remove an user from the user group, click the 🗑 icon for the required user in the "Joined" user list. When you click the "Pending" option button, all pending users and the specific invitation code are displayed in case of resending the code to the specific users.



My User Group User Group Members ✕

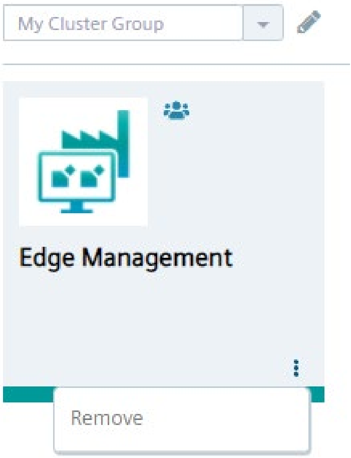
○ Joined ● Pending

Member Email	Code
william.smith@siemens.com,michelle.brown@siemens.com	P1Nn1d3e

3.7.6 Removing apps

Procedure

1. Click the ⋮ icon of the app you want to remove from the group.
2. Click "Remove".



The "Remove Application" screen is displayed.

3. Click "Remove".

The app is removed from the group.

3.8 Settings

3.8.1 Settings

Under "Settings", you manage the settings of your cluster or the node included in the cluster respectively.

By clicking the drop-down list on the left, you can switch between these 2. The first entry is the cluster which represents an overview of all available resources and nodes. The second entry represents the node which is included in the cluster and which runs containerized applications, for example the IEM-OS. At the moment, only 1 node is available.
For both, the following are the configurable settings:

- Alerts
- Configuration
- Connectivity
- Storage
- System
- Recovery

Note

Disabled backup and restore feature

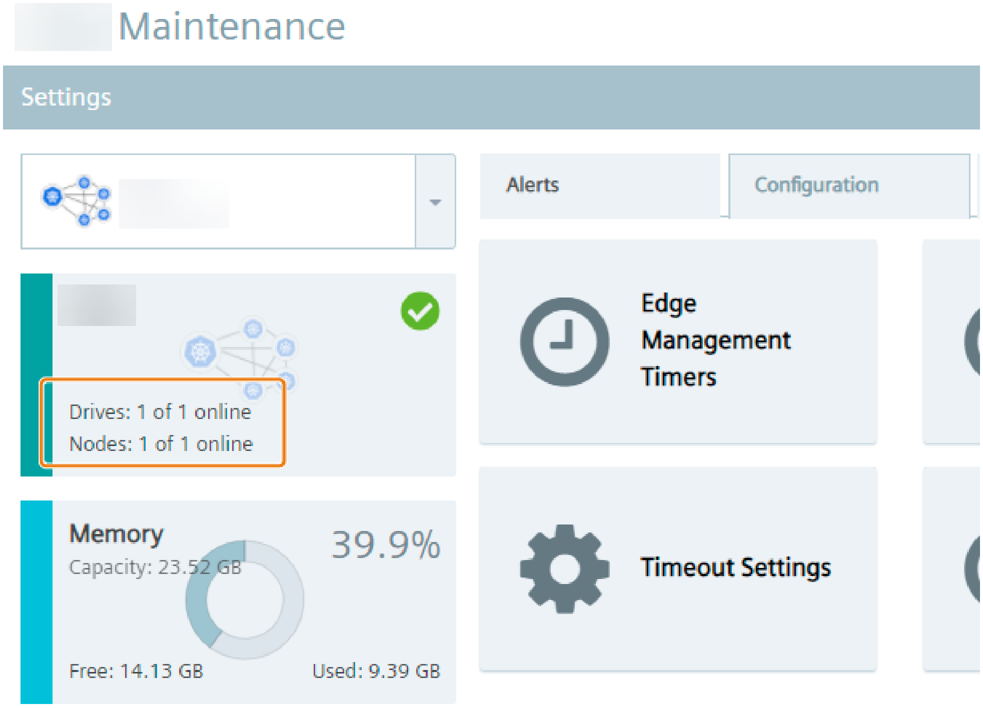
Since Industrial Edge Management V1.1, the "Recovery" tab is disabled.

- Members

The functionalities and enabled features in each tab are adapted to the selected entry from the drop-down list.

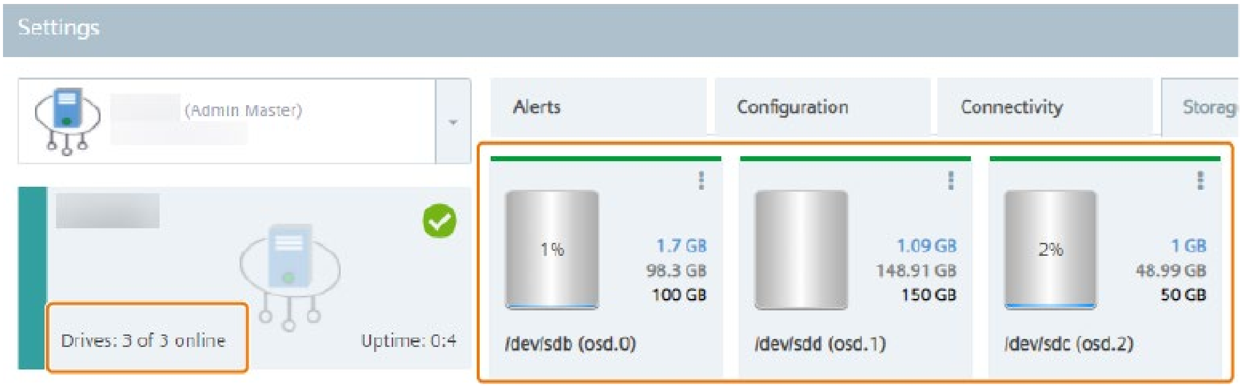
Statistics

Below the drop-down list depending on the selected entry, either the statistics and system properties of the cluster or of the node are displayed. When you select the cluster, drives and nodes and their status are being displayed.



When you setup the IEM-OS, 2 hard disks are required. The first one is for the OS and the second one is for the application's data. Drives in this case relate to the first hard disk. Nodes in this case relate to the 1 node that is included in the cluster and that you can also select from the drop-down list.

When you select the node from the drop-down list, status and number of drives are displayed as well. The node can contain multiple disks beside the one that you added when setting up the IEM-OS for the application's data. You find information on how to add a disk respectively additional storage to the system in the "Adding additional storage to the IEM (Page 41)" subsection. These disks are used to create 1 big data pool to store application's data. If you add more than 1 hard disk, this will be reflected accordingly with the drives.



If the node is offline, the drives attached to this node will also be in offline status. If the node has 3 disks and 1 disk is removed from the VM directly, the status will show 1 drive offline and 2 drives online.

3.8.2 Alerts

The "Alerts" tab lists the following alerts with regard to the cluster or the node:

- Health
- CPU
- Memory
- Storage
- Connectivity

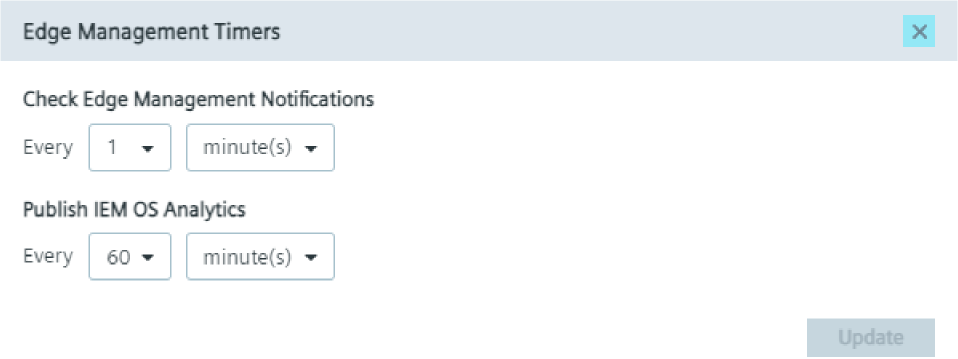
You also have the possibility to search and filter the alert list.

3.8.3 Configuration

In the "Configuration" tab you configure alerts and timer settings.

Edge Management Timers

When you click the "Edge Management Timers" tile, the "Edge Management Timers" screen is displayed:



Edge Management Timers

Check Edge Management Notifications

Every 1 minute(s)

Publish IEM OS Analytics

Every 60 minute(s)

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

- Check Edge Management Notifications:

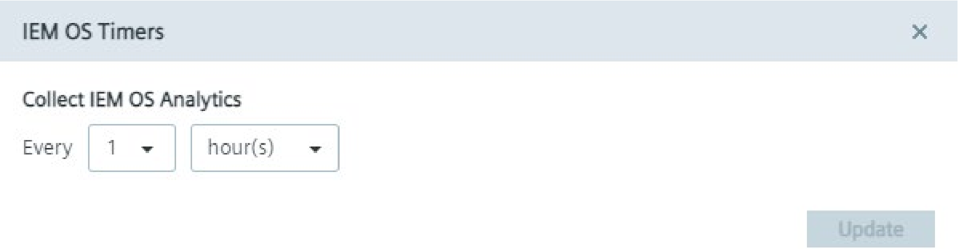
  Time period of retrieving jobs from the IEM. By default, the IEM-OS retrieves jobs every minute. Minimum value is 10 seconds and maximum value is 30 minutes.
- Publish IEM OS Analytics:

  Time Period of sending statistics of the IEM-OS to the IEM. By default, the IEM-OS sends its statistics every 60 minutes to the IEM. Minimum value is 10 seconds and maximum value is 60 minutes.

To save the changes, click "Update".

IEM OS Timers

When you click the "IEM OS Timers" tile, the "IEM OS Timers" screen is displayed:



Collect IEM OS Analytics

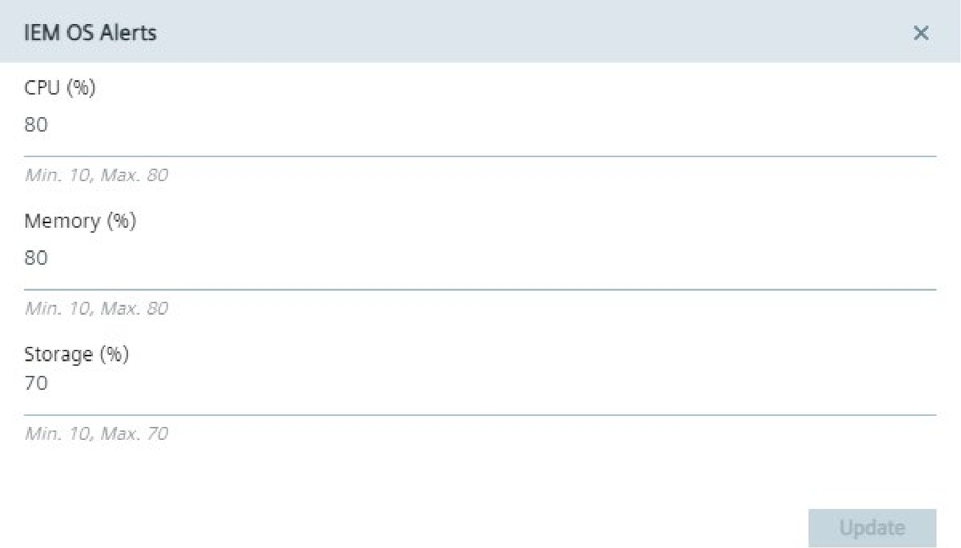
Every 1 hour(s)

In this screen, you set the time period of updating the IEM-OS statistics. By default, the IEM-OS updates every hour its statistics. Minimum value is 1 minute and maximum value is 23 hours.

To save the changes, click "Update".

IEM OS Alerts

When you click the "IEM OS Alerts" tile, the "IEM OS Alerts" screen is displayed:



CPU (%)
80
Min. 10, Max. 80

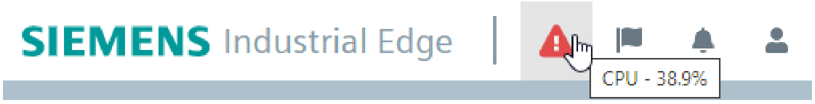
Memory (%)
80
Min. 10, Max. 80

Storage (%)
70
Min. 10, Max. 70

In this screen, you configure alert thresholds for the IEM-OS. You configure the following utilization thresholds:

- CPU
- Memory
- Storage

Whenever 1 of these resources exceeds its utilization threshold, a warning icon is displayed in the header of the Maintenance UI and its message is displayed via tooltip.

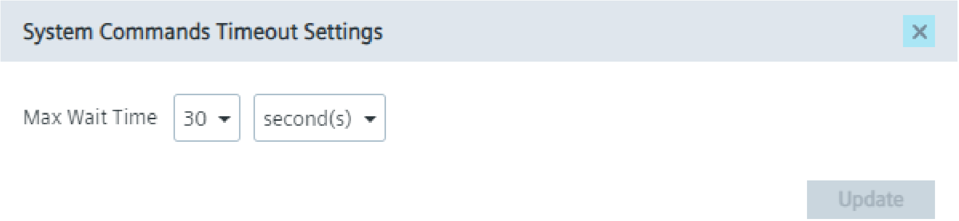


In that case, either expand the utilization threshold or decrease the utilization itself. To save the changes, click "Update".

Timeout Settings

Installed apps on the IEM-OS that are subscribed to the event service, that you have activated during the creation of the app in the IE App Publisher, receive a notification when you perform a system event, for example an IEM-OS shutdown or reboot.

When you click the "Timeout Settings" tile, the "System Commands Timeout Settings" screen is displayed:


System Commands Timeout Settings

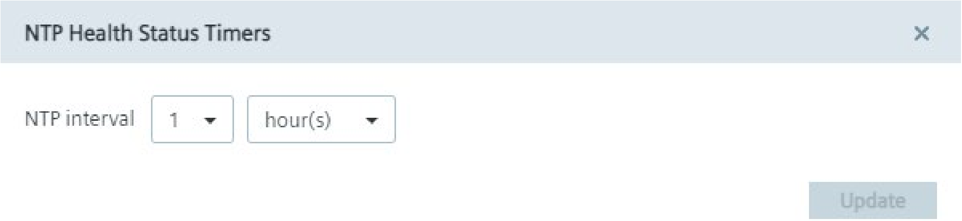
Max Wait Time 30 second(s)

In this screen, you set the maximum waiting time for these apps to acknowledge the triggered system event. After the set time has passed, the system event will be performed. By default, the maximum time is 5 minutes. Minimum value is 1 minute and maximum value is 60 minutes. To save the changes, click "Update".

If the IEM-OS does not get an acknowledgement from the app, the IEM-OS performs the system event anyways. In that case, app data may be lost.

NTP Health Status Timers

When you click the "NTP Health Status Timers" tile, the ""NTP Health Status Timers" screen is displayed:


NTP Health Status Timers

NTP interval 1 hour(s)

In this screen you set the monitoring interval in which the IEM-OS checks the NTP server status. By default, the interval is set to 1 hour. Maximum interval is 1 day and minimum interval is 1 minute. To save the changes, click "Update".

Any changes of the NTP server status will be displayed in the "Recent Events" screen.

3.8.4 Connectivity

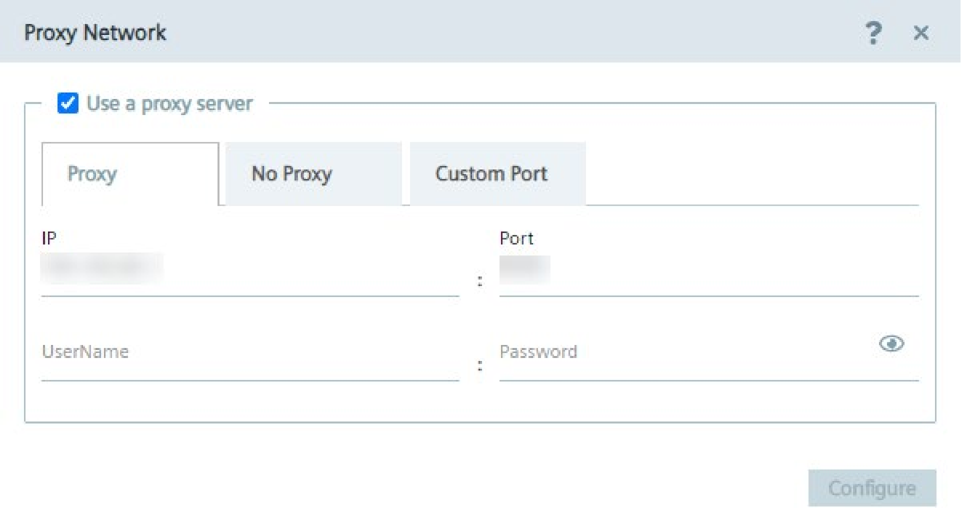
In the "Connectivity" tab, you check your network connection and set your proxy settings.

LAN Network

When you click the "LAN Network" tile, you can check the network properties of your IEM-OS. By clicking the ✎ icon, you configure your DNS servers.

Proxy Network

When you click the "Proxy Network" tile, you open the proxy settings.



Proxy Network

☑ Use a proxy server

IP [redacted] : Port [redacted]

UserName : Password

You can configure the following proxy settings:

- Proxy
- No proxy
- Custom port

After you have configured the proxy settings, you save the proxy settings by clicking "Configure".

Proxy

In the "Proxy" tab, you activate, if needed, the use of a proxy server to connect to the IEM and configure the proxy server.

To configure the proxy server, proceed as follows:

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

   The input fields for the proxy server are enabled.
2. Enter the IP address and the corresponding port of the proxy server in the according input fields.
3. In case of an additional authentication for the proxy server, enter username and the corresponding password in the according input fields.

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

   – The password must start with an alphabetic character

   – The password must not contain complex characters, such as \ . * "

   – The password must not be longer than 21 characters

   The settings apply for HTTP and HTTPS proxy servers.

No proxy

In the "No Proxy" tab, add all IP addresses which shall be accessed directly (without use of proxy).

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

If you want to add a further IP address which shall be accessed directly, enter the IP or domain in the "IP" input field and click the + icon.

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, that you have configured during the setup of the IEM, to the no proxy address list. Otherwise, several errors can occur when you use the IEM.

Custom port

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.

3.8.5 Storage

The "Storage" tab provides an overview of all created and added hard disks in the IEM-OS. Each hard disk displays the following storage properties:

- Maximum available disk space
- Used disk space
- Free disk space

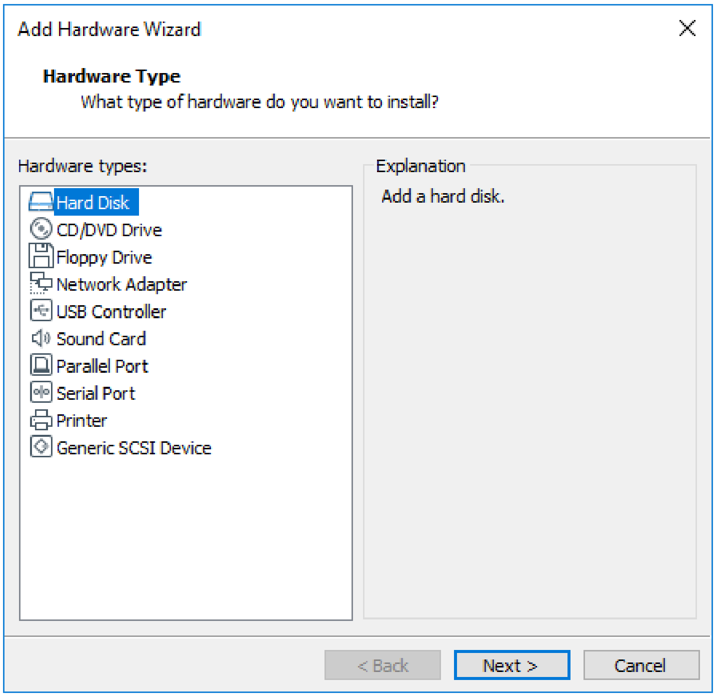
The percentage represents the used disk space.

3.8.5.1 Adding additional storage to the IEM

Adding additional hard disk - VMware Workstation

1. Open the VM settings of your IEM.
2. Under the "Hardware" tab, click "Add".

   The "Add Hardware Wizard" screen is displayed.



Add Hardware Wizard

Hardware Type

What type of hardware do you want to install?

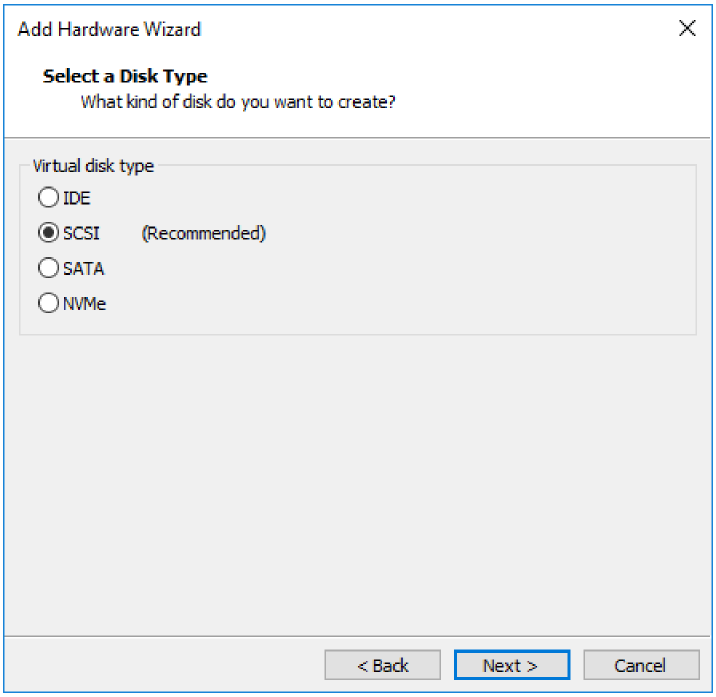
Hardware types:

Explanation

Add a hard disk.

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

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



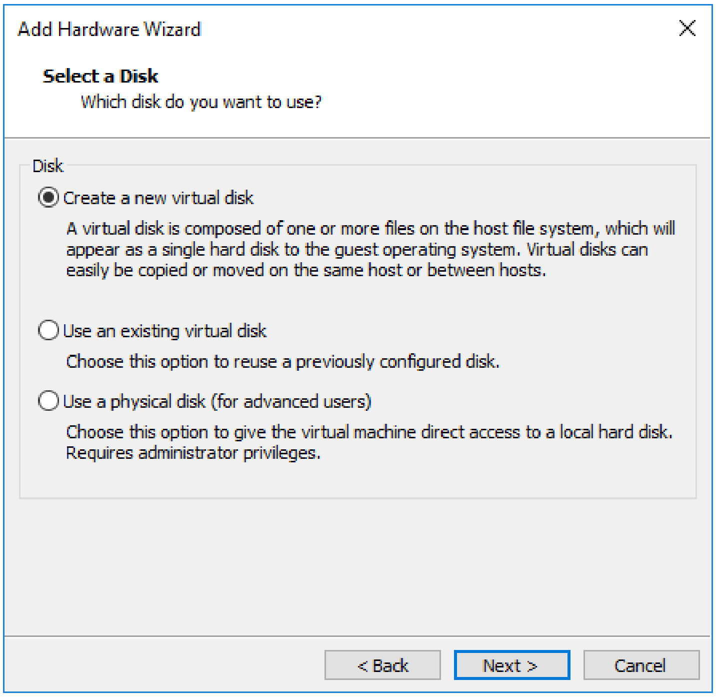
Add Hardware Wizard

Select a Disk Type
What kind of disk do you want to create?

Virtual disk type

○ IDE
● SCSI (Recommended)
○ SATA
○ NVMe

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



Add Hardware Wizard

Select a Disk
Which disk do you want to use?

Disk

● Create a new virtual disk

A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.

○ Use an existing virtual disk

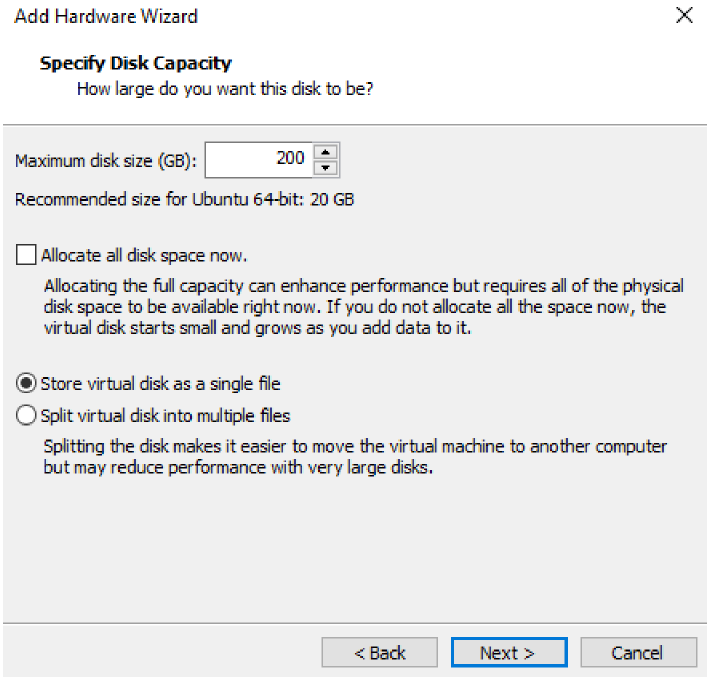
Choose this option to reuse a previously configured disk.

○ Use a physical disk (for advanced users)

Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.

6. Specify your needed disk size.

7. Select "Store virtual disk as a single file" and click "Next".



Add Hardware Wizard

Specify Disk Capacity
How large do you want this disk to be?

Maximum disk size (GB): 200

Recommended size for Ubuntu 64-bit: 20 GB

□ Allocate all disk space now.

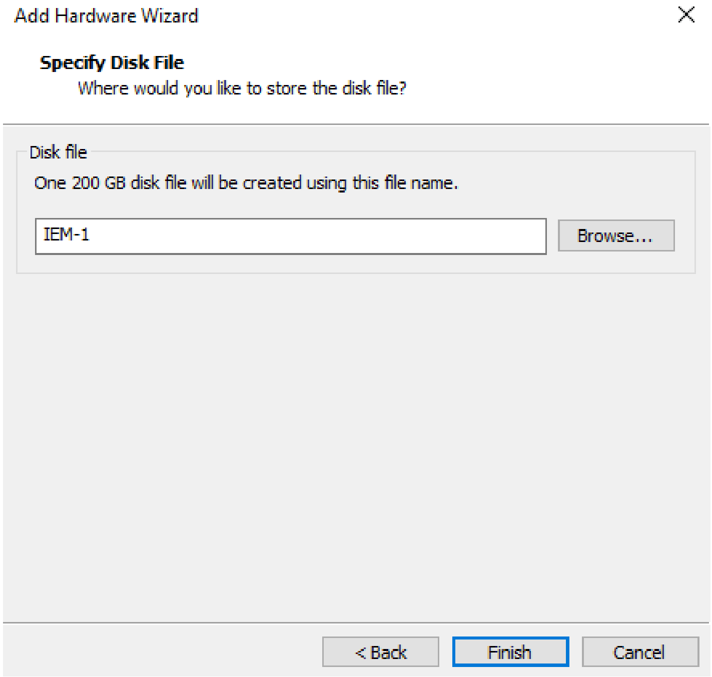
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

● Store virtual disk as a single file

○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

8. If you want to, change the recommended name of the new virtual disk.



Add Hardware Wizard

Specify Disk File
Where would you like to store the disk file?

Disk file

One 200 GB disk file will be created using this file name.

IEM-1

The disk file will be stored under the entered file name.

9. Click "Finish".

   The new virtual hard disk has been created and is added to the hardware list in the left navigation.

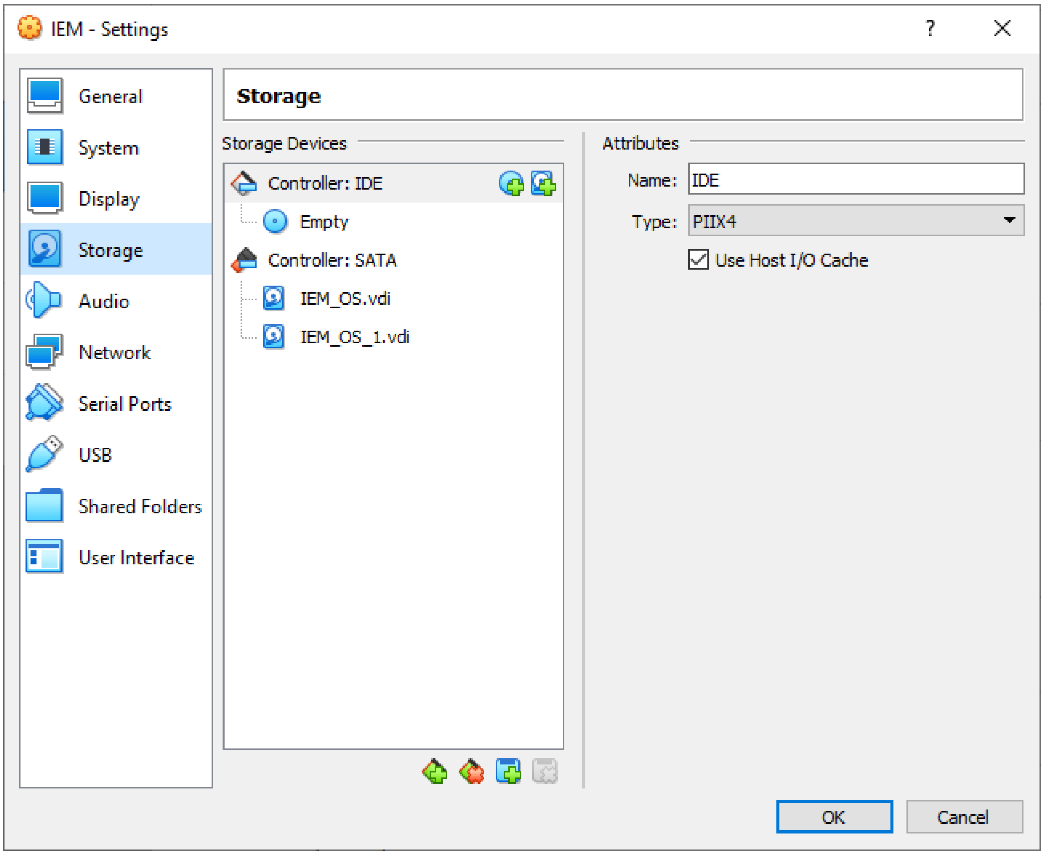
10. Close the VM settings.

Adding additional hard disk - Oracle VirtualBox

1. Select the VM on which the IEM-OS runs.
2. Click "Settings".

   The VM settings are displayed.

3. In the navigation on the left side, click "Storage".



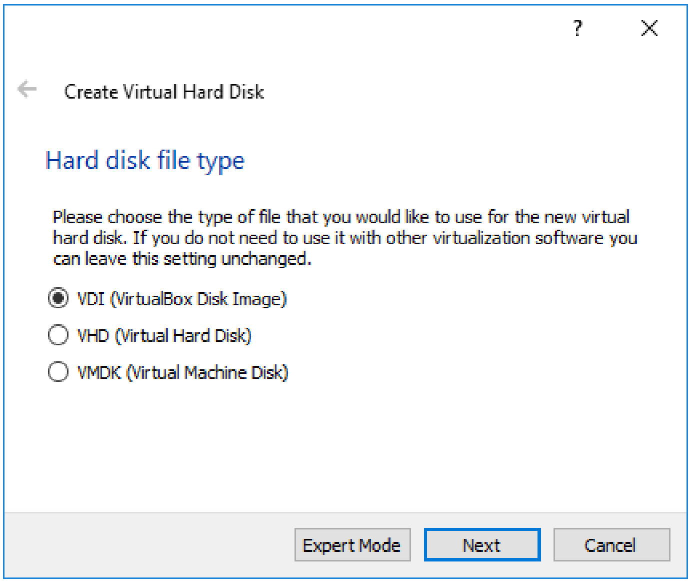
Name: IDE
Type: PIIX4
☑ Use Host I/O Cache

4. To add an additional hard disk, select "Controller: SATA" and click the icon.

   The "Hard Disk Selector" screen is displayed.

5. Click "Create".

   The "Create Virtual Hard Disk" screen is displayed.

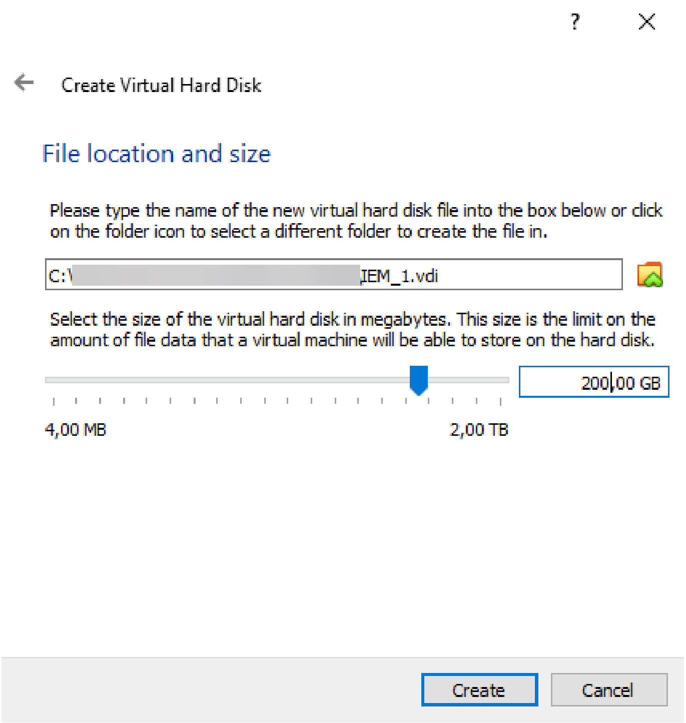


Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

6. Select the "VDI (VirtualBox Disk Image)" check box and click "Next".
7. Select the "Dynamically allocated" check box and click "Next".
8. Specify your needed disk size.



File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\[redacted]IEM_1.vdi

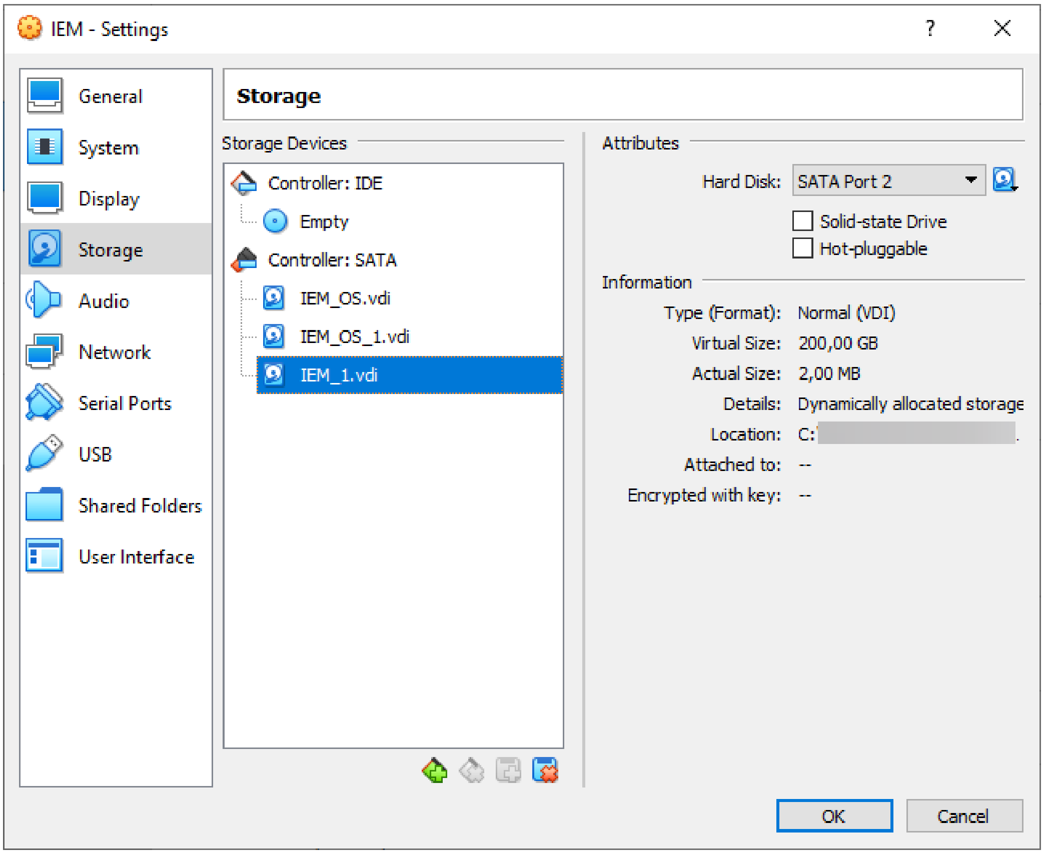
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

200,00 GB

9. Click "Create".

10. Click "Choose".

    The hard disk is added to the hardware list under "Controller: SATA".



Storage

Storage Devices

- Controller: IDE
  - Empty
- Controller: SATA
  - IEM_OS.vdi
  - IEM_OS_1.vdi
  - IEM_1.vdi

Attributes

Hard Disk: SATA Port 2

□ Solid-state Drive

□ Hot-pluggable

Information

Type (Format):	Normal (VDI)
Virtual Size:	200,00 GB
Actual Size:	2,00 MB
Details:	Dynamically allocated storage
Location:	C:[redacted]
Attached to:	--
Encrypted with key:	--

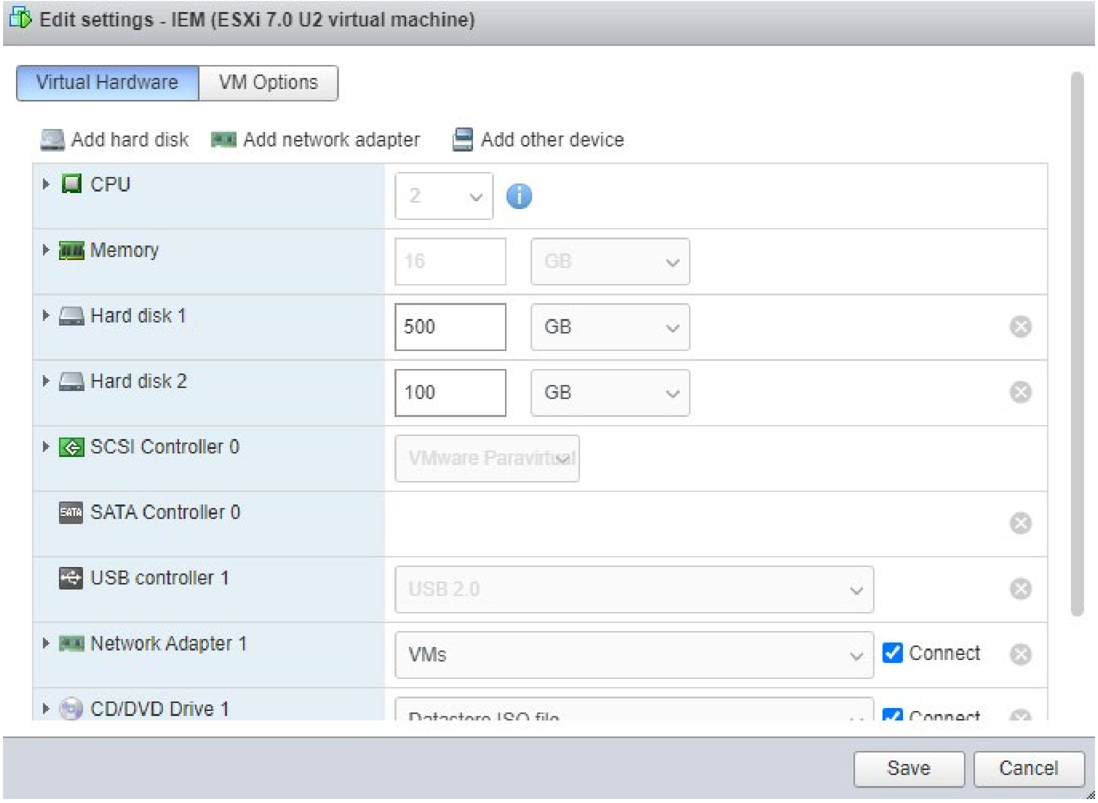
11. Close the VM settings.

Adding additional hard disk - VMware ESXi

1. In the navigation on the left, click "Virtual Machines".
2. Select the VM on which the IEM-OS runs.

3. Right click and select the "Edit settings" menu command.

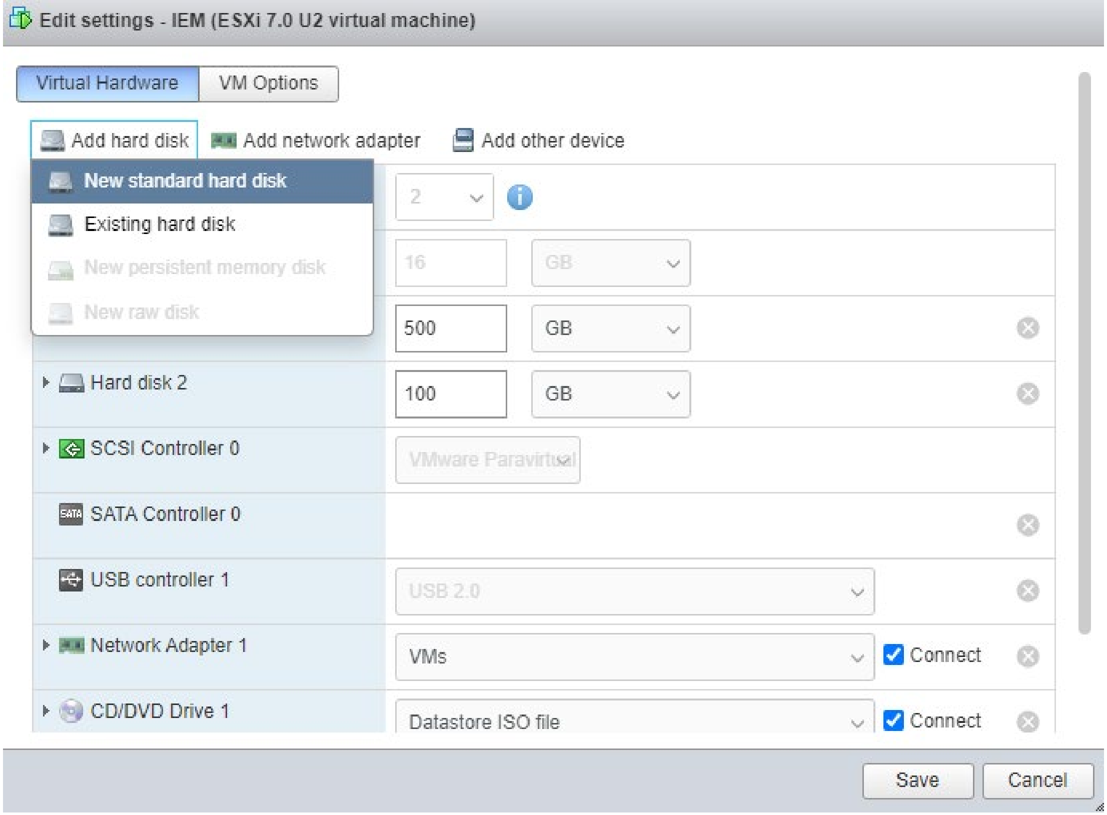
   The VM settings are displayed.



Edit settings - IEM (ESXi 7.0 U2 virtual machine)

CPU	2			
Memory	16	GB		
Hard disk 1	500	GB		
Hard disk 2	100	GB		
SCSI Controller 0	VMware Paravirtual			
SATA Controller 0				
USB controller 1	USB 2.0			
Network Adapter 1	VMs		☑ Connect	
CD/DVD Drive 1	Datastore ISO file		☑ Connect	

4. Click "Add hard disk" and select "New standard hard disk".

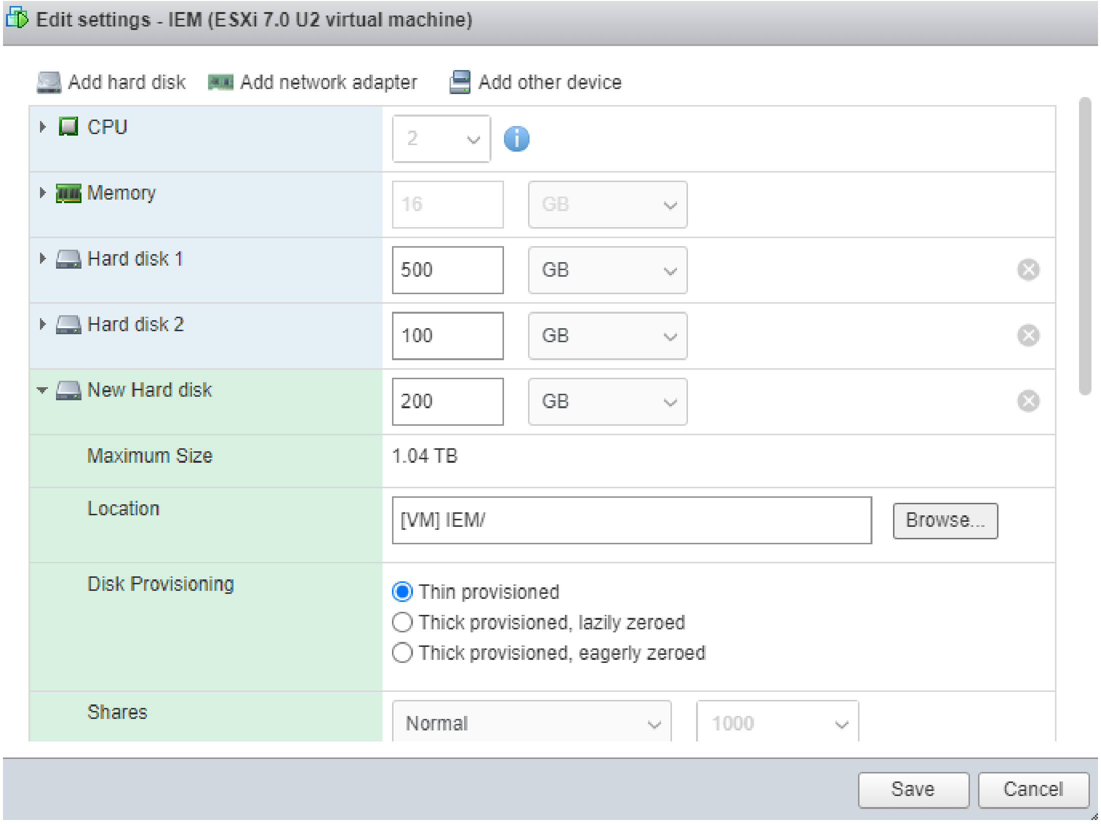


2
16 GB
500 GB
Hard disk 2: 100 GB
SCSI Controller 0: VMware Paravirtual
SATA Controller 0
USB controller 1: USB 2.0
Network Adapter 1: VMs ☑ Connect
CD/DVD Drive 1: Datastore ISO file ☑ Connect

A new virtual hard disk is created.

5. Specify your needed disk size.

6. Expand the new hard disk and select "Thin provisioned" under "Disk Provisioning".



Edit settings - IEM (ESXi 7.0 U2 virtual machine)

CPU	2	
Memory	16	GB
Hard disk 1	500	GB
Hard disk 2	100	GB
New Hard disk	200	GB
Maximum Size	1.04 TB	
Location	[VM] IEM/	
Disk Provisioning	● Thin provisioned ○ Thick provisioned, lazily zeroed ○ Thick provisioned, eagerly zeroed	
Shares	Normal	1000

Thin provisioned means that the storage on the physical hard disk is only allocated when needed. Otherwise, the disk's storage size remains small.

7. Click "Save".

The new virtual hard disk has been created and is added to the hardware list.

Adding additional storage to the IEM

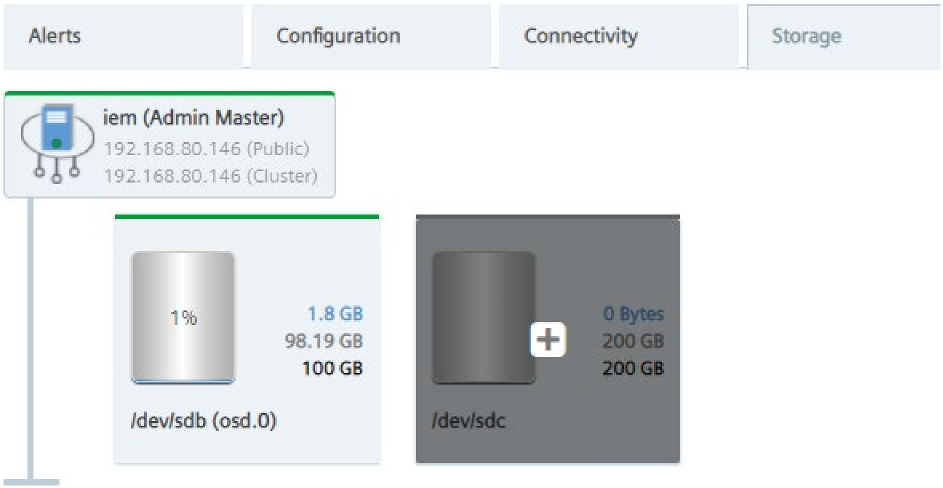
1. Open the Maintenance UI of the IEM.
2. Navigate to "Settings > System".
3. Click the "Cluster Reboot" tile.
4. Reboot the cluster by clicking "Reboot".

   The VM on which the IEM-OS runs is getting rebooted.
5. Wait until the reboot is finished.

   When the reboot is finished, you can extend your existing storage.

6. Navigate to "Settings > Storage".

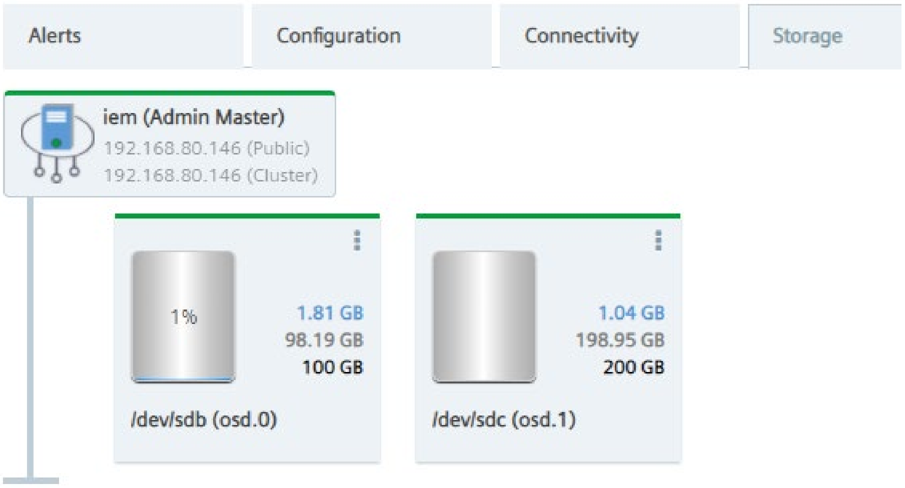
   The new available virtual hard disk is displayed.



7. To add the newly created storage to your IEM, click the ➕ icon.
8. Confirm by clicking "Add".

   The created disk space is being added to the IEM.
9. When the disk space has been added successfully to the IEM, click "Ok".

   The additional storage is now available for your usage.



3.8.6 System

In the "System" tab, you perform administrative and maintenance tasks of your cluster or node.

The following are the administrative and maintenance tasks of your cluster:

Parameter	Description
Cluster Shutdown	- Shutdown the cluster - The shutdown will be performed after the time has passed that you can configure under the "Timeout Settings" section in the "Configuration (Page 36)" subsection.
Cluster Reboot	- Reboot the cluster - The reboot will be performed after the time has passed that you can configure under the "Timeout Settings" section in the "Configuration (Page 36)" subsection.
Cluster Delete	Delete all cluster information and settings
Download Cluster Logs	Download logs of the cluster in a *.tar.gz file
Update Industrial Edge Management	Update the Industrial Edge Management OS
NTP Server	Adding and editing NTP servers
Restart NTP Services	Restart NTP services

Note

Updating the Industrial Edge Management OS

You find the procedure and additional information on how to update the Industrial Edge Management OS, and other components, in the "Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/10979534)" manual.

The following are the administrative and maintenance tasks of your node:

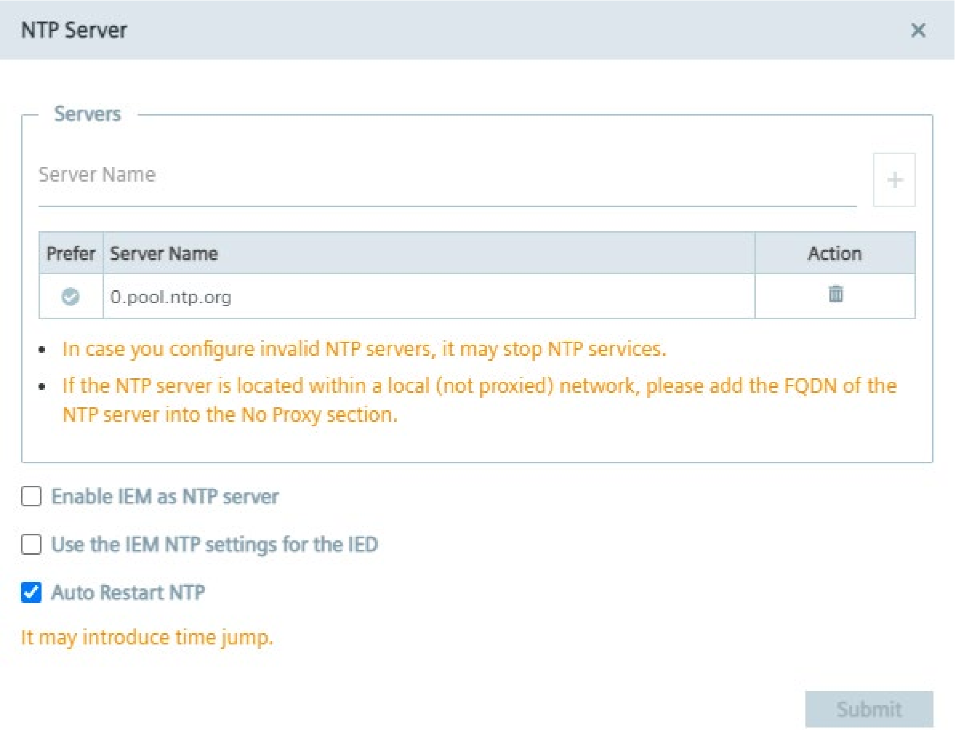
Parameter	Description
Node Shutdown	Shutdown the node
Node Reboot	Reboot the node
Download Node Logs	Download the logs of the node in a *.tar.gz file
Update Industrial Edge Management	Update the Industrial Edge Management OS
NTP Server	Adding and editing NTP servers
Restart NTP Services	Restart NTP services

3.8.6.1 Adding and editing NTP servers

Adding an NTP server

1. Click the "NTP Server" tile.

   The "NTP Server" screen is displayed.



NTP Server ×

Servers

Server Name +

Prefer	Server Name	Action
✓	0.pool.ntp.org	🗑

- In case you configure invalid NTP servers, it may stop NTP services.
- If the NTP server is located within a local (not proxied) network, please add the FQDN of the NTP server into the No Proxy section.

□ Enable IEM as NTP server

□ Use the IEM NTP settings for the IED

☑ Auto Restart NTP

It may introduce time jump.

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

2. In the "Server Name" input field, enter the NTP server.
3. To add the NTP server, click the plus icon.

   The NTP server is added to the server list.

4. By clicking the ✓ icon, you select the NTP server as preferred NTP server which signals the NTP service to always select this NTP server as synchronization source, in case the server is available.

   Preferred NTP servers are marked with ✓.

5. By selecting the "Enable IEM as NTP server" check box, the NTP services in the IEM serve as an NTP server for other NTP clients, for example Edge Devices.

   This option removes the dependency that an NTP server must be configured in the local automation network and serves Edge Devices which cannot access any global or local servers within the local network.

6. By selecting the "Use the IEM NTP settings for the IED" check box, Edge Devices that are getting connected to this IEM use the same preferred NTP server for time synchronization.

Note

Selecting NTP server

You can just select either the "Enable IEM as NTP server" or the "Use the IEM NTP settings for the IED" at the same time.

7. By selecting the "Auto Restart NTP" check box, the automatic restart of NTP services is enabled.

   By default, the "Auto Restart NTP" check box is enabled. If, due to any kind of reason, NTP services in the IEM have stopped and the "Auto Restart NTP" check box is enabled, the NTP monitoring service will automatically restart the NTP services.

Note

Data loss due to leap in time

If NTP services in the IEM have stopped and the automatic restart of NTP services is enabled via this option, a leap in time might occur after automatically restarting NTP services. Be aware that time series based applications might be affected by this leap in time resulting in losing data. If you do not want this risk of losing data, disable the "Auto Restart NTP" check box.

8. Click "Submit".

Note

Editing NTP servers

When you have changed the settings of an NTP server, click "Submit" to save the changes.

3.8.7 Members

The "Members" tab lists all members registered in the IEM-OS and all users requesting access to the IEM-OS.

Approving users

The admin of the IEM-OS can approve users requesting access to the IEM-OS.

To approve users requesting access to the IEM-OS, click the ⋮ icon of the user under the "Action" column and click "Approve". Confirm by clicking "Approve".

Afterwards, the users can sign into the IEM-OS.

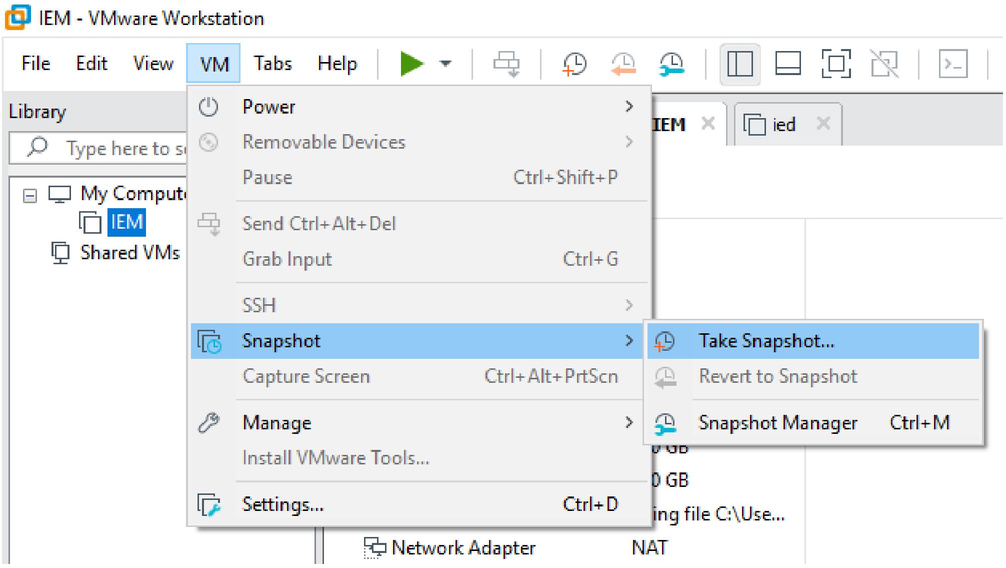
3.9 Backup and restore

3.9.1 Creating a backup of the IEM-OS

You create a backup of the IEM-OS by taking a snapshot of the VM. To avoid errors, take snapshots only when the VM is powered off.

Creating a backup via VMware Workstation

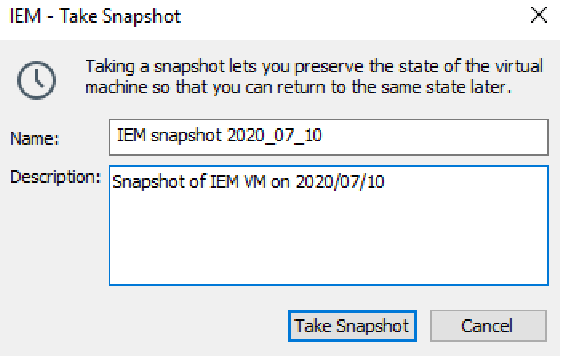
1. Open VMware Workstation.
2. Select the VM which runs the IEM-OS.
3. Click "VM" and click the "Snapshot > Take Snapshot" command.



The "Take Snapshot" screen is displayed.

4. In the "Name" input field, enter a unique snapshot name.

5. In the "Description" input field, enter a snapshot description.



IEM - Take Snapshot

Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.

Name: IEM snapshot 2020_07_10

Description: Snapshot of IEM VM on 2020/07/10

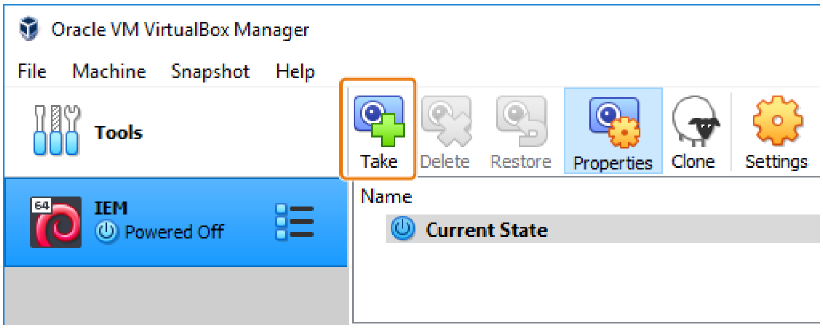
6. Click "Take Snapshot".

   The snapshot is saved.

Creating a backup via Oracle VirtualBox

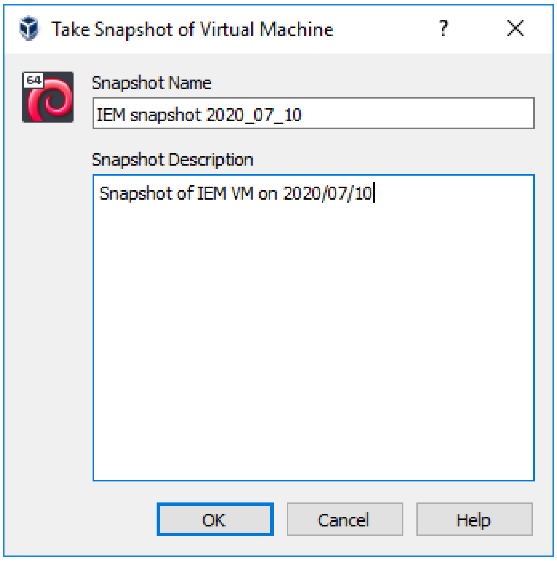
1. Open Oracle VirtualBox.
2. Select the VM which runs the IEM-OS.
3. Click the ☰ icon and click "Snapshots".

   A list of all snapshots is displayed.
4. Select "Current State" from the list and click "Take".



   The "Take Snapshot" screen is displayed.
5. In the "Snapshot Name" input field, enter a unique snapshot name.

6. In the "Snapshot Description" input field, enter a snapshot description.



Snapshot Name: IEM snapshot 2020_07_10

Snapshot Description: Snapshot of IEM VM on 2020/07/10

7. Click "OK".

   The snapshot is saved.

3.9.2 Restoring the IEM-OS from a backup

You restore the IEM-OS from a previously saved backup by restoring a snapshot of the VM.

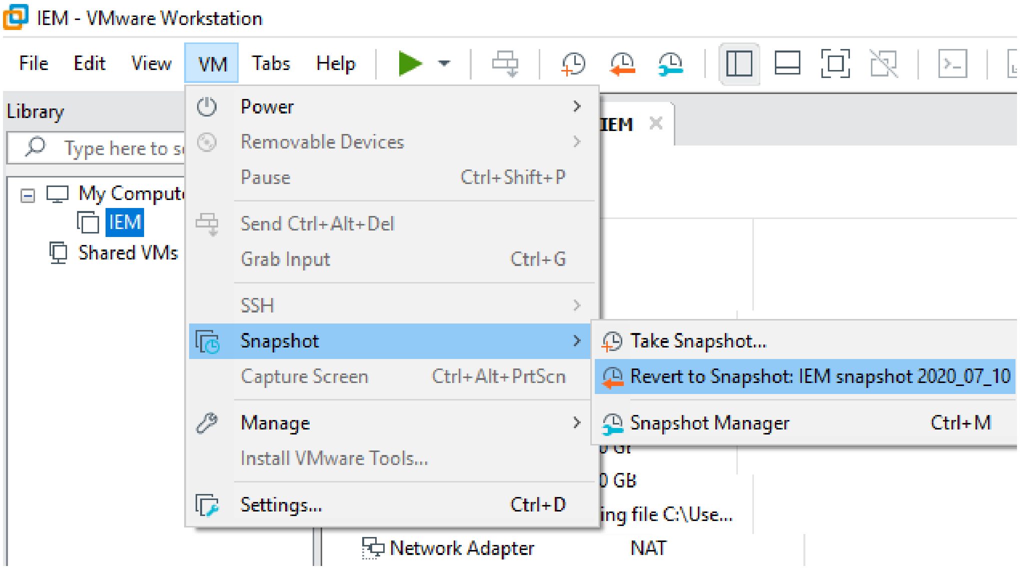
Requirement

You have taken a snapshot of the VM.

Restoring from a backup via VMware Workstation

1. Open VMware workstation.
2. Select the VM which runs the IEM-OS.

3. Click "VM" and click the "Snapshot > Revert to Snapshot" command to restore the latest taken snapshot or select a specific snapshot.



The confirmation screen is displayed.

4. To restore the selected snapshot, click "Yes".

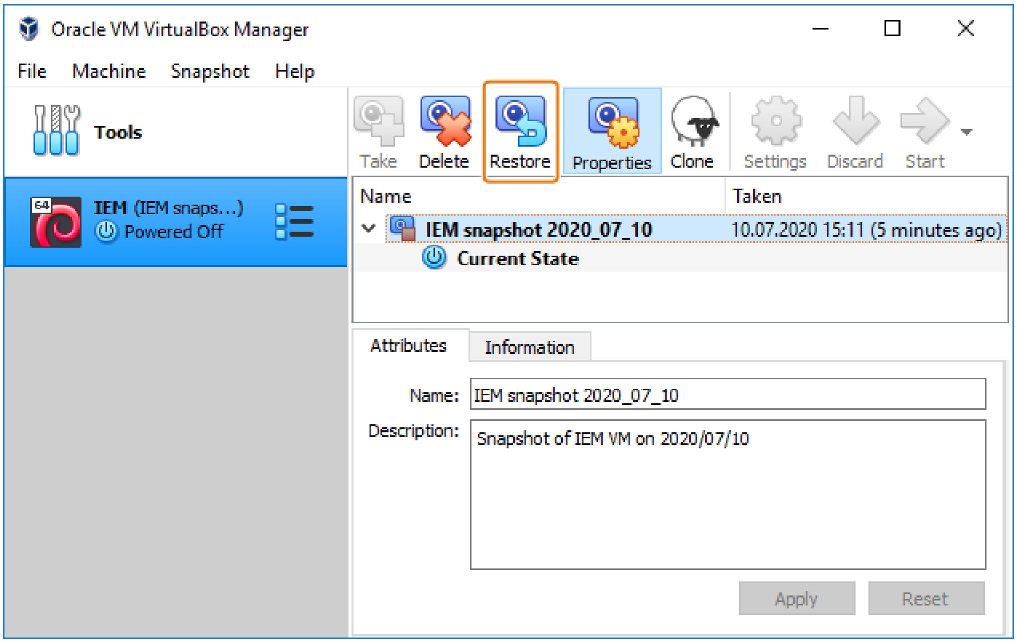
The VM is restored.

Restoring from a backup via Oracle VirtualBox

1. Open Oracle VirtualBox.
2. Select the VM which runs the IEM-OS.
3. Click the ☰ icon and click "Snapshots".

A list of all snapshots is displayed.

4. Click on the snapshot which you want to restore.
5. Click "Restore".



Name	Taken
IEM snapshot 2020_07_10	10.07.2020 15:11 (5 minutes ago)
Current State	

Name: IEM snapshot 2020_07_10

Description: Snapshot of IEM VM on 2020/07/10

The VM is restored.

3.10 Industrial Edge Management Services

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

Installing IEM Services manually

If you have already set up an IEM-OS and a new IEM Service is released, you must install the IEM Service manually. The IEM-OS checks every day at midnight (UTC time) if a new IEM Service is available. If a new IEM Service is released and available, an according notification will be displayed in the "Recent Events" screen in the Maintenance UI. You can then install the IEM Service manually from the catalog in the Maintenance UI as for example described for the manual installation of the IE State Service (Page 150).

Management UI 4

4.1 Sign up

Requirement

- An Industrial Edge Management (IEM) has been set up according to the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)" manual.
- The VM allocated to the IEM is running.

Note

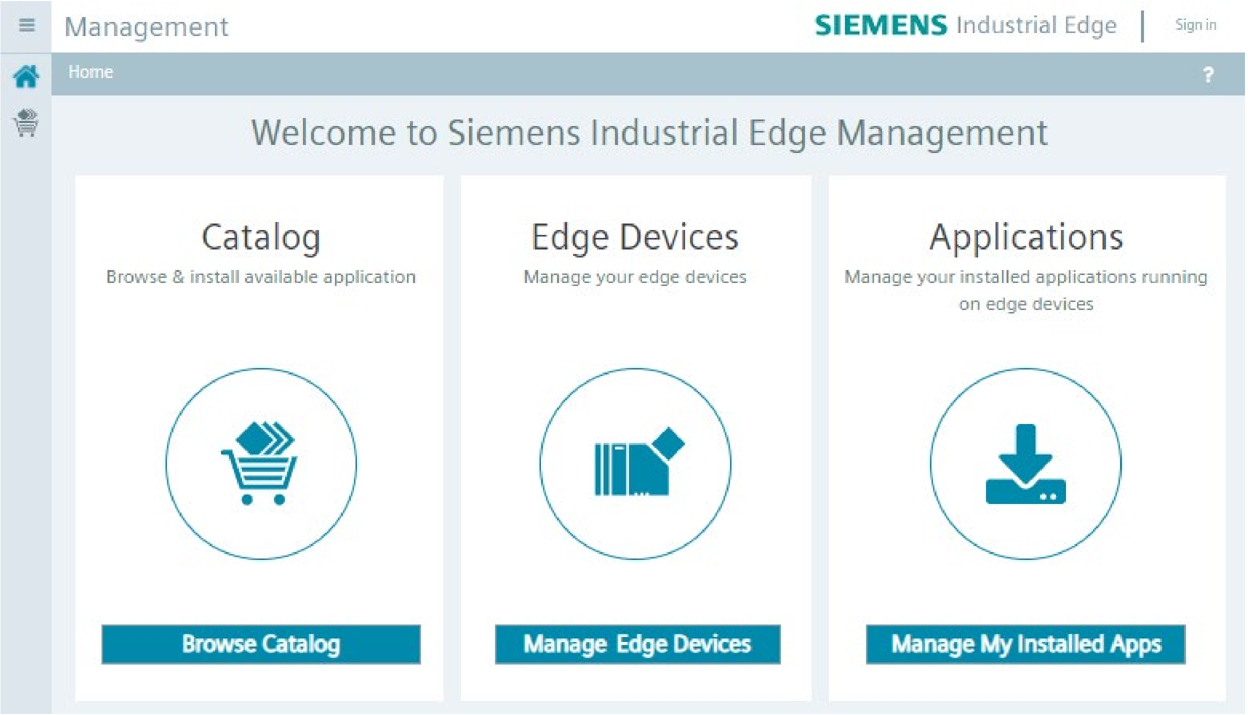
Reboot or shutdown of the VM

Only when the VM is running, the IEM is available. When you reboot or shutdown the VM in which the IEM is running, the IEM is unavailable.

Procedure

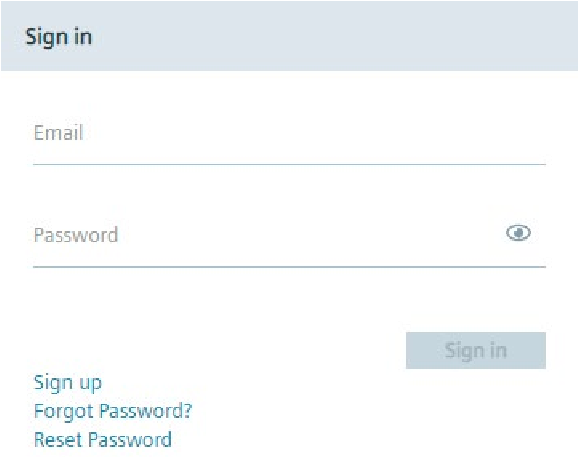
1. Open the IEM you want to sign up to by entering the IEM URL into an Internet browser.

   The login screen of the Management UI is displayed.



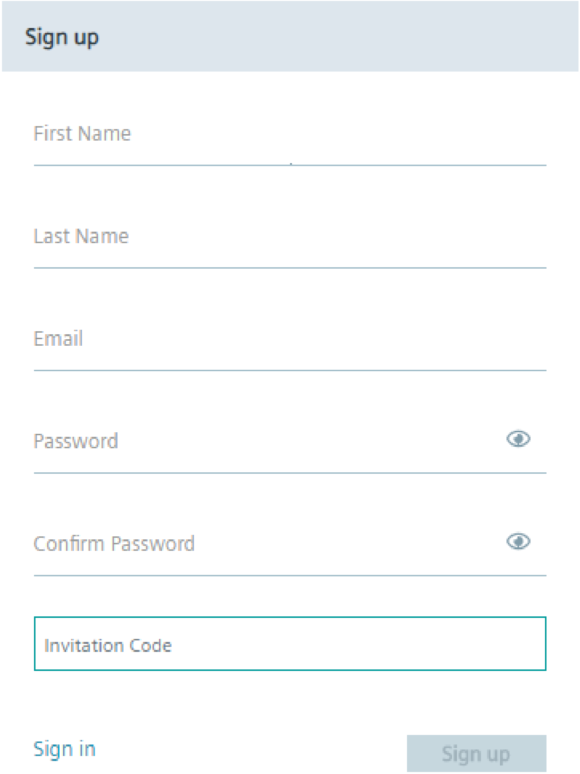
2. Register as a new user by clicking "Sign in".

   The "Sign in" screen is displayed.



3. Click "Sign up".

   The "Sign up" screen is displayed.



4. Enter the required information in the "Sign Up" screen.

   The password must meet the following criteria:

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

   The following characters are recognized as special characters: ! @ # $ % ^ & * . ( ) _ +
5. Click "Sign Up".

   Your account has been created and you will be redirected to the "Sign in" screen again. The admin of the IEM must now approve your user account request.
6. Contact the admin of the IEM for approval of your user account request.
7. Wait until the admin of the IEM has approved your user account request.

   Depending on whether the admin of the IEM has configured an email server or not in the IEM, the approval takes some time.

   After the admin has approved your user account, the admin will contact you. Afterwards, you are able to log into the IEM respectively the Management UI.

4.2 Log in and sign out

Requirement

- The admin of the IEM has approved your user account request.
- The VM allocated to the IEM is running.

Note

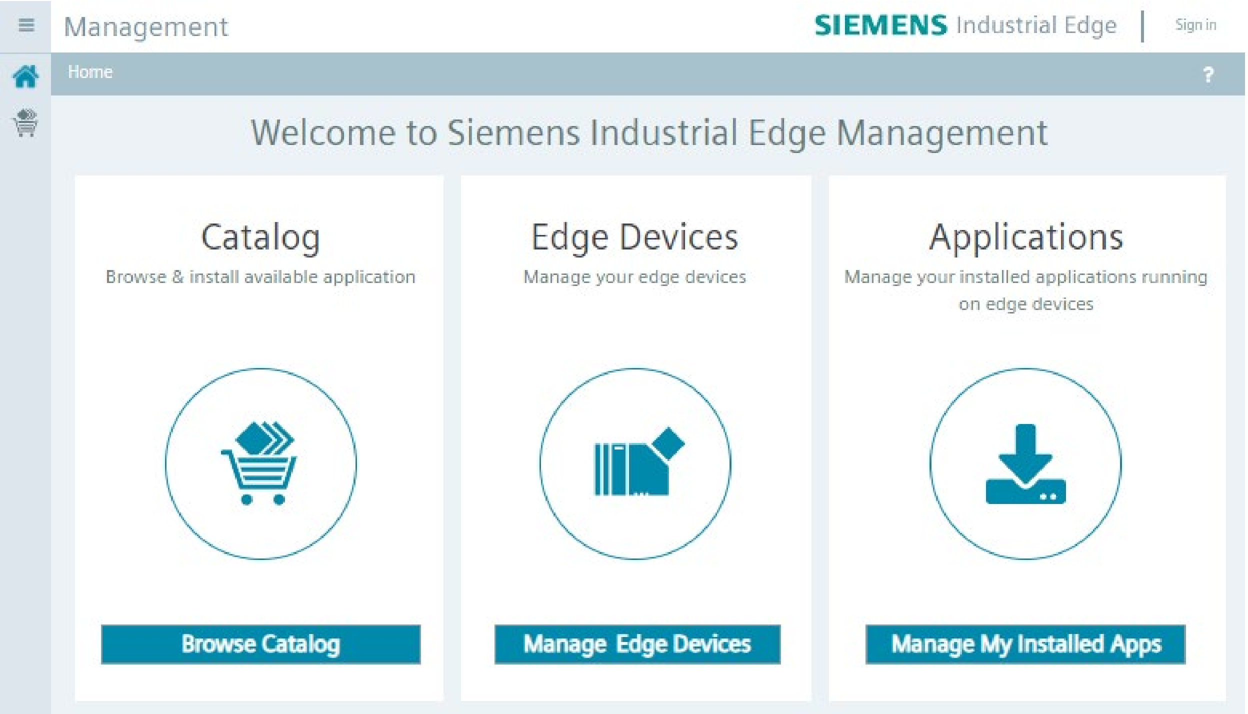
Reboot or shutdown of the VM

Only when the VM is running, the IEM is available. When you reboot or shutdown the VM in which the IEM is running, the IEM is unavailable.

Log in

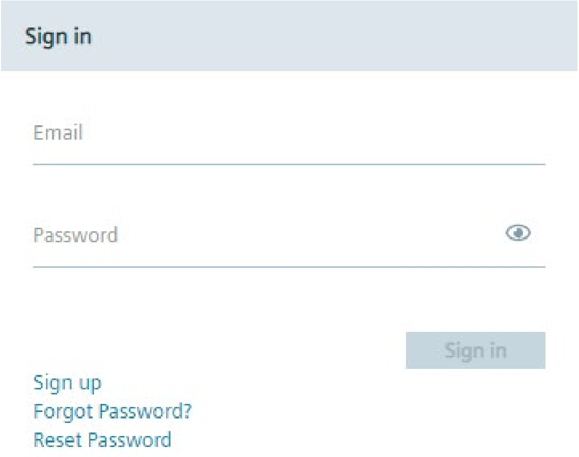
1. Open the IEM you want to log into by entering the IEM URL into an Internet browser.

   The login screen of the Management UI is displayed.



2. In the top-right corner, click "Sign in".

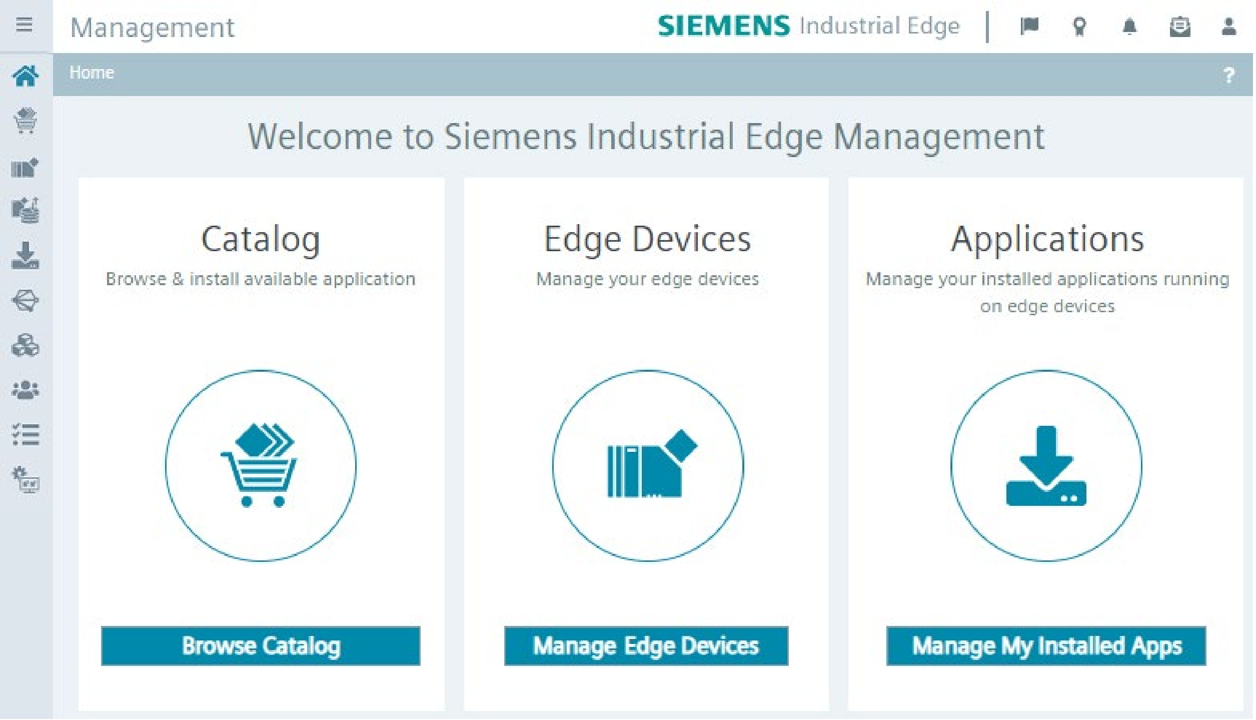
   The "Sign in" screen is displayed.



3. In the "Email" input field, enter your email address.

4. In the "Password" input field, enter your password.
5. Click "Sign in".

   The home page of the Management UI is displayed.



Welcome to Siemens Industrial Edge Management

Catalog
Browse & install available application

Edge Devices
Manage your edge devices

Applications
Manage your installed applications running on edge devices

Note

Failed login attempts

After 5 failed login attempts, logging into the Management UI is temporary locked. In that case, you must wait 15 minutes to be able to log in again.

Sign out

1. Click the user icon in the top-right corner.
2. Click "Sign out".

   You are signed out from the IEM.

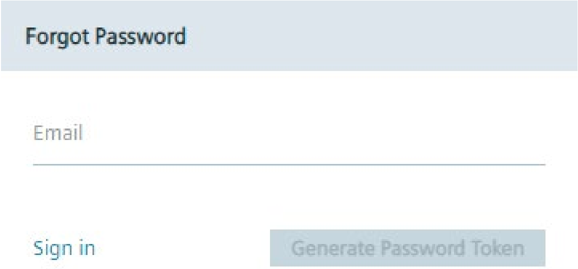
4.3 Reset password

If you have forgotten your password, you can set a new password through generating a temporarily password token.

Procedure

1. In the "Sign in" screen, click "Forgot Password".

   The "Forgot Password" screen is displayed.

   Forgot Password

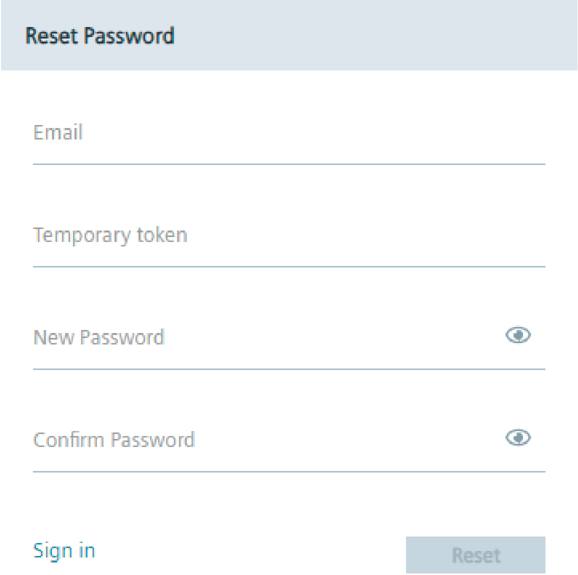
   Email

2. In the "Email" input field, enter your email address.
3. Click "Generate Password Token".

   A password token is generated which the admin can check under "Registered Users" in the Admin UI of the IEM.

   If the admin has configured an email server, you will automatically receive an email containing the password token. If the admin has not configured an email server, the admin must share the password token manually with you.

   The "Reset Password" screen will be opened.

   Reset Password

   Email

   Temporary token

   New Password

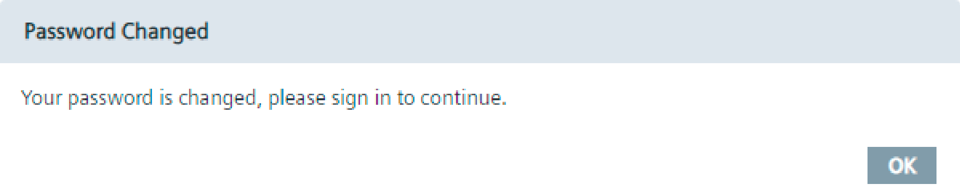
   Confirm Password

4. In case that an email server is not configured, contact the admin to receive the password token.

5. When you have received the password token, enter the following in the "Reset Password" screen:
   - Email: Your email address
   - Temporary token: Generated password token
   - New Password: New user password
   - Confirm Password: Confirm new user password

   The new password must meet again the password criteria.
6. Click "Reset".

   If the password token was valid, you successfully changed your password.



Password Changed

Your password is changed, please sign in to continue.

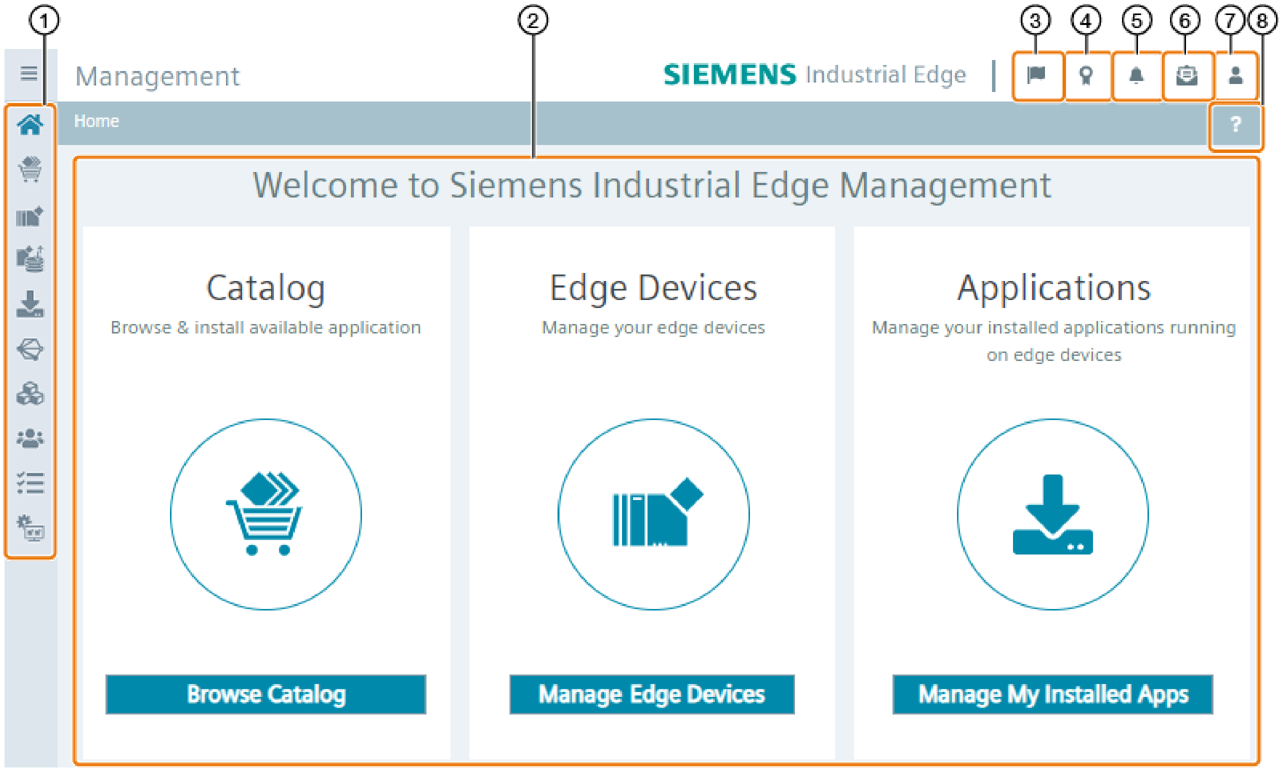
7. Click "Ok".

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

4.4 Home page

After you log in, the home page of the Management UI is displayed.

The following figure shows the home page:



Welcome to Siemens Industrial Edge Management

Catalog
Browse & install available application
Browse Catalog

Edge Devices
Manage your edge devices
Manage Edge Devices

Applications
Manage your installed applications running on edge devices
Manage My Installed Apps

① Navigation menu
② Main screen
③ Open job status of imported apps
④ Download IEM and IED root and intermediate certificates
⑤ Open "Alerts" screen
⑥ Accept invitations
⑦ Logged user
⑧ User interface explanation

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

To navigate within the Management UI, use the navigation menu on the left.

4.5 Certificate Management

4.5.1 Types of certificates

There are various certificates and certificate authorities (CA) generated and used in Industrial Edge:

- IEM internal root-CA and appropriate intermediate CA are generated during the setup
- The certificate chain of these CAs is distributed across Industrial Edge to establish the Chain of Trust for the entire system

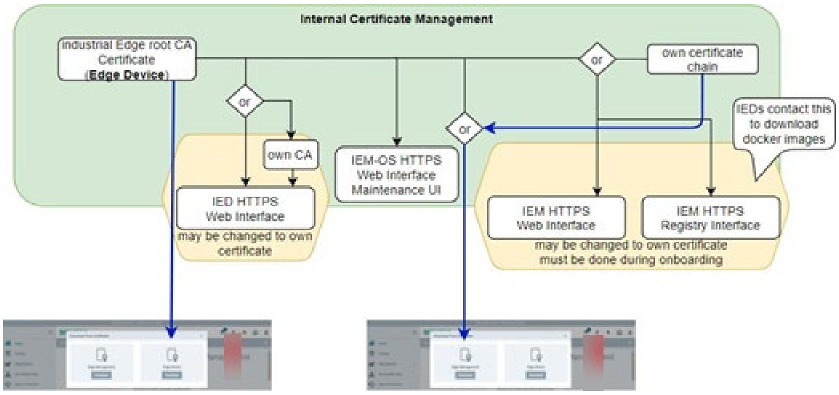
- The intermediate CA is used to create and sign default IED certificates to secure all IED public interfaces via TLS
- The intermediate CA is also used to create and sign default IEM certificates to secure following interfaces via TLS**:**
  - Container Registry Interface
  - Management UI
  - Maintenance UI
- Customers can replace following certificates:
  - IED certificates at any time
  - IEM certificates (Container Registry Interface and Management UI) during the IEM setup

Note

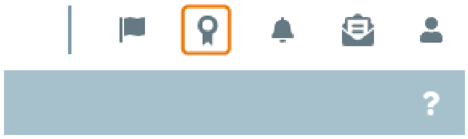
If a private CA is used to issue the certificates, you must include the full chain from the intermediate certificate of the CA to the final root certificate.

  - The certificate chain of the custom uploaded certificate which is stored as "Edge Management"
- IEDs connect to the IEM and to the Registry Interface and must trust the "Edge Management" root-CA (which is replaced if custom certificates are used)

The following figure shows an overview of the certificate management in Industrial Edge:


Internal Certificate Management
Industrial Edge root CA Certificate (Edge Device)
or
own CA
IED HTTPS Web Interface
may be changed to own certificate
IEM-OS HTTPS Web Interface Maintenance UI
or
or
own certificate chain
IEDs contact this to download docker images
IEM HTTPS Web Interface
IEM HTTPS Registry Interface
may be changed to own certificate must be done during onboarding

You can download the CA certificates by clicking the download certificates icon in the Management UI of the IEM:

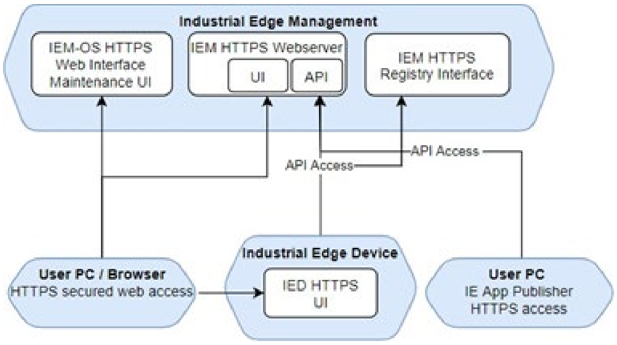


4.5.2 Communication relations

Several certificates and certificate chains are used to secure the communication between several interfaces:

- The IEM has 3 web interfaces (Maintenance UI, Management UI and Admin UI) accessible to users
- The IEM has an API interface in the webserver which is accessed by IEDs and the Industrial Edge App Publisher though API calls
- The IEM App has 2 public interfaces:
  - UI & API interface to manage apps and Edge Devices in the IEM
  - Registry Server interface to provide container images to IEDs
- The IED has 1 web interface for UI & API access

The following figure shows an overview on the encrypted interfaces and on accessing apps:



4.5.3 Secure connection to the IEM

To run the IEM in a secure environment, you must use the according certificates.
The IEM supports the following certificates:

- Certificates from the IEM
- Self-signed certificates
- Wildcard or SAN certificates

Certificates from the IEM and self-signed certificates

When you use certificates from the IEM itself or self-signed certificates and log into the IEM, the connection to the IEM is not secure. In that case, you must download the CA-chain and import it to the settings of the Internet browser. You find the procedure on importing the CA-chain to the settings of the Internet browser in the "Importing certificates to the Internet browser (Page 70)" subsection.

After you have imported the CA-chain to the Internet browser and refresh the IEM, the connection to the IEM is secure.

Wildcard or SAN certificates

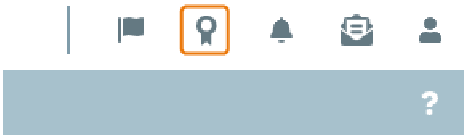
When you use wildcard certificates and log into the IEM, the connection to the IEM is secure.

4.5.3.1 Importing certificates to the Internet browser

The following procedure describes the import of certificates with the "Google Chrome" Internet browser. Proceed in the same manner for other Internet browsers.

Procedure

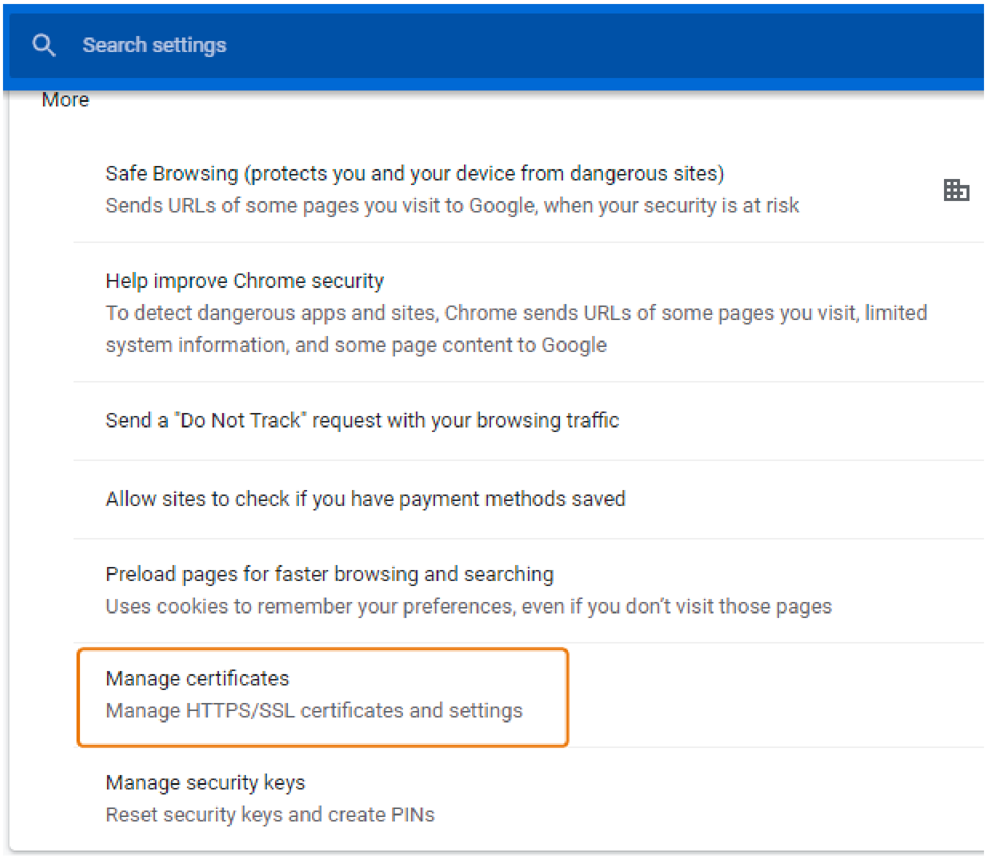
1. Open the IEM and sign in.
2. Click on the download certificate icon.



3. To download the certificates from the IEM, click "Download" inside the "Edge Management" tile.

   The CA-chain is being downloaded to the standard download folder of your Internet browser.
4. Open the settings of the Internet browser.

5. Open the "Manage certificates" settings.



Search settings

More

Safe Browsing (protects you and your device from dangerous sites)
Sends URLs of some pages you visit to Google, when your security is at risk

Help improve Chrome security
To detect dangerous apps and sites, Chrome sends URLs of some pages you visit, limited system information, and some page content to Google

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

Manage security keys
Reset security keys and create PINs

6. Click "Import".
7. Import the certificates by following the instructions on the screen and by selecting the downloaded CA-chain.

   When the import was successful, an according message is displayed.

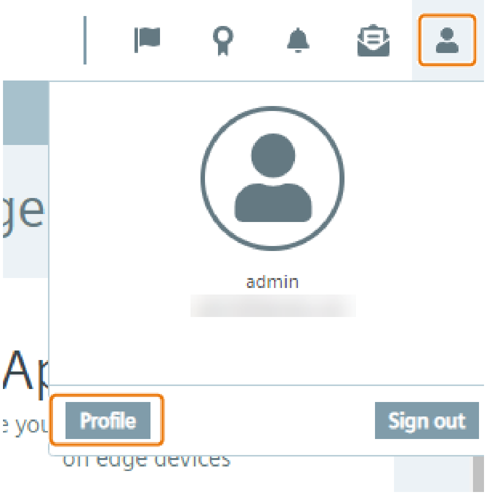
4.6 Alerts

By clicking the 🔔 icon, the "Alerts" screen is displayed. The "Alerts" screen displays the following alerts and notifications:

- Edge Devices which are offline for more than 1 hour
- Job status alerts, for example app installations and completed app updates
- Edge Device CPU, memory and storage resource utilization alerts
- Available app updates on Edge Devices notifications
- Edge Device certificate expiry and renewal alerts

4.7 User profile

To open your user profile, click the user icon in the top-right corner and click "Profile".



To close the user profile and return to the Mnagement UI, click "Home" underneath the header.

In the user profile, you have the possibility to edit the following settings:

- Profile: Editing your user profile
- Change Password: Changing your password
- Profile Picture: Setting a profile picture
- Security: Editing your multi-factor authentication

Editing your profile

In the "Profile" section, you edit the following profile parameters:

Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
Email	Email address of the user

After you have updated your profile parameters, click "Update" to save your changes.

Changing password

1. In the "Current Password" input field, enter your current password.
2. In the "New Password" input field, enter your new password.

   The password must meet the following criteria:

   – At least 8 characters

   – At least 1 upper case letter

   – At least 1 special character

   – At least 1 number

   The following characters are recognized as special characters: ! @ # $ % ^ & * . ( ) _ +
3. In the "Confirm Password" input field, confirm your new password.
4. To save your new password, click "Change".

Setting a profile picture

1. To upload a profile picture, click the ✎ icon.
2. Select a profile picture.
3. To save your profile picture, click "Save".

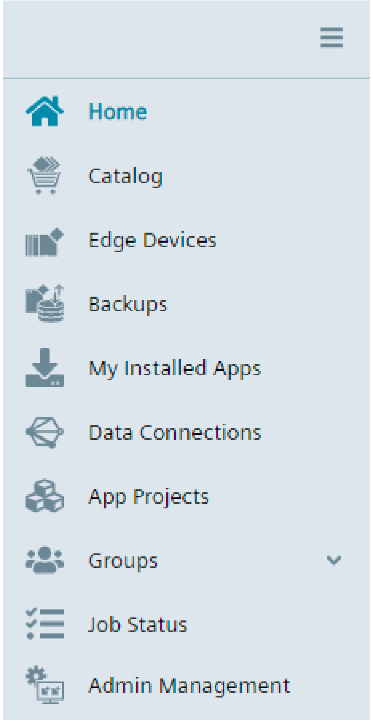
Security settings

In the "Security" section, you can set a multi-factor authentication through your entered email address.

A multi-factor authentication through your email address requires an email server which the admin of the IEM has configured in the Admin UI. The admin of the IEM configures an email server in the "Cloud Servers > Email Servers" section in the Admin UI.

4.8 Navigation

The following figure shows the navigation menu:



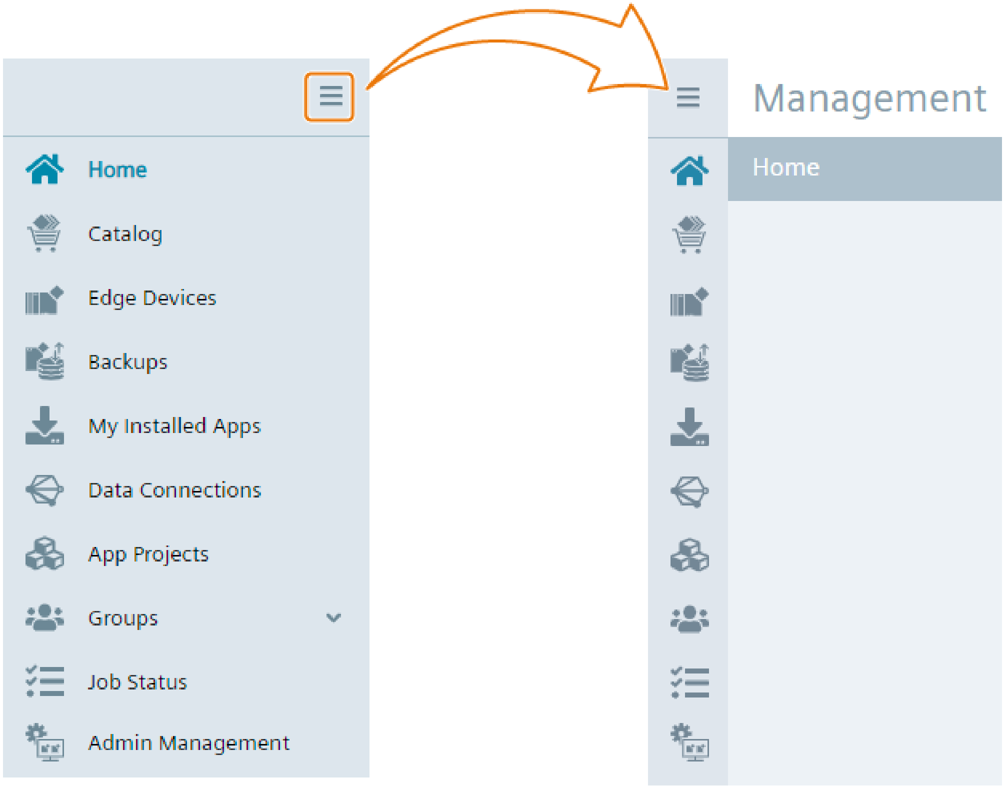
The following modules are available:

Module	Description
🏠	Home Navigate to the home page
🛒	Catalog Install available apps from the catalog
	Edge Devices Connect Edge Devices to the Industrial Edge Management
	Backups Restore or delete IED states
⬇	My Installed Apps Overview and management of all installed apps in the IEM
	Data Connections Launching apps configured by a configurator

Module	Description
	App Projects Create own projects for private coherent apps, and join app groups to contribute to shared apps
	Groups • My User Groups: Create groups and share private apps for group members • My Admin Groups: Create groups and share Edge Devices for group members
	Job Status Display executed Edge App and Edge Device jobs
	Admin Management Open the Admin UI (only available for users with admin permissions)

Hiding and displaying the navigation menu

You hide and display the navigation menu by clicking the icon in the navigation menu:



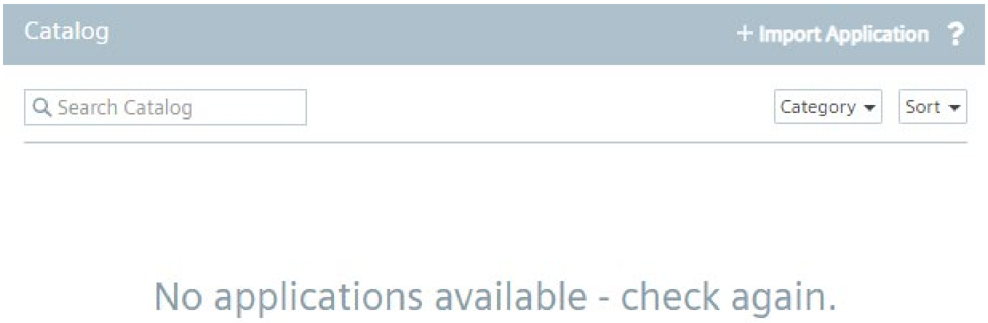
Catalog 5

5.1 Overview

The catalog provides all Edge Apps that you have manually imported or that you have copied from the Industrial Edge Hub to your IEM. From the catalog, you install these Edge Apps onto your Edge Devices.

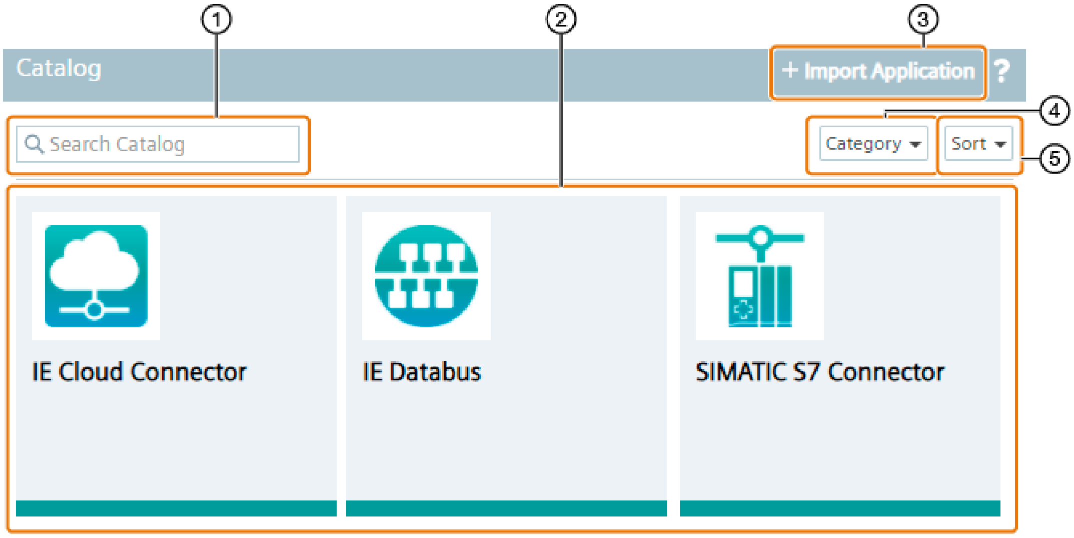
Catalog

If there are no apps imported or copied yet, the "Catalog" screen is displayed as follows:



No applications available - check again.

Once you have imported or copied an app, the "Catalog" screen is displayed as follows for example:



① Search the catalog for a keyword and press <Enter>

② Available Edge Apps

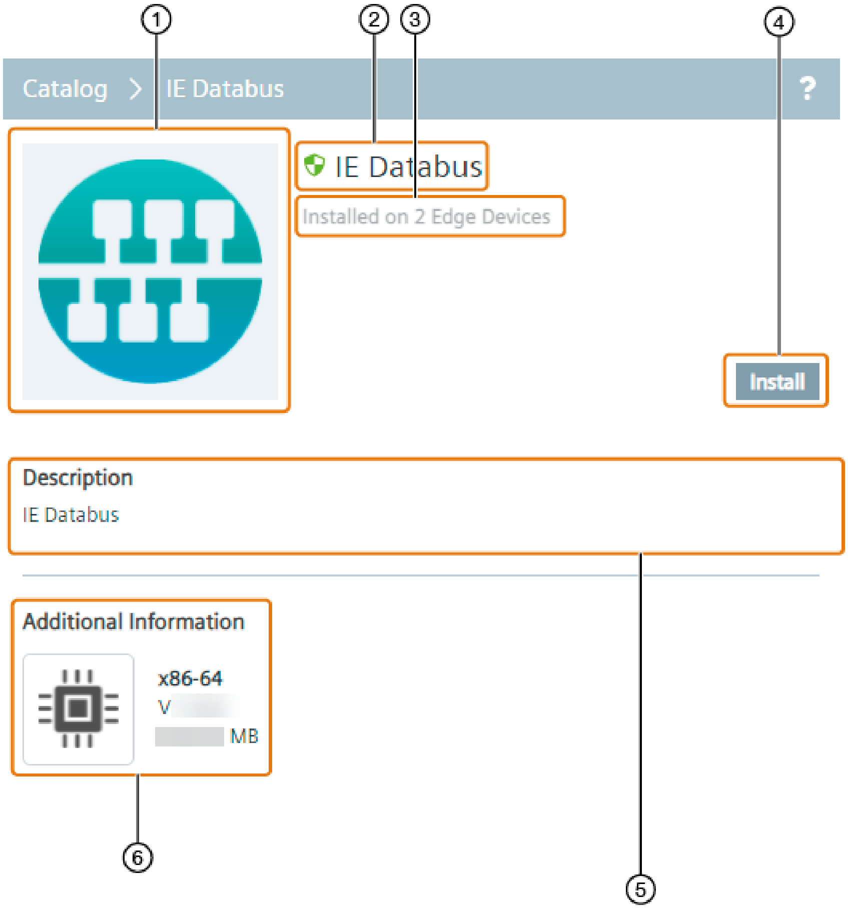
③ Import an Edge App to the catalog

④ Display only a specific category

⑤ Sort the available Edge Apps by the intended sorting order

App details

To open app details, click the tile of the app. The following figure shows an example of app details:



① Edge App icon

② Name of the Edge App

③ Number of Edge Devices on which the app is already installed

④ Install the app onto your Edge Devices

⑤ Description of the Edge App

⑥ Additional Information

Following information are provided:

- Architecture of the Edge App
- Version of the Edge App
- Size of the Edge App

5.2 Importing Edge Apps

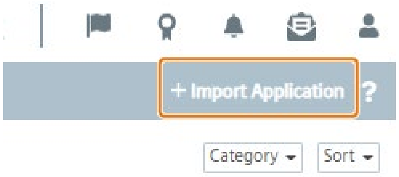
You have the possibility to import an Edge App in the "*.app" file format.

Requirement

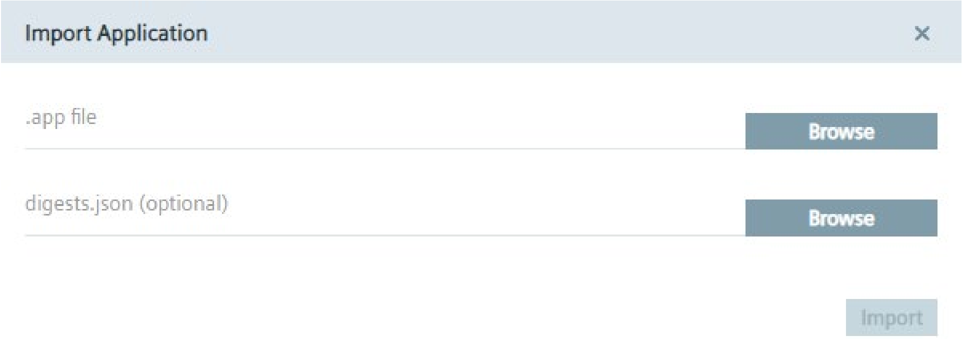
The app is available in the "*.app" file format.

Procedure

1. Click "Import Application".



The "Import Application" screen is displayed.

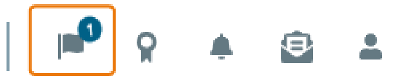


2. Next to the ".app file" text field, click "Browse" and select the Edge App in the "*.app" file format.
3. Optionally, you can verify the app by clicking "Browse" next to the "digests.json" text field and selecting the digest.json file of the specific app.

   You get the digest.json file from the app provider.

   The digest.json file will be compared to the same file that is included in the "*.app" file. This step is useful for checking the app integrity for unsigned apps.
4. Click "Import".

   The Edge App is being imported.
5. Check the status of the import by clicking the jobs icon.



When the import is completed, the Edge App is available in the catalog.

5.3 Installing an app from the catalog

The following procedure describes the installation of the "IE Databus" System App as an example.

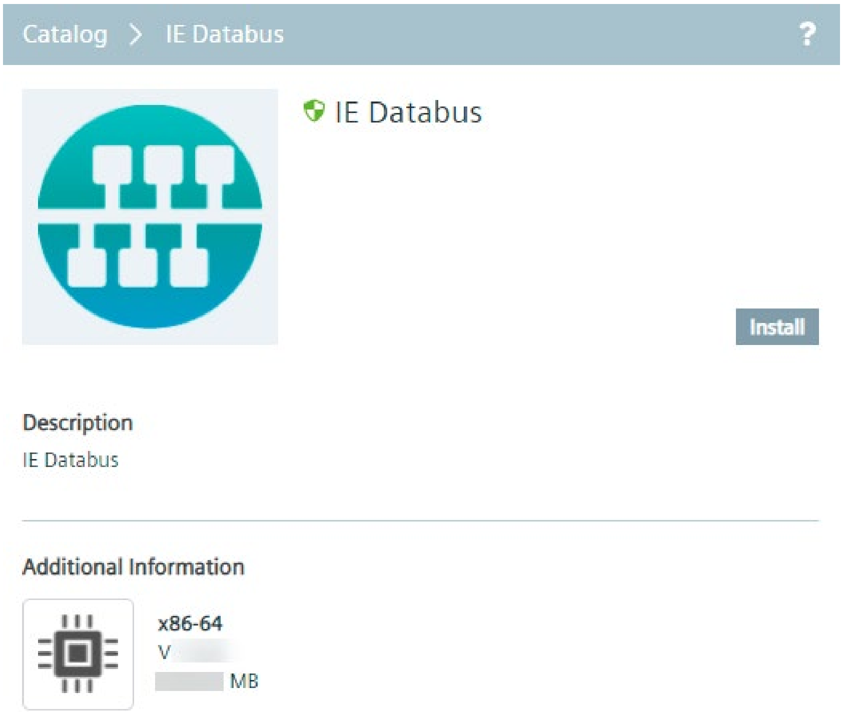
Requirement

- Minimum 1 Edge Device is onboarded to the IEM.
- The app is available in the catalog.

Procedure

1. In the catalog, click the tile of the app, in this example the "IE Databus" System App.

   The app details are displayed.



Description

IE Databus

Additional Information

x86-64
V [redacted]
[redacted] MB

Note

Verified Edge Apps

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

2. Click "Install".

   The "Install App" screen is displayed.

3. Depending on the app, you may have to select a configuration.

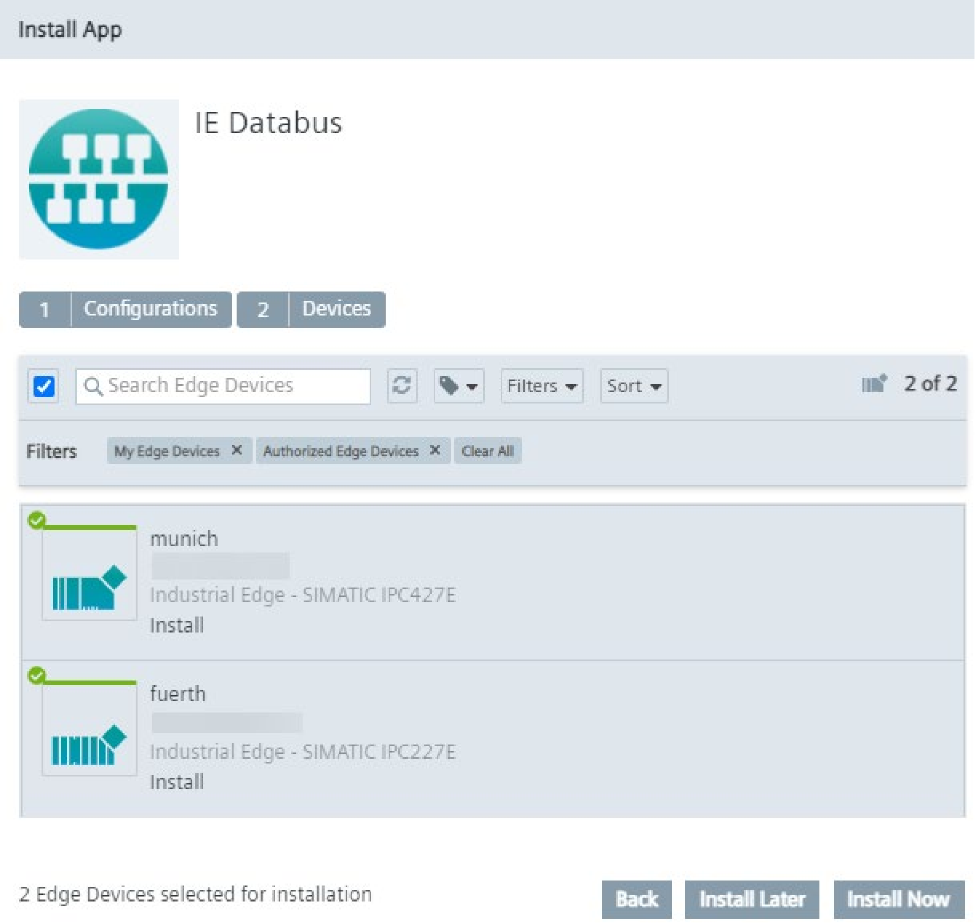
   To identify the needed configuration and steps, check the installation instructions in the documentation of the specific app.

   Note

   Installing System App

   When you install the "IE Databus" System App, do not select any configuration.

4. Click "Next".
5. Select the Edge Devices on which you want to install the app to.



Install App

IE Databus

1 Configurations | 2 Devices

☑ Search Edge Devices | Filters | Sort | 2 of 2

Filters: My Edge Devices ✕ | Authorized Edge Devices ✕ | Clear All

munich
[redacted]
Industrial Edge - SIMATIC IPC427E
Install

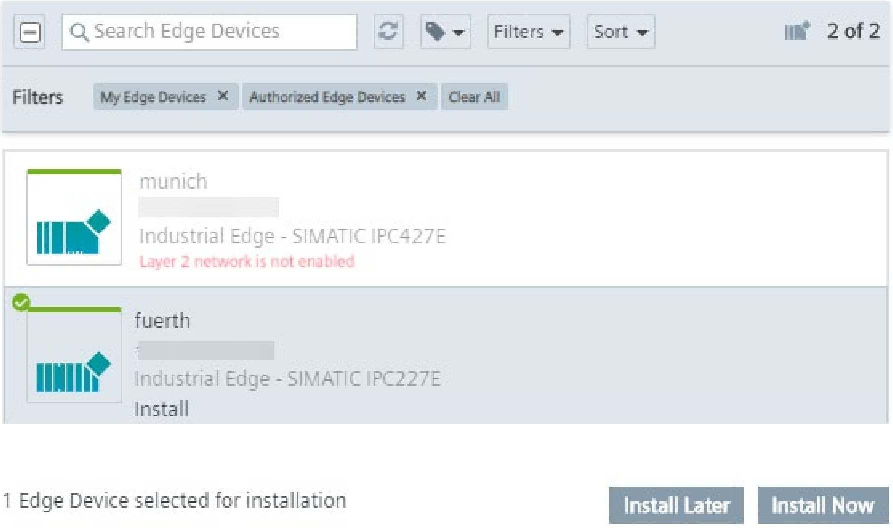
fuerth
[redacted]
Industrial Edge - SIMATIC IPC227E
Install

2 Edge Devices selected for installation

Back | Install Later | Install Now

You can select several Edge Devices to install the app to.

You cannot install apps that require a Layer 2 (L2) network access on Edge Devices that do not support such a L2 network access, as for example displayed below.



munich
[redacted]
Industrial Edge - SIMATIC IPC427E
Layer 2 network is not enabled

fuerth
[redacted]
Industrial Edge - SIMATIC IPC227E
Install

1 Edge Device selected for installation

If you need to install apps that require L2 network access, you can set up a Layer 2 network access on this Edge Device as described in the "Edge Device UI > Settings > Connectivity > Network and Layer 2 network access settings" subsection in the "Industrial Edge Runtime - Operation (https://support.industry.siemens.com/cs/us/en/view/109783785)" manual.

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

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

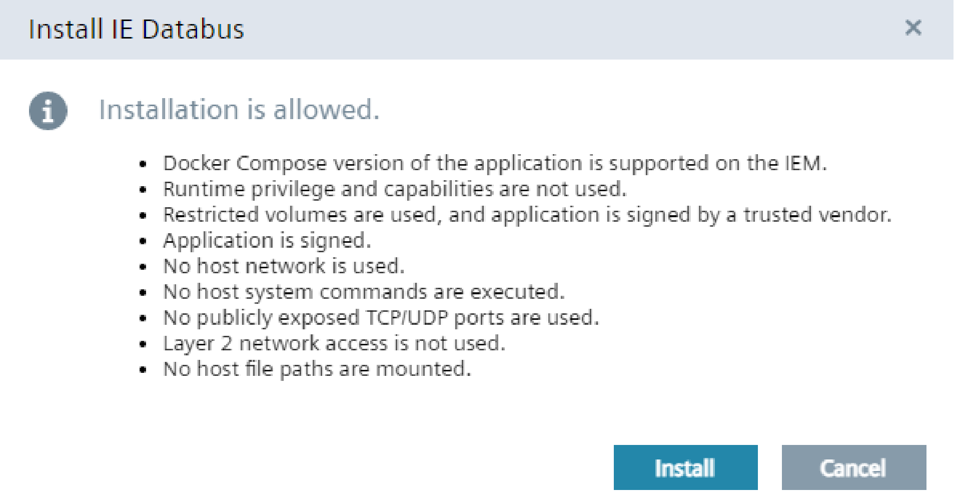
   Note

   Installation date and time

   When you select "Install Later", a calendar and the local system time is displayed for selecting the installation date and time.

   The "Install" screen is displayed which shows capabilities and services which will be used by the app. Depending on the app, the installation is allowed, allowed with warnings or blocked.

   – If the installation is allowed without any warnings, the screen is displayed as follows for example:



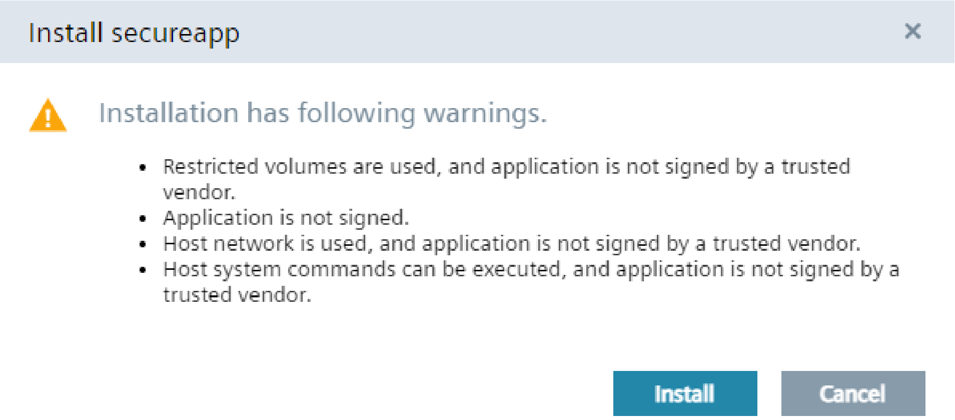
Install IE Databus

Installation is allowed.

- Docker Compose version of the application is supported on the IEM.
- Runtime privilege and capabilities are not used.
- Restricted volumes are used, and application is signed by a trusted vendor.
- Application is signed.
- No host network is used.
- No host system commands are executed.
- No publicly exposed TCP/UDP ports are used.
- Layer 2 network access is not used.
- No host file paths are mounted.

   By clicking "Install", the app will be installed.

   – If the installation is allowed but indicates several warnings, the screen is displayed as follows for example:



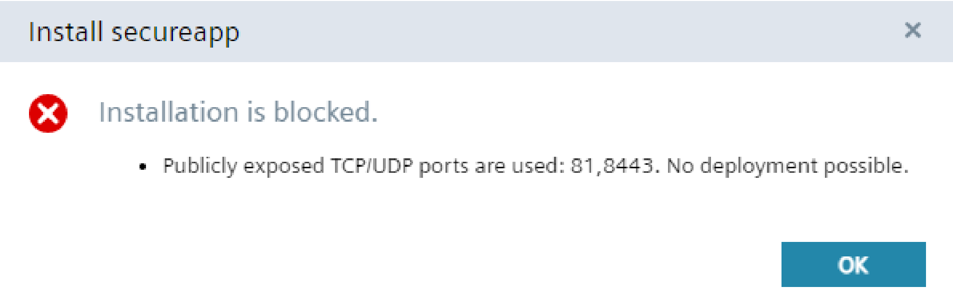
Install secureapp

Installation has following warnings.

- Restricted volumes are used, and application is not signed by a trusted vendor.
- Application is not signed.
- Host network is used, and application is not signed by a trusted vendor.
- Host system commands can be executed, and application is not signed by a trusted vendor.

In this case, check the warnings. If the warnings are neglectable and you still want to install the app, click "Install". Otherwise, click "Cancel".

– If the installation is blocked due to security risks for example, the screen is displayed as follows:



Install secureapp

Installation is blocked.

- Publicly exposed TCP/UDP ports are used: 81,8443. No deployment possible.

In this case, you cannot install the app.

7. To install the app, click "Install".

   The app is being installed. You can check the installation status in the "Job Status" menu item.

Note

Installation time of apps

The installation time of apps vary depending on (but not limited) network conditions, hardware specifications of each Edge Device or size of the apps.

See also

Privileged and network mode (Page 204)

Edge Devices

6

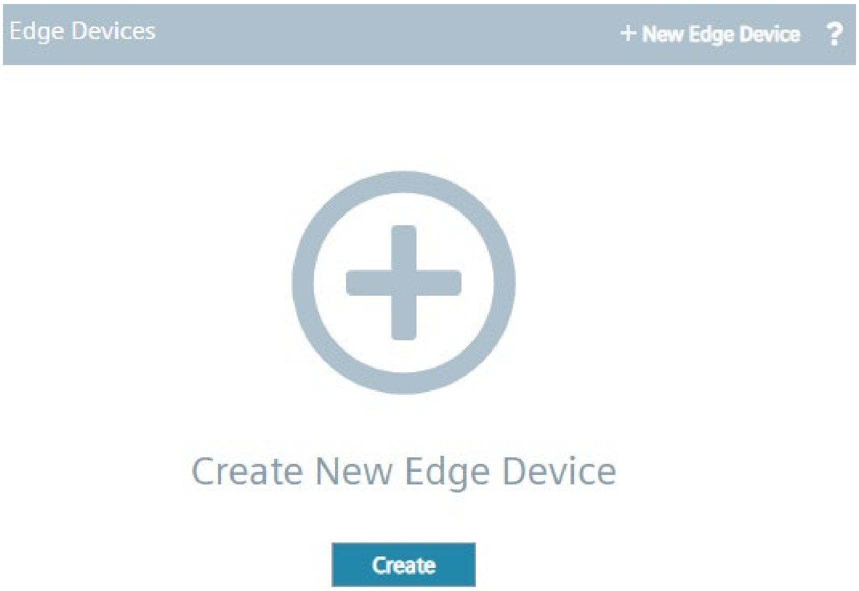
6.1 Overview

The "Edge Devices" screen provides you an overview of all Edge Devices that are connected to your IEM and the possibility of adding new Edge Devices to the IEM. The screen also includes all (foreign) Edge Devices from other groups that are unlocked and shared with you. You find more information on creating groups and sharing Edge Devices with other users in the "My Admin Groups (Page 217)" subsection.

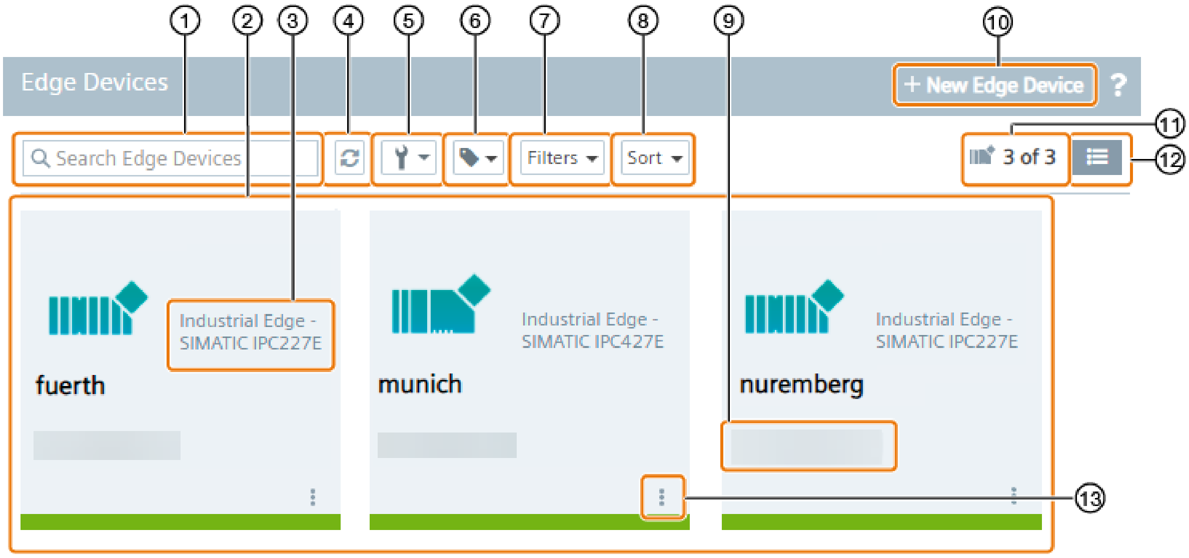
Connected Edge Devices

The layout of the "Edge Devices" screen varies depending on whether or not Edge Devices have already been added to the IEM.

If you have added no Edge Devices yet to the IEM, the "Edge Devices" screen is displayed as follows:



Once you add an Edge Device to the IEM, the "Edge Devices" screen is displayed as follows for example:



① Search bar: Enter a keyword to search for within the Edge Device table

② Connected Edge Devices inclusive following information:

- Edge Device icon
- Edge Device name
- IP address of the Edge Device
- Edge Device type

③ Edge Device type

④ Refresh Edge Device screen

⑤ Edge Device system commands

⑥ Filter Edge Devices by labels or add new labels

⑦ Filter Edge Devices by your own Edge Devices or Edge Devices shared with you

⑧ Sort Edge Device table

⑨ IP address of the Edge Device

⑩ Add new Edge Devices to the IEM

⑪ Number of Edge Devices

⑫ Switch between tile and table view

⑬ Edge Device operations

In case you have enabled the remote access of an Edge Device, you will be redirected to the Edge Device UI by clicking the tile of the Edge Device. You find more information on enabling the remote access of an Edge Device in the "Enabling and disabling remote access (Page 126)" subsection.

By filtering the Edge Device table (⑦) for "Authorized Edge Devices", only shared Edge Devices are displayed.

The available Edge Device operations depend on the permissions you have. The available permissions are listed in the "Roles (Page 221)" subsection.

Note

Using a proxy server after installing the IEM

When you use a proxy server to connect to the IEM after you have installed the IEM and you want to open the Edge Device UI, you must prior add the "Edge Management URL" and "Edge Management Hub URL" name of the IEM to the no proxy address list in the Maintenance UI settings. Otherwise, an error occurs displaying that the Edge Device is temporarily unavailable.

6.2 Connecting an Edge Device

When you add an Edge Device in the Management UI, an Edge Device configuration file is created. You need this configuration file to successfully onboard your Edge Device in the IEM.

Requirements for adding an Edge Device

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

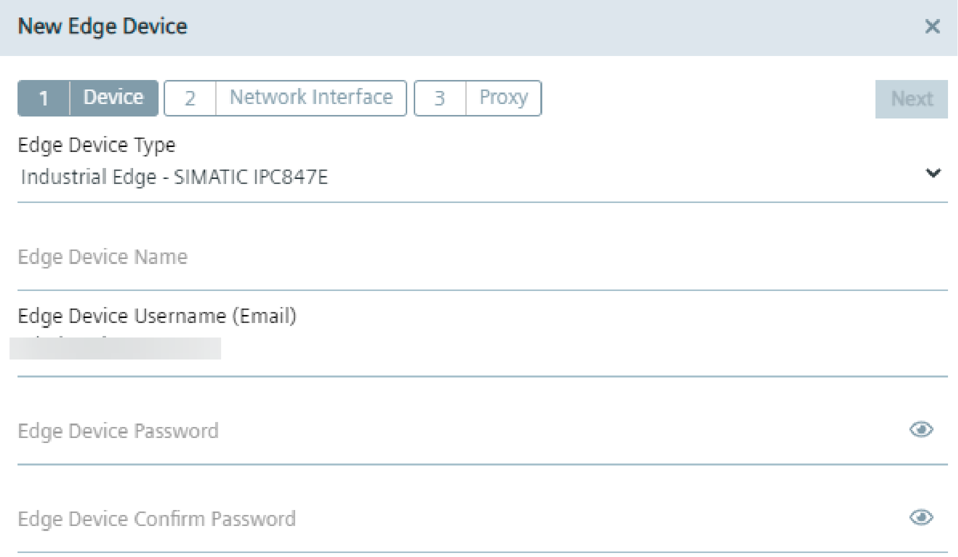
6.2.1 Creating the Edge Device configuration file

Procedure

1. Open and log into the Management UI.
2. Navigate to the "Edge Devices" menu item.

3. In the "Edge Devices" screen, click "New Edge Device".

   The "New Edge Device" screen is displayed.



New Edge Device

Edge Device Type
Industrial Edge - SIMATIC IPC847E

Edge Device Name

Edge Device Username (Email)
[redacted]

Edge Device Password

Edge Device Confirm Password

4. In the "Device" tab, enter all the required information according to the "New Edge Device - Parameters" subsection.

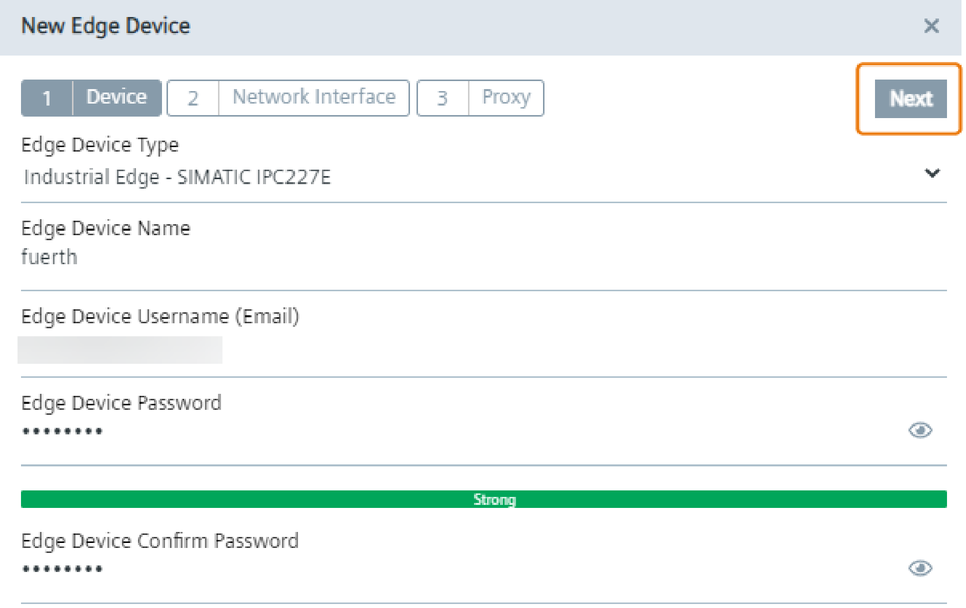
Note

Synchronizing Edge Device Types

Only Edge Device Types that are synchronized with the IEM are available. The admin of the IEM can synchronize Edge Device Types with the IEM under "Admin Management > Device Catalog". You find further information on synchronizing Edge Device Types in the "Admin UI > Device Catalog" subsection in the "Industrial Edge Management - Operation" manual.

---

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



New Edge Device

Edge Device Type
Industrial Edge - SIMATIC IPC227E

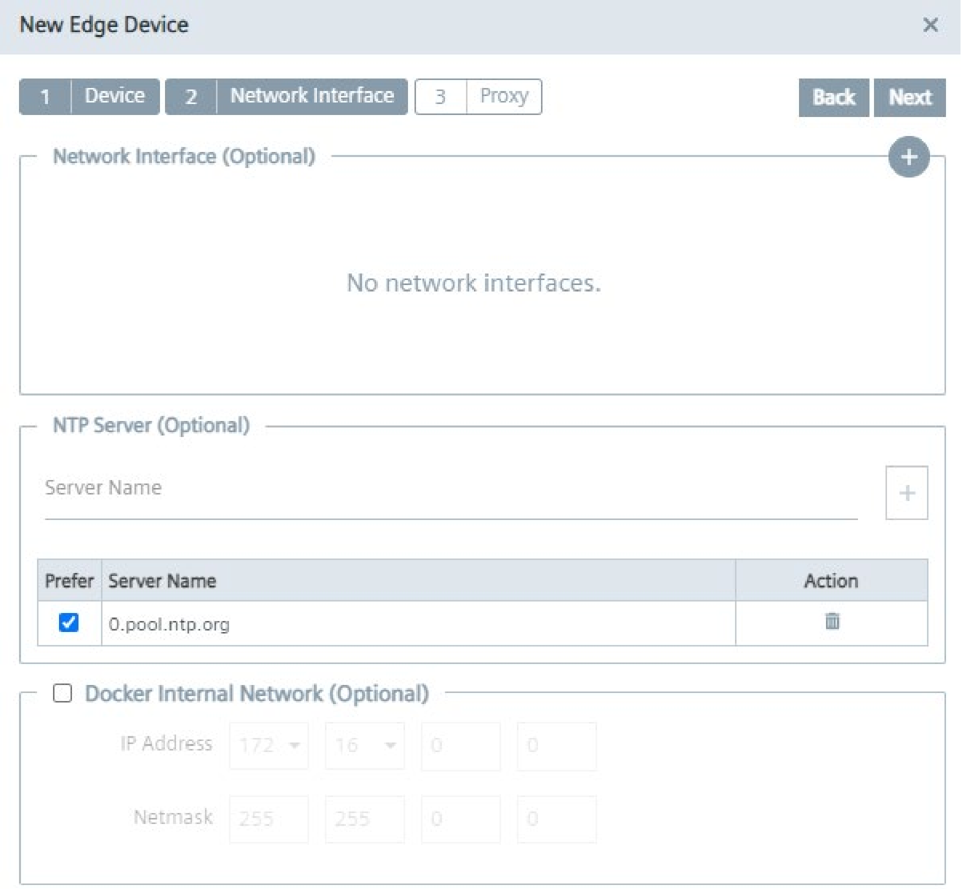
Edge Device Name
fuerth

Edge Device Username (Email)

Edge Device Password
••••••••

Edge Device Confirm Password
••••••••

The "Network Interface" tab is displayed.



New Edge Device

Network Interface (Optional)

No network interfaces.

NTP Server (Optional)

Server Name

Prefer	Server Name	Action
☑	0.pool.ntp.org	🗑

□ Docker Internal Network (Optional)

IP Address 172 16 0 0

Netmask 255 255 0 0

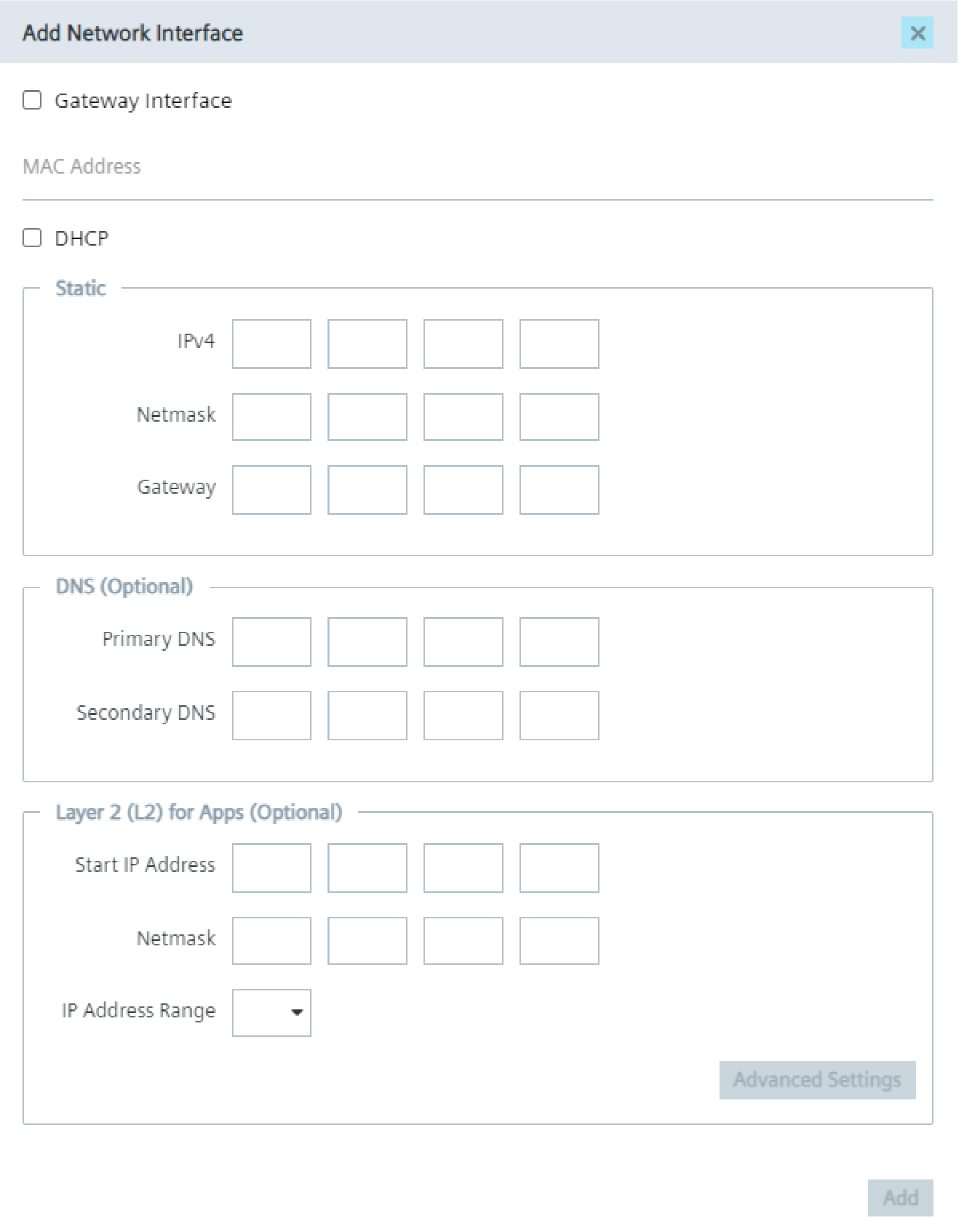
6. To configure the network interface settings for the Edge Device, click the ⊕ icon under the "Network Interface" section.

   Configuring the network interface settings for the Edge Device is optional. It depends on the Edge Device Type whether you must configure the network interface settings or not. If you do not need to configure the network interface settings, the Edge Device is using the default network interface settings provided by the Device Builder. In this case, you can proceed configuring an NTP server and a Docker network as described from step 11 ongoing.

   Note

   You can find the available type of the network interface connection of the respective Edge Device Types in the Edge Device Type details under "Admin Management > Device Catalog". Contact the Device Builder or check the documentation of that Edge Device Type to know, if you must configure the network interface settings for the Edge Device or not.

   The "Add Network Interface" screen is displayed.



Depending on the Edge Device Type, the Edge Device Type and its network interfaces are displayed at the top of the screen.

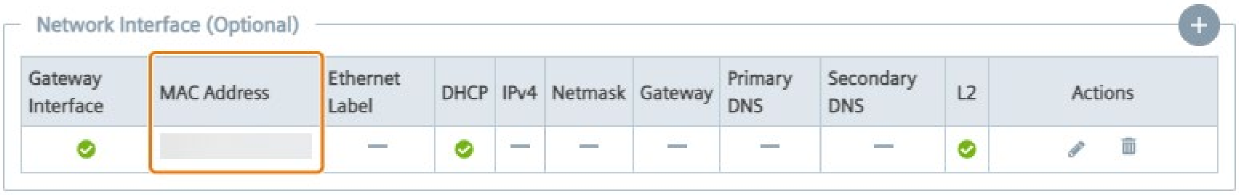
7. Enter the network interface settings of the Edge Device according to the "New Edge Device - Parameters" subsection.
8. If required, set up a Layer 2 network access on this Edge Device under the "Layer 2 (L2) for Apps" section.

   Setting up a Layer 2 network access for apps is optional. You find more information on the Layer 2 network access for apps in the "Layer 2 network access" subsection. When setting up a Layer 2 network access, enter the required information according to the "New Edge Device - Parameters" subsection.

9. When finished, click "Add".

   The configured network interface is added.

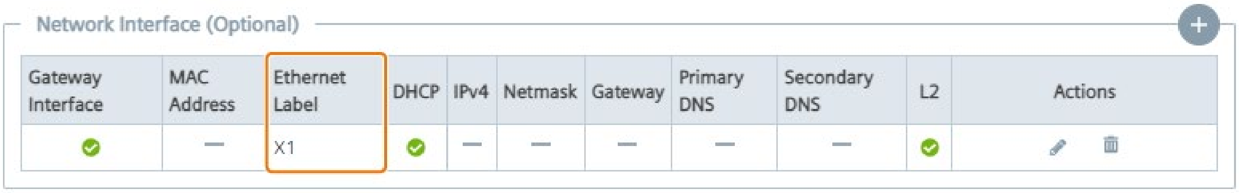
   If you have entered a MAC address, the MAC address is displayed in the table.



Network Interface (Optional)

Gateway Interface	MAC Address	Ethernet Label	DHCP	IPv4	Netmask	Gateway	Primary DNS	Secondary DNS	L2	Actions
✓		—	✓	—	—	—	—	—	✓	✎ 🗑

If you have selected an Ethernet label, instead of the MAC address, the Ethernet label is displayed in the table.

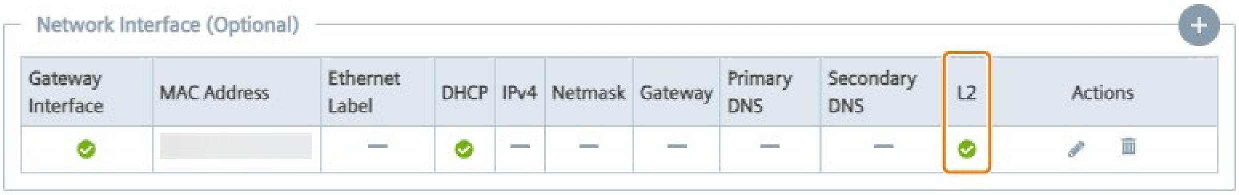


Network Interface (Optional)

Gateway Interface	MAC Address	Ethernet Label	DHCP	IPv4	Netmask	Gateway	Primary DNS	Secondary DNS	L2	Actions
✓	—	X1	✓	—	—	—	—	—	✓	✎ 🗑

You can add more than 1 network interface by clicking the + icon again and adding another network interface. If the maximum number of network interfaces is reached, the + icon is disabled.

If you have configured a Layer 2 network access, the L2 check mark is activated which means that the L2 network access is enabled.



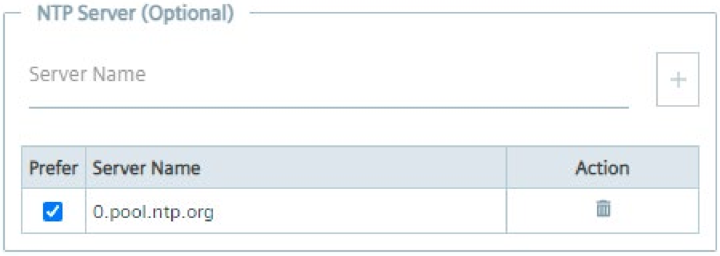
Network Interface (Optional)

Gateway Interface	MAC Address	Ethernet Label	DHCP	IPv4	Netmask	Gateway	Primary DNS	Secondary DNS	L2	Actions
✓		—	✓	—	—	—	—	—	✓	✎ 🗑

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

10. Select 1 Network Time Protocol (NTP) server you want to use for this Edge Device under the "NTP Server" section.

    When you already have configured an NTP server during the setup of the Industrial Edge Management or when you added an NTP server in the Maintenance UI settings and selected the "Use Same NTP On IED" check box, the NTP servers are displayed under the "NTP Server" section .

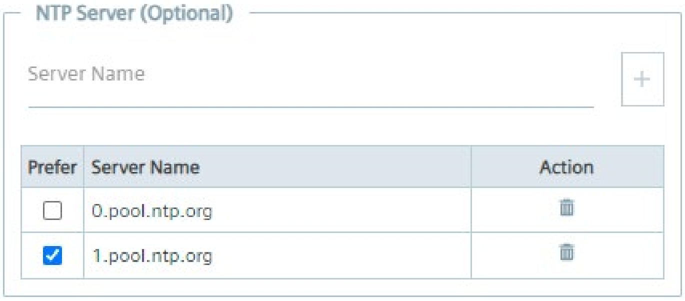
    

    NTP Server (Optional)

    Server Name +

Prefer	Server Name	Action
☑	0.pool.ntp.org	🗑

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

    NTP Server (Optional)

    Server Name +

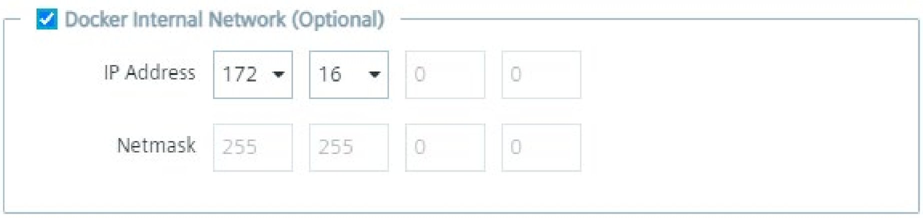
Prefer	Server Name	Action
☐	0.pool.ntp.org	🗑
☑	1.pool.ntp.org	🗑

Note

Time synchronization of the Industrial Edge Management and Edge Devices

A flawless operation of the Industrial Edge Management and Edge Devices require time synchronization of the Industrial Edge Management and Edge Devices. To properly synchronize the time on the Industrial Edge Management and Edge Devices, an NTP server is required. Either use the default configured Debian NTP servers which will be used once you connect the PC, on which the Industrial Edge Management is running, with the Internet. Or, when you operate the Industrial Edge Management and Edge Devices disconnected from the Internet in your local network, provide an own NTP server to which the Industrial Edge Management and Edge Devices must be able to connect to.

11. If you want to change the default Docker network, click the "Docker Internal Network" check box.



☑ Docker Internal Network (Optional)

IP Address 172 16 0 0

Netmask 255 255 0 0

By default, the Edge Device contains 2 Docker networks, 1 for the proxy-redirect and 1 for the docker0 interface (that you create via the "IP Address" input field). When you install an app which creates a new Docker network on the Edge Device, the Docker network of the installed app must not overlap the Docker networks of the Edge Device and need free Docker network IP ranges on the Edge Device.

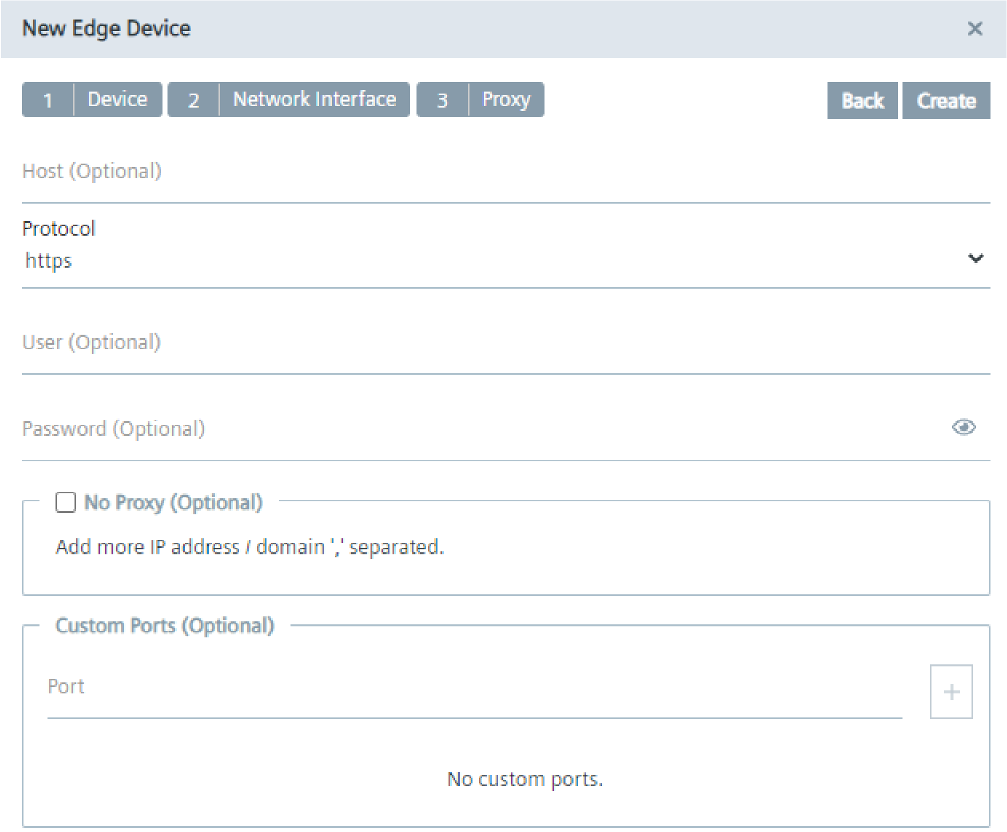
By default, the docker0 interface starts with 172.17.0.0. Using a different docker0 interface is optional.

12. In the "IP Address" input field, select the IP address of the docker0 interface you want to use for the Edge Device.

The IP address of the docker0 interface is the start of the docker0 interface. The subnet mask is not configurable.

13. Click "Next".

14. In the "Proxy" tab, enter, if needed, all required proxy information according to the "New Edge Device - Parameters" subsection.



New Edge Device

Protocol
https

□ No Proxy (Optional)

Add more IP address / domain ',' separated.

No custom ports.

15. Click "Create".

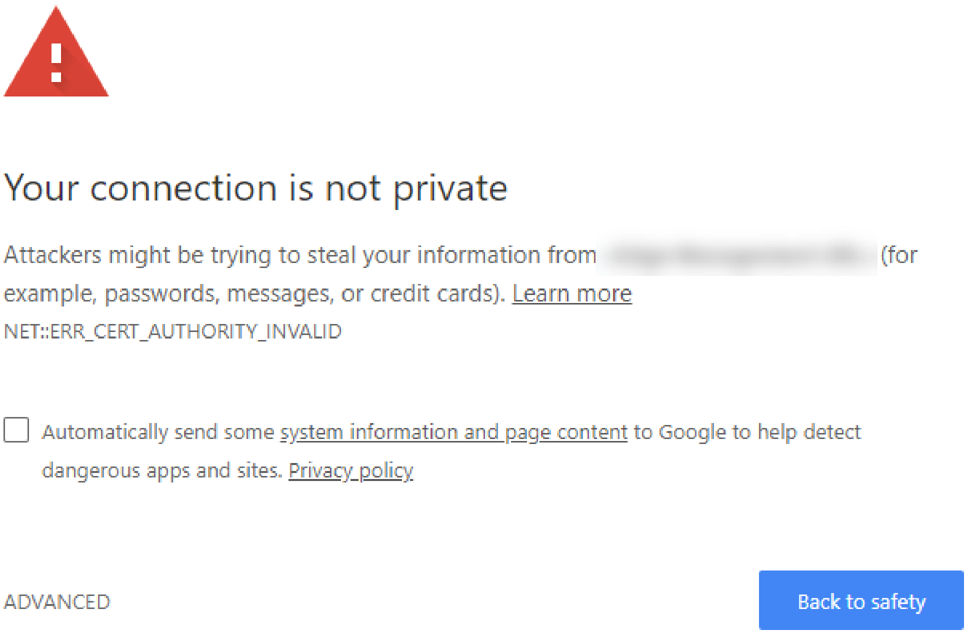
A configuration file named "device-<Edge Device Name>" is downloaded to the standard download folder of your Internet browser.

6.2.2 Onboarding the Edge Device

Procedure

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

   A certificate warning is displayed.



Your connection is not private

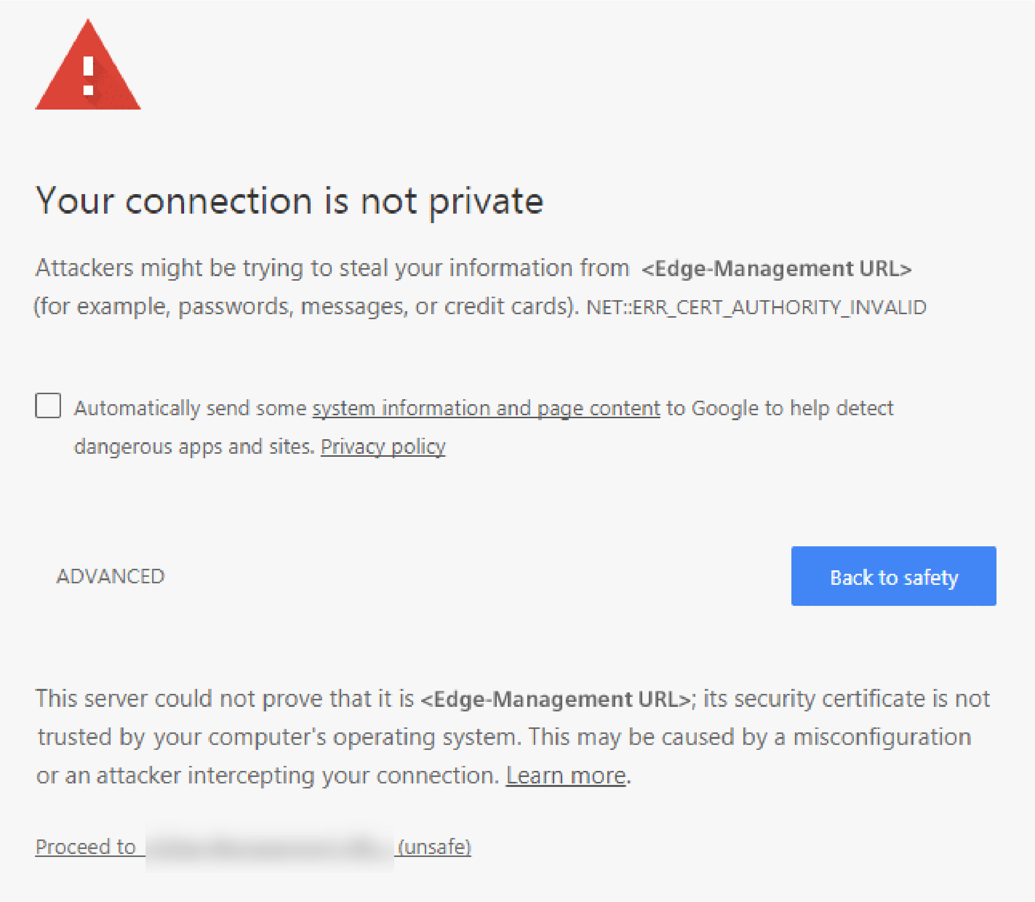
Attackers might be trying to steal your information from [redacted] (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

2. Click "Advanced".

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



Your connection is not private

Attackers might be trying to steal your information from **<Edge-Management URL>** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

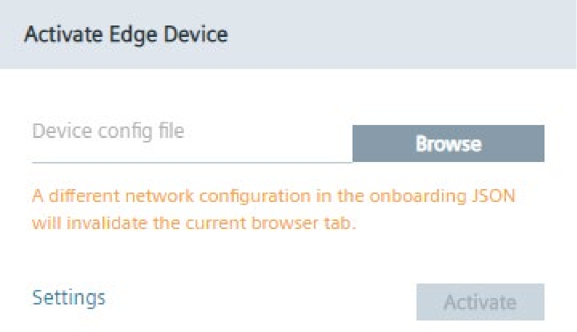
ADVANCED

Back to safety

This server could not prove that it is **<Edge-Management URL>**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

Proceed to [redacted] (unsafe)

The "Activate Edge Device" screen is displayed.



Activate Edge Device

Device config file

Browse

A different network configuration in the onboarding JSON will invalidate the current browser tab.

Settings

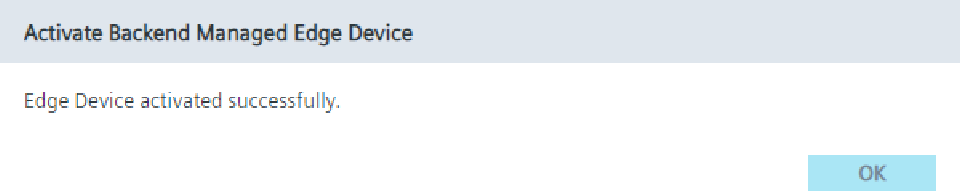
Activate

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

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

   You find the procedure on how to configure each setting in the "Settings" subsection.
6. After configuring the settings, click "Activate".

   The Edge Device is being connected to the IEM. When the connecting process was successful, an according message is displayed.

   Activate Backend Managed Edge Device

   Edge Device activated successfully.

7. Click "Ok".

   You will be redirected to the Edge Device UI.

   Note

   Connection successful

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

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

   The home page of the Edge Device UI is displayed.

Note

When you onboard a SIMATIC IPC Edge Device, you also have the possibility to onboard it via a USB flash drive. You find the procedure and additional information on this procedure in the "SIMATIC IPC Industrial Edge Device - Operation (https://support.industry.siemens.com/cs/us/en/view/109803878)" manual.

6.2.3 New Edge Device - Parameters

Device

Parameter	Description
Edge Device Type	Device type of the Edge Device you want to onboard, for example SIMATIC IPC227E
Edge Device Name	• Unique domain wide name of the Edge Device • Must contain 3 - 15 characters • Only lower case letters and numbers
Edge Device Username	Valid email address of the user for signing into the Edge Device
Edge Device Password	• Password for signing into the Edge Device • Minimum 8 characters • Minimum 1 upper case letter • Minimum 1 special character • Minimum 1 number • The following characters are recognized as special characters: ! @ # $ % ^ & * . ( ) _ +
Edge Device Confirm Password	Confirm Edge Device password

Network Interface

Parameter	Description
Gateway Interface	• In a typical setup, the IEM and cloud access are reachable via default route and default gateway. In this case, enable the "Gateway Interface" check box for the network interface, for example either X1 or X2, to which the default router and the default gateway is connected to • If this default network interface is not reachable or the connection to the interface fails, a connection to another network interface is attempted to be established
MAC Address	• Depending on the Edge Device Type, either "MAC Address", "Ethernet Label" or both is available • If the Edge Device Type requires a MAC address, this field is enabled • In case both "MAC Address" and "Ethernet Label" are available, select 1 of them you want to use • Enter the MAC address of the network interface which is currently configured • Use colons as separations • Example MAC address: 00:0c:29:82:3f:81

Parameter	Description
Ethernet Label	• Depending on the Edge Device Type, either "MAC Address", "Ethernet Label" or both is available • If the Edge Device Type requires an Ethernet label, this field is enabled • In case both "MAC Address" and "Ethernet Label" are available, select 1 of them you want to use • Select the network interface you want to use to connect the Edge Device to the IEM
DHCP	• Enable or disable IP address assignment through DHCP • If this check box is selected, the IP address is assigned through DHCP • When the check box is disabled, static IP address assignment is used
IPv4	• Only enabled when DHCP is disabled • IP address of the Edge Device in the network • Input of the IP address is mandatory when DHCP is disabled
Netmask	• Only enabled when DHCP is disabled • Subnet mask in the "255 255 0 0" format, for example • Input of the subnet mask is mandatory when DHCP is disabled
Gateway	• Only enabled when DHCP is disabled • IP address of the gateway • Input of the IP address is mandatory when DHCP is disabled
Primary DNS	• Primary DNS server address • Input of the DNS server address is optional
Secondary DNS	• Secondary DNS server address • Input of the DNS server address is optional
Start IP Address	• L2 network access is optional • Start of the L2 network access IP address range • Number in the last octet must be even • Input of Start IP Address is mandatory for L2 network access usage
Netmask	• Netmask defines the section in which the IP addresses are located • Input of netmask is mandatory for L2 network access usage
IP Address Range	• Length of the IP address range for usage of Edge Apps with direct L2 network access • Minimum IP address range is 2, maximum range is 256 • Valid displayed IP address range depends on last number in Start IP address, for example: – If last number of Start IP address is 16: 1, 2, 4, 8 and 16 is available – If last number Start IP address is 172: 1, 2 and 4 is available – If last number Start IP address is 0: 1, 2, 4, 8, 16, 32, 64, 128 and 256 is available • Input of IP address range is mandatory for L2 network access usage

Note

MAC address and Ethernet label

It depends on the Edge Device Type which input type is required for the network interface settings, whether MAC address or Ethernet label. The Edge Device builder by himself forces which type is required and must be provided to onboard the Edge Device to the IEM.

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

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

Note

IP address and broadcast IP address of subnet

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

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

Proxy

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

6.2.4 Layer 2 network access

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

When you onboard an Edge Device to the IEM, you define the IP address range of the Layer 2 network access which is then reserved for communication between Edge Apps and automation devices. To install and use Edge Apps on Edge Devices that need to communicate with automation devices, you must enable the Layer 2 network access on the respective Edge Devices during the onboarding procedure. Edge Apps that require a Layer 2 network access can only be installed on Edge Devices with an appropriate configured Layer 2 network access. The Layer 2 network access activation and configuration is saved to the Edge Device configuration file.

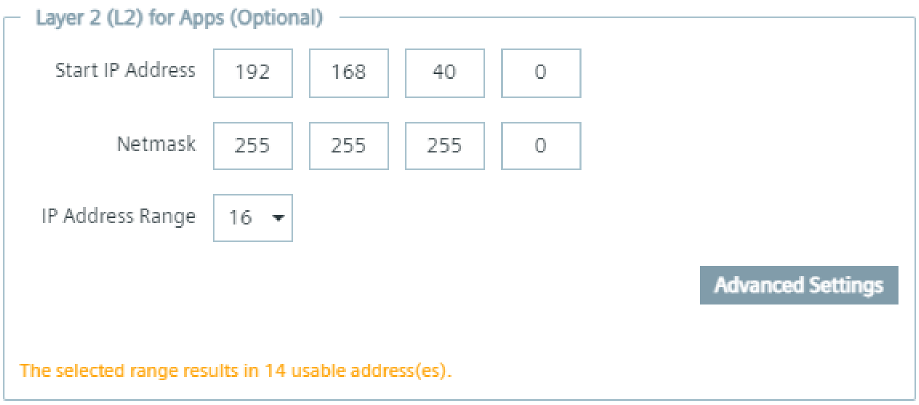
If you edit a configured Layer 2 network access on the Edge Device while apps running on this Edge Device are using the Layer 2 network access, the apps will first stop running. After you have finished editing the Layer 2 network access, the apps will restart and run again with the new settings. If you remove a configured Layer 2 network access on this Edge Device while apps running on this Edge Device are using the Layer 2 network access, the apps will not work anymore.

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

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

6.2.4.1 Configuring a Layer 2 network access

Set up a Layer 2 network access on the Edge Device under the "Layer 2 (L2) for Apps" section, as shown below for example:



Layer 2 (L2) for Apps (Optional)

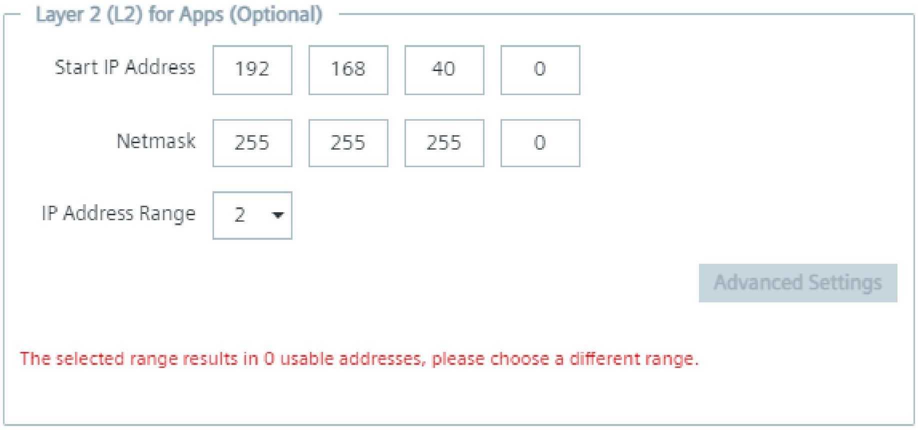
Start IP Address: 192 . 168 . 40 . 0

Netmask: 255 . 255 . 255 . 0

IP Address Range: 16

The selected range results in 14 usable address(es).

Depending on the starting IP address and the IP range of the Layer 2 network access, defined by the subnet that you provide, a certain amount of IP addresses are available for the Layer 2 network access. In this example, the IP address range shows 16 reserved IP addresses. Since 1 IP address is reserved for the gateway and 1 is reserved for the network itself, 14 IP addresses are usable. Setting up a Layer 2 network access configuration with just 2 reserved IP addresses is not valid since 2 IP addresses are reserved by default, 1 for the gateway and 1 for the network itself.


Layer 2 (L2) for Apps (Optional)

Start IP Address 192 168 40 0

Netmask 255 255 255 0

IP Address Range 2

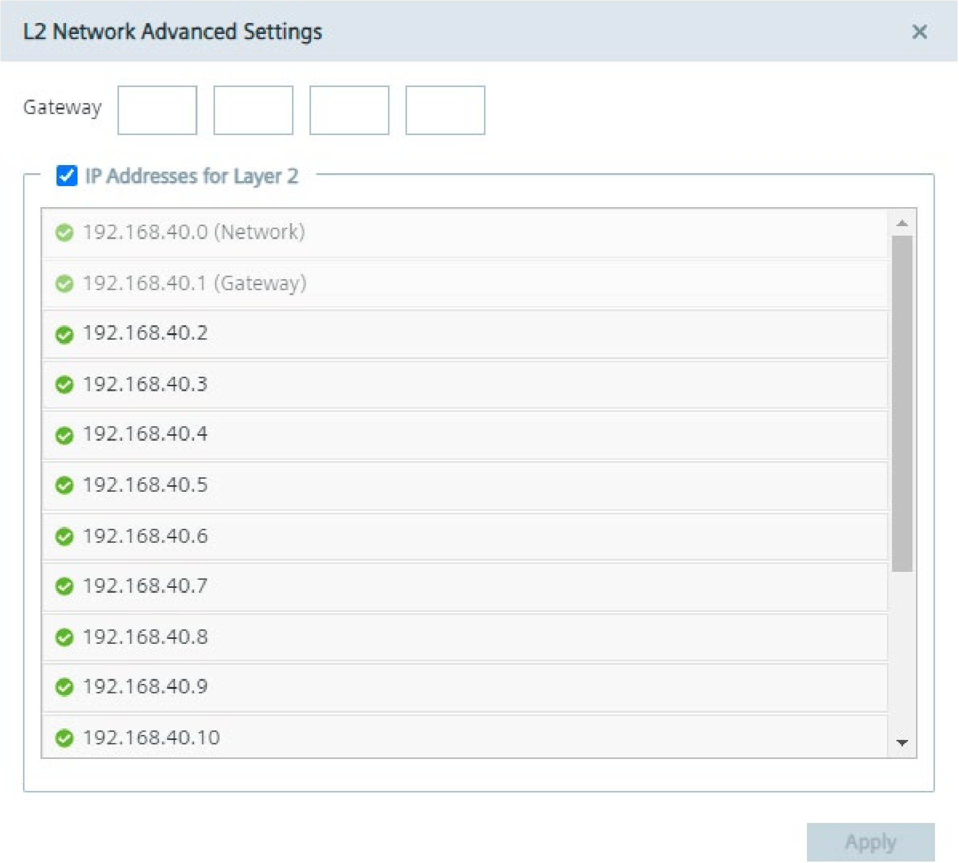
The selected range results in 0 usable addresses, please choose a different range.

To use the Layer 2 network access, the selected IP address range must be minimum 3.

Note

The amount of usable IP addresses is always displayed in the dialog.

When you click "Advanced Settings", you can specify which IP addresses can be used for the Layer 2 network access in the defined IP range. After clicking "Advanced Settings", a list with several IP addresses, depending on the starting IP address and the IP range, are displayed, as shown below for example:



L2 Network Advanced Settings

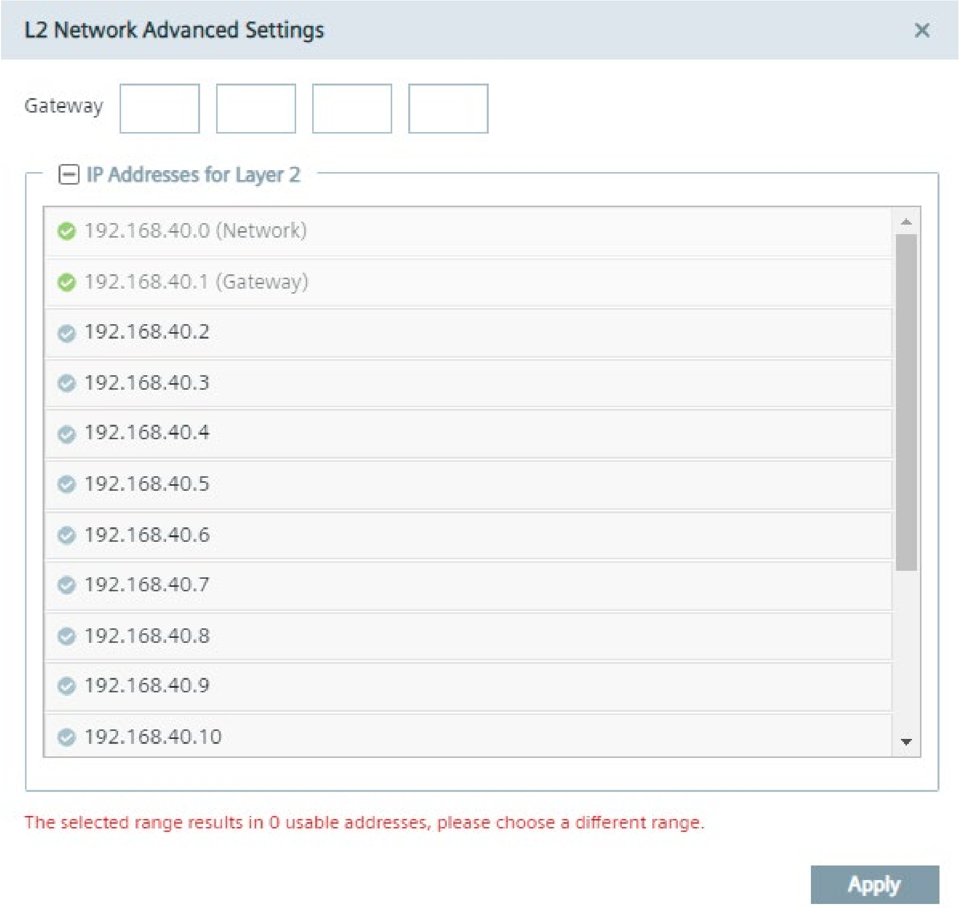
Gateway

☑ IP Addresses for Layer 2

- ✓ 192.168.40.0 (Network)
- ✓ 192.168.40.1 (Gateway)
- ✓ 192.168.40.2
- ✓ 192.168.40.3
- ✓ 192.168.40.4
- ✓ 192.168.40.5
- ✓ 192.168.40.6
- ✓ 192.168.40.7
- ✓ 192.168.40.8
- ✓ 192.168.40.9
- ✓ 192.168.40.10

By selecting an IP address, the IP address can be used for the Layer 2 network access for apps. By not selecting an IP address, the IP address is blocked and will not be used.

Again, since 1 IP address is reserved for the gateway and 1 is reserved for the network itself, minimum 1 IP address other than these 2 must be selected. Otherwise, an error will be displayed.



L2 Network Advanced Settings

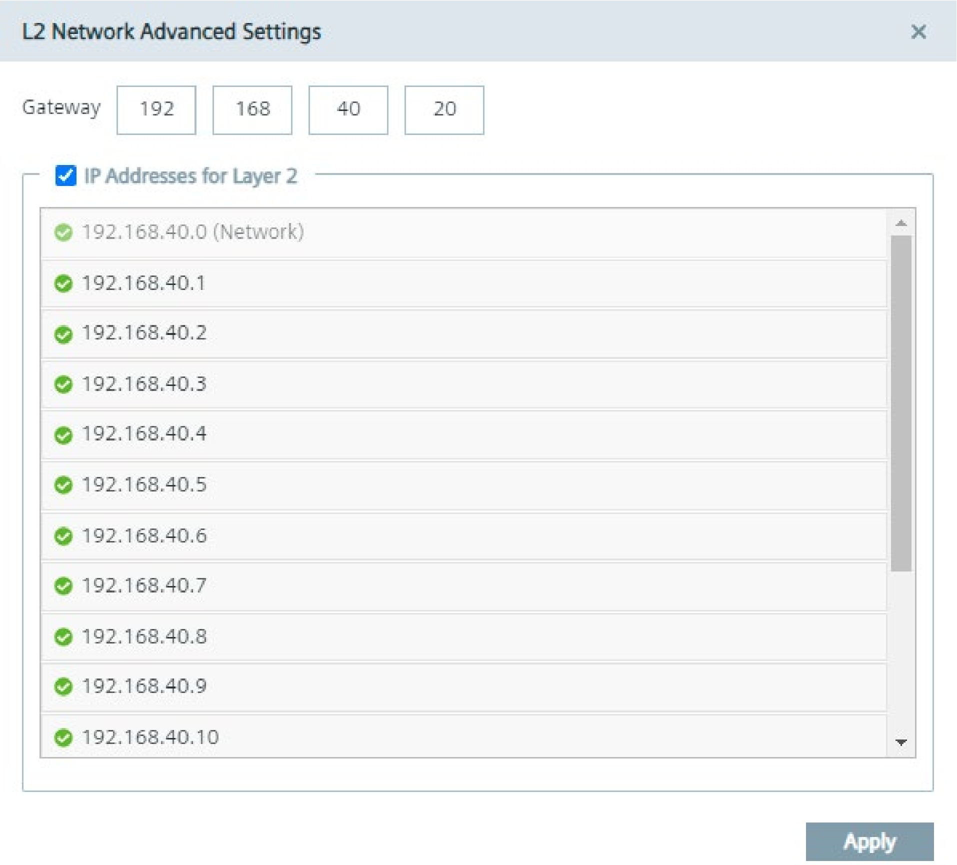
Gateway

IP Addresses for Layer 2

- 192.168.40.0 (Network)
- 192.168.40.1 (Gateway)
- 192.168.40.2
- 192.168.40.3
- 192.168.40.4
- 192.168.40.5
- 192.168.40.6
- 192.168.40.7
- 192.168.40.8
- 192.168.40.9
- 192.168.40.10

The selected range results in 0 usable addresses, please choose a different range.

By default, the gateway is within the entered IP range. Under "Gateway", you can define an IP address for the gateway to obtain 1 more available IP address in the given IP range, but the IP address of the gateway must be within the entered subnet.



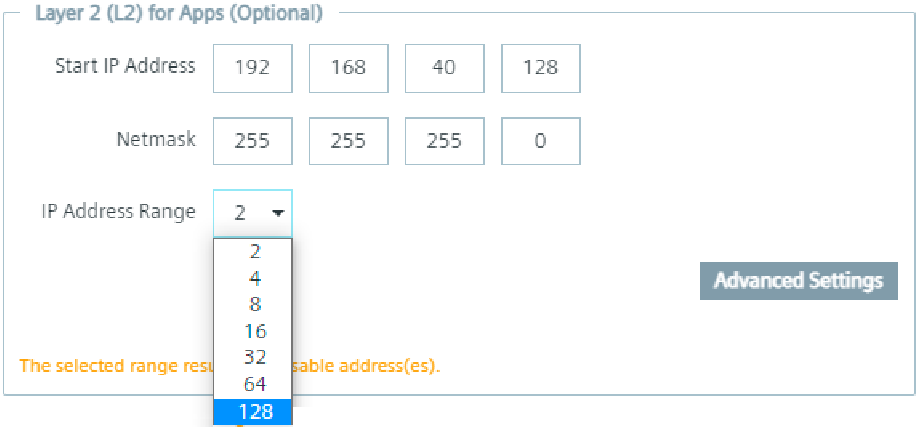
L2 Network Advanced Settings

Gateway: 192 . 168 . 40 . 20

☑ IP Addresses for Layer 2

- ✓ 192.168.40.0 (Network)
- ✓ 192.168.40.1
- ✓ 192.168.40.2
- ✓ 192.168.40.3
- ✓ 192.168.40.4
- ✓ 192.168.40.5
- ✓ 192.168.40.6
- ✓ 192.168.40.7
- ✓ 192.168.40.8
- ✓ 192.168.40.9
- ✓ 192.168.40.10

If you select the maximum available IP address range back in the "Layer 2 (L2) for Apps" section, 1 IP address will be also reserved for broadcast, as shown below for example.



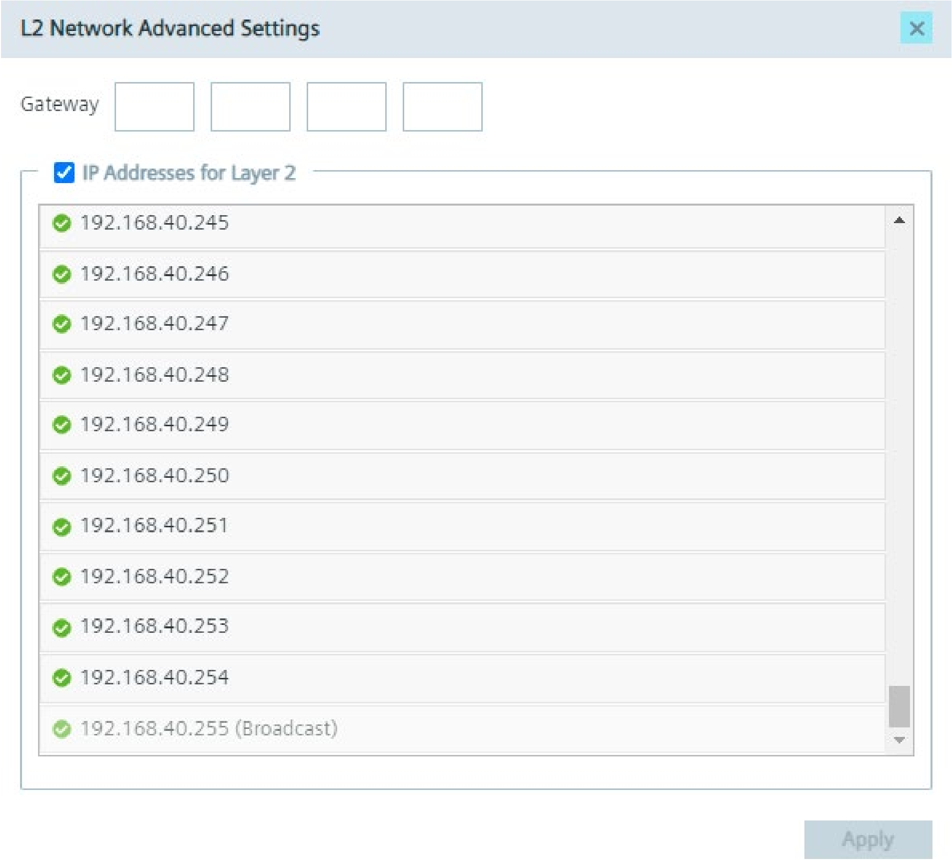
Layer 2 (L2) for Apps (Optional)

Start IP Address: 192 . 168 . 40 . 128

Netmask: 255 . 255 . 255 . 0

IP Address Range: 2

The selected range resu sable address(es).



Gateway

☑ IP Addresses for Layer 2

- ✓ 192.168.40.245
- ✓ 192.168.40.246
- ✓ 192.168.40.247
- ✓ 192.168.40.248
- ✓ 192.168.40.249
- ✓ 192.168.40.250
- ✓ 192.168.40.251
- ✓ 192.168.40.252
- ✓ 192.168.40.253
- ✓ 192.168.40.254
- ✓ 192.168.40.255 (Broadcast)

To save the Layer 2 network access changes, click "Apply".

6.2.5 Settings

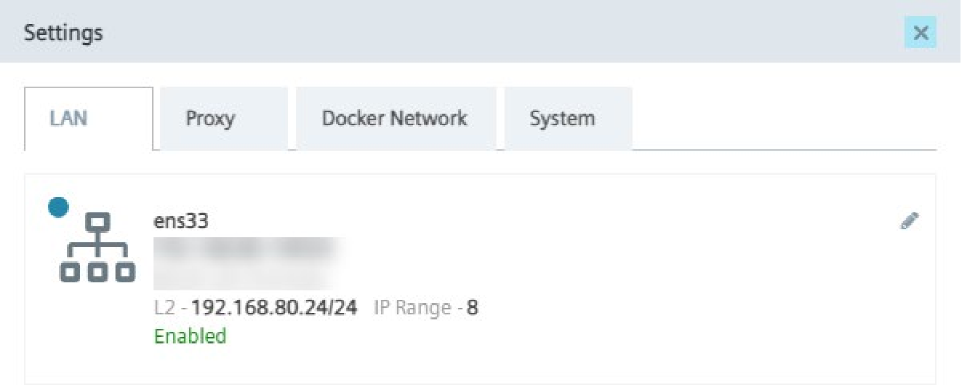
6.2.5.1 Editing network and Layer 2 network access settings

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

Procedure

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

   The "Settings" screen is displayed.



ens33
[redacted]
L2 - 192.168.80.24/24 IP Range - 8
Enabled

Note

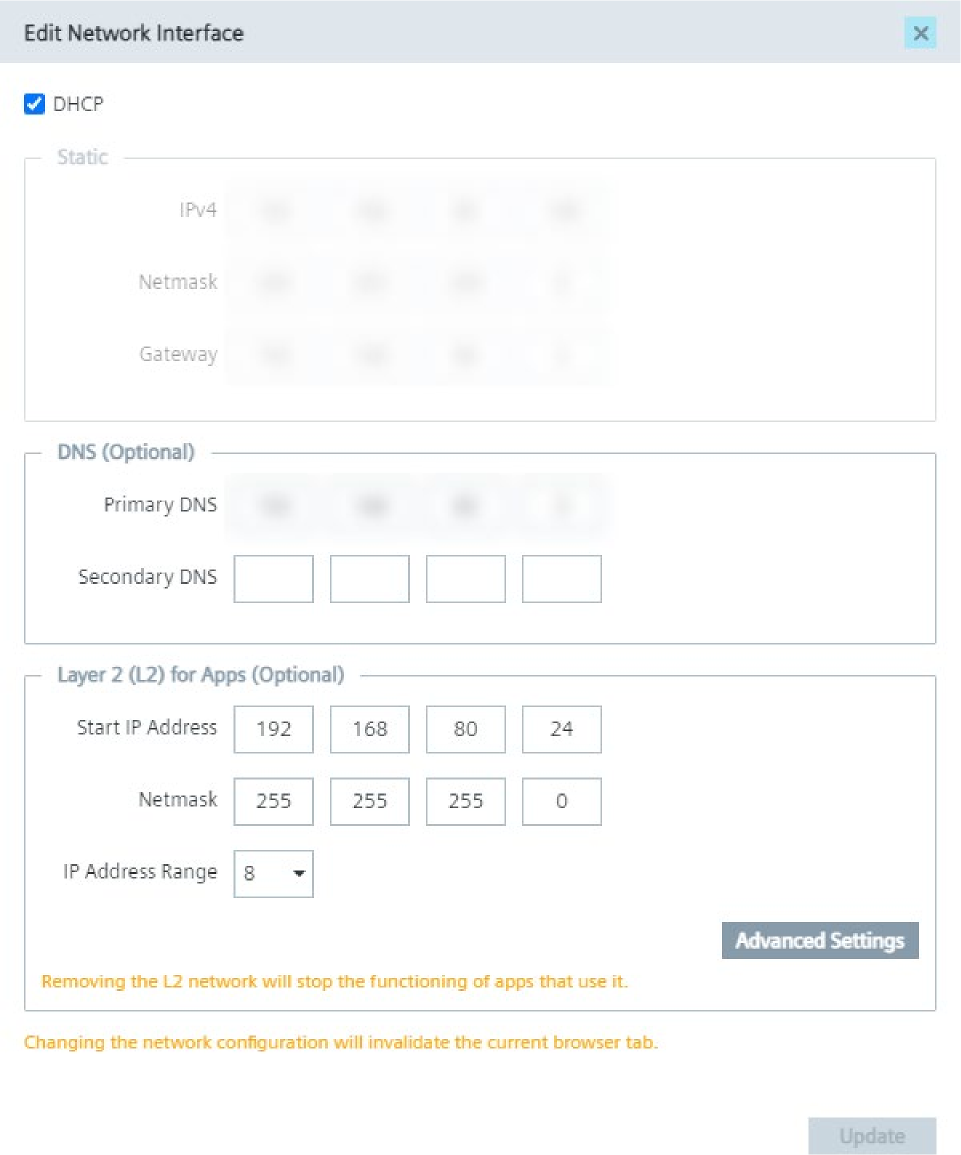
Connected network interface

When you select a network interface, for example X1 or X2, during the creation of the Edge Device configuration file that should be used to connect the Edge Device to the IEM, the respective network interface will be also displayed in this screen.

---

2. To edit the network settings, click the ✎ icon.

   The "Edit Network Interface" screen is displayed.



Edit Network Interface

☑ DHCP

Static

IPv4 [redacted]

Netmask [redacted]

Gateway [redacted]

DNS (Optional)

Primary DNS [redacted]

Secondary DNS

Layer 2 (L2) for Apps (Optional)

Start IP Address 192 168 80 24

Netmask 255 255 255 0

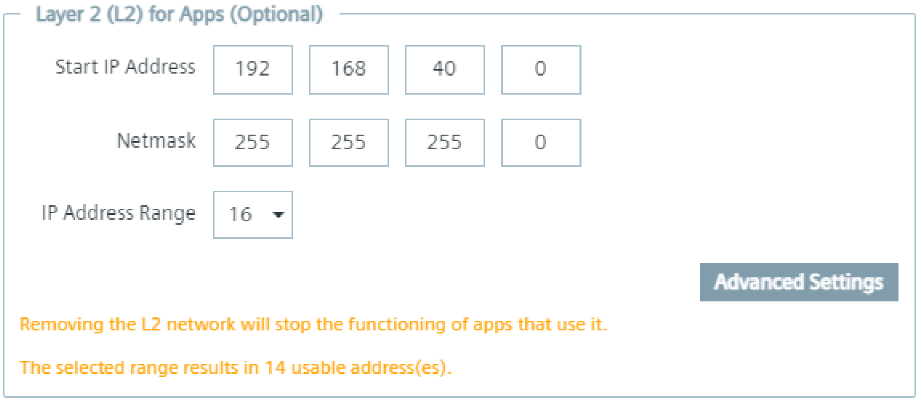
IP Address Range 8

Removing the L2 network will stop the functioning of apps that use it.

Changing the network configuration will invalidate the current browser tab.

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

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


Layer 2 (L2) for Apps (Optional)

Start IP Address 192 168 40 0

Netmask 255 255 255 0

IP Address Range 16

Removing the L2 network will stop the functioning of apps that use it.

The selected range results in 14 usable address(es).

Note

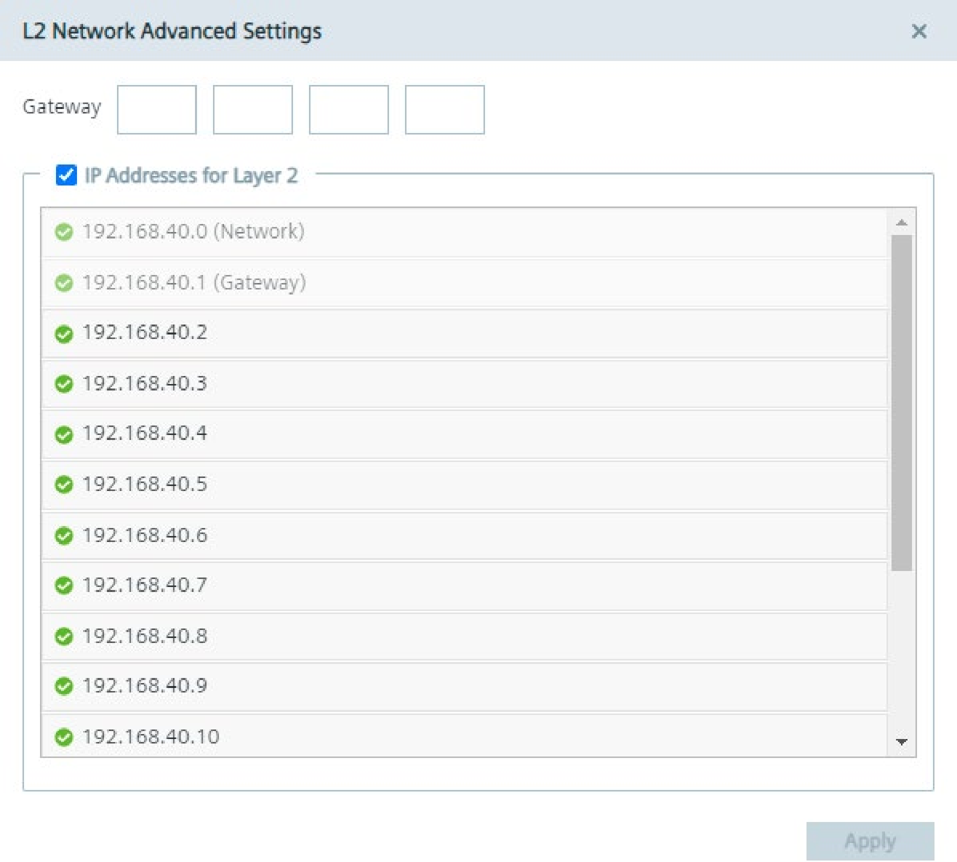
Removing Layer 2 network access

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

You find more information on the Layer 2 network access in the "Layer 2 network access (Page 104)" and the "New Edge Device - Parameters (Page 101)" subsections.

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

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



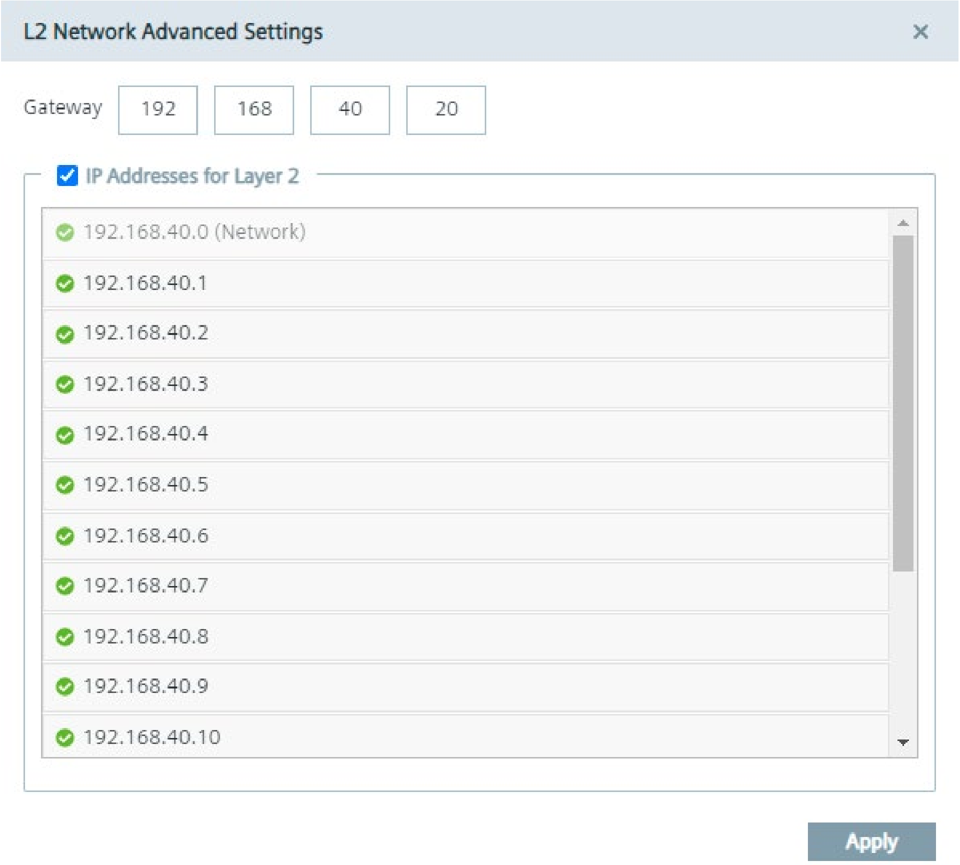
L2 Network Advanced Settings ×

Gateway

☑ IP Addresses for Layer 2

✓ 192.168.40.0 (Network)
✓ 192.168.40.1 (Gateway)
✓ 192.168.40.2
✓ 192.168.40.3
✓ 192.168.40.4
✓ 192.168.40.5
✓ 192.168.40.6
✓ 192.168.40.7
✓ 192.168.40.8
✓ 192.168.40.9
✓ 192.168.40.10

   By selecting an IP address, the IP address can be used for the Layer 2 network access for apps. By not selecting an IP address, the IP address is blocked and will not be used. By default, the gateway is within the entered IP range. Under "Gateway", you can define an IP address for the gateway to obtain 1 more available IP address in the given IP range, but the IP address of the gateway must be within the entered subnet.



L2 Network Advanced Settings

Gateway 192 168 40 20

☑ IP Addresses for Layer 2

- ✓ 192.168.40.0 (Network)
- ✓ 192.168.40.1
- ✓ 192.168.40.2
- ✓ 192.168.40.3
- ✓ 192.168.40.4
- ✓ 192.168.40.5
- ✓ 192.168.40.6
- ✓ 192.168.40.7
- ✓ 192.168.40.8
- ✓ 192.168.40.9
- ✓ 192.168.40.10

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

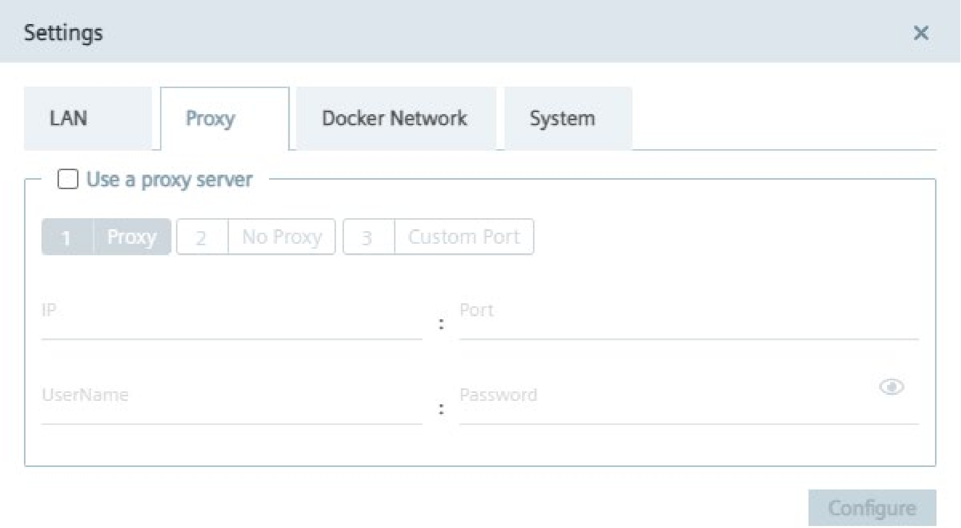
6.2.5.2 Setting up a proxy server

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

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

Procedure

1. Click the "Proxy" tab.



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

   The input fields for the proxy server settings are enabled.

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

4. If needed, enter username and the corresponding password in the according input fields in case of an additional authentication for the proxy server.

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

   – The password must start with an alphabetic character

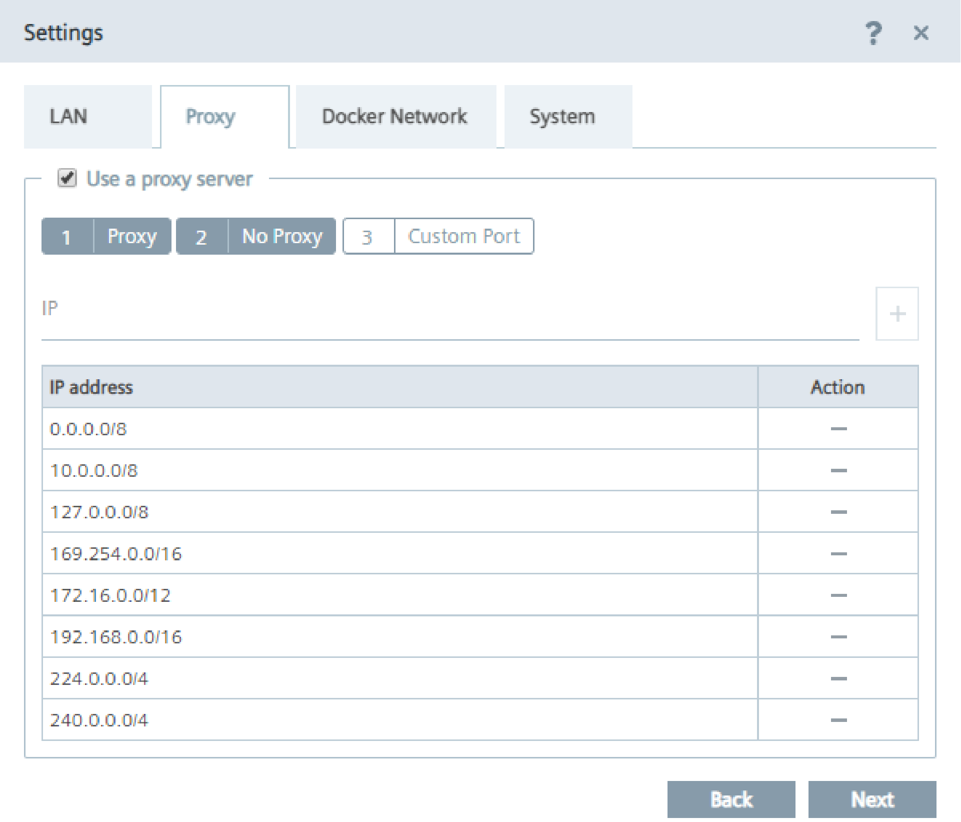
   – The password must not contain complex characters, such as \ . * "

   – The password must not be longer than 21 characters

   The settings apply for HTTP and HTTPS proxy servers.

5. Click "Next".

   The "No Proxy" tab is displayed.



☑ Use a proxy server

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	—

   In the "No Proxy" tab, add all the IP addresses which shall be accessed directly (without use of proxy).

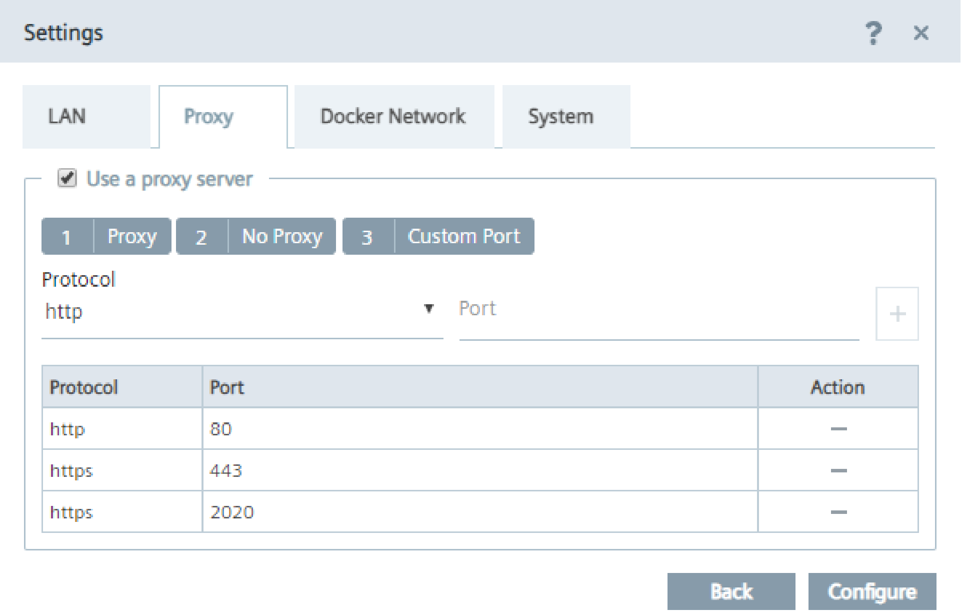
   By default, several no proxy addresses are listed which are required by the IEM.

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

   The address is added to the no proxy list.

7. Click "Next".

   The "Custom Port" tab is displayed.



☑ Use a proxy server

Protocol: http

Protocol	Port	Action
http	80	−
https	443	−
https	2020	−

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

By default, several ports are listed which are required by the IEM.

Note

Default no proxy addresses and ports

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

---

8. If you want to add a further port, select the required protocol from the "Protocol" drop-down list and enter the required port.

9. To add the port, click the + icon.

   The port is added to the port list.

10. To add the proxy settings, click "Configure".

11. Confirm the proxy settings by clicking "Ok".

    The proxy settings are saved.

Note

Setting up a proxy server after onboarding the Edge Device

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

6.2.5.3 Configuring the Docker network

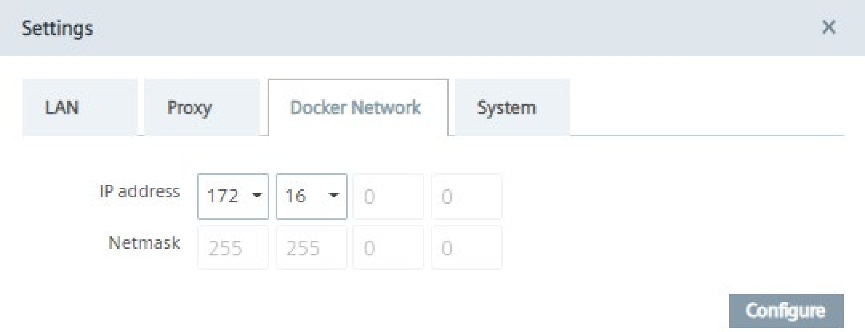
In the "Docker Network" tab, you can edit the IP range of the docker0 interface of the Edge Device, if necessary.

The IP address of the docker0 interface is the start of the docker0 interface. By default, the docker0 interface starts with 172.17.0.0. By default, the Edge Device contains 2 Docker networks, 1 for the proxy-redirect and 1 for the docker0 interface (that you create in the "IP Address" input field). When you install an app which creates a new Docker network on the Edge Device, the Docker network of the installed app must not overlap the Docker networks of the Edge Device and need free Docker network IP ranges on the Edge Device. Otherwise, if you want to install an app that tries to create a new Docker network on the Edge Device but the Edge Device has no free Docker network IP ranges, the app installation fails.

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

Procedure

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



Settings

IP address: 172 . 16 . 0 . 0

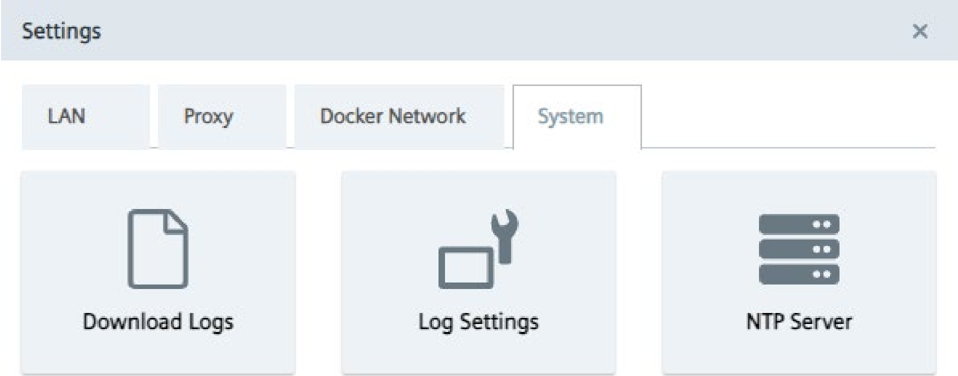
Netmask: 255 . 255 . 0 . 0

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

6.2.5.4 Downloading logs

Procedure

1. Click the "System" tab.



2. Click the "Download Logs" tile.

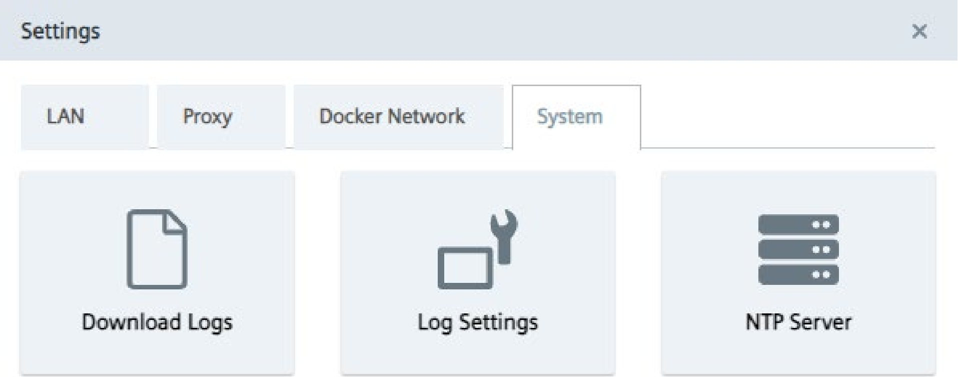
   The log file is being downloaded to the standard download folder of your Internet browser.

6.2.5.5 Editing log settings

Under "Log Settings", you allow or prevent Edge Apps to log into the internal memory of the Edge Device.

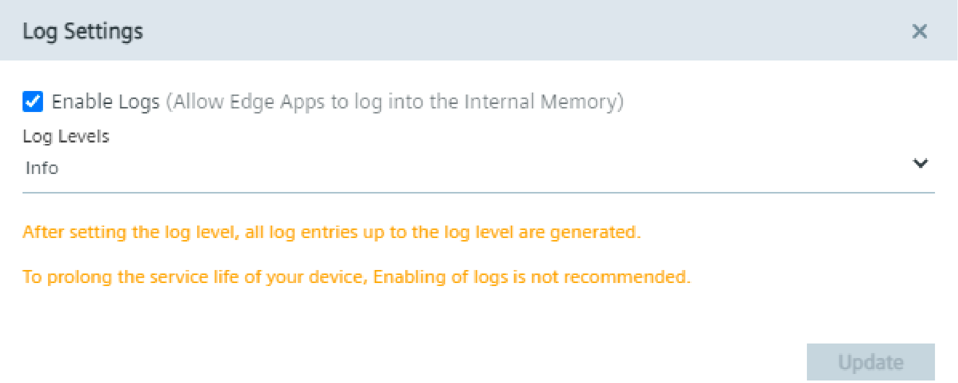
Procedure

1. Click the "System" tab.



2. Click the "Log Settings" tile.

   The "Log Settings" screen is displayed.


Log Settings

☑ Enable Logs (Allow Edge Apps to log into the Internal Memory)

Log Levels: Info

After setting the log level, all log entries up to the log level are generated.

To prolong the service life of your device, Enabling of logs is not recommended.

   By default, Edge Apps are allowed to log into the internal memory. By default, the "Info" log level is selected which means that all log levels up to this level are generated.

3. From the drop-down list, select the log level you want to log into the internal memory.

   All log levels up to this selected log level are generated and logged into the internal memory.

4. If you want to prevent Edge Apps to log into the internal memory of the Edge Device, deselect the "Enable Logs" check box.

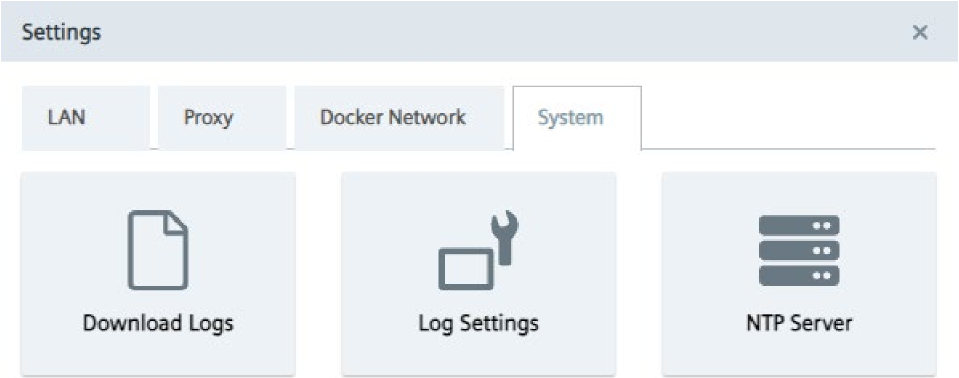
6.2.5.6 Adding an NTP server

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

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

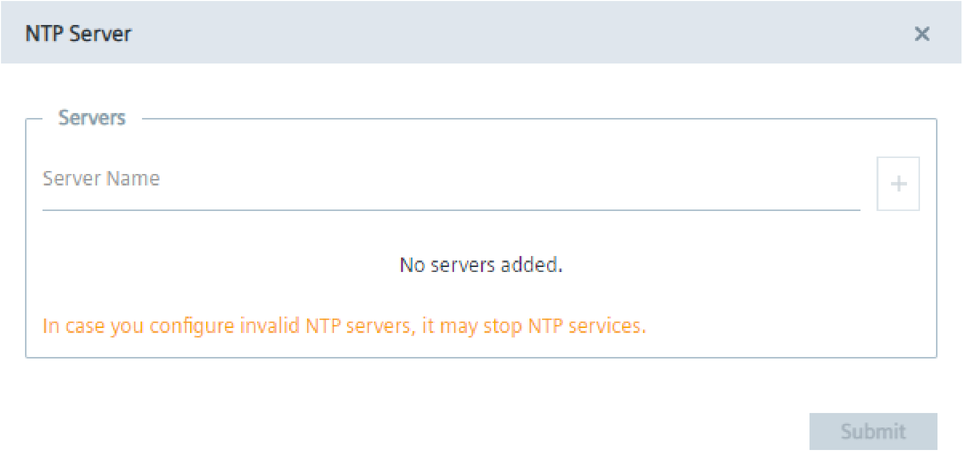
Procedure

1. Click the "System" tab.



2. Click the "NTP Server" tile.

   The "NTP Server" screen is displayed.



No servers added.

In case you configure invalid NTP servers, it may stop NTP services.

3. If you have not added minimum 1 NTP server or you want to add more NTP servers, enter the NTP server in the "Server Name" input field.
4. To add the NTP server, click the plus icon.

   The NTP server is added to the server list. You can add several NTP servers. In case that 1 of them is unavailable, the next NTP server from the list will get active.
5. Click "Submit".

6.2.6 Secure connection

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

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

Connected Edge Device with wildcard or SAN certificates

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

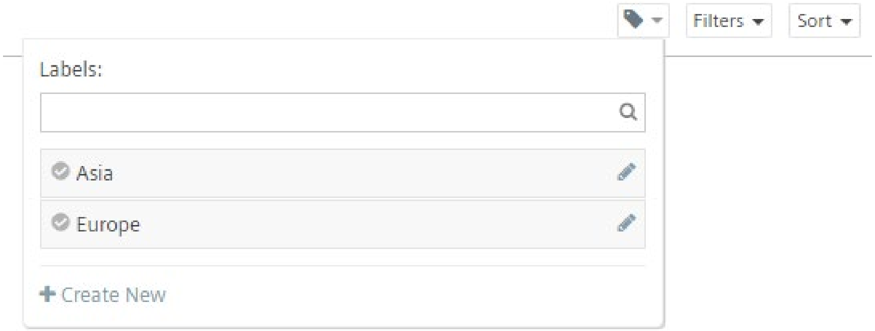
6.3 Managing labels

By default, all new Edge Devices have no labels assigned to them. You have the possibility to assign 1 or more labels to several Edge Devices. In that way, you group your Edge Devices.

Creating new labels

1. Click the 🏷▾ icon.

   All existing labels are displayed.



2. Click "Create New".

   The "New Label" screen is displayed.

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

Note

Subgrouping labels

Once you have created a label, the "New Label" screen has a different layout. If you want to subgroup a label to another label, select the "Nest label under" check box and select the parent label from the drop-down list.

---

4. Click "Create".

   The label is created.

Assigning labels to Edge Devices

1. Click the ⋮ icon of the Edge Device for which you want to assign a label.
2. Click "Manage Labels".

   The "Manage Labels" screen is displayed.

3. Select the label you want to assign to the selected Edge Device.
4. Click "Apply".

   The label is assigned to the Edge Device. When you switch to the table view, all assigned labels to an Edge Device are additionally displayed.

6.4 Checking statistics

Procedure

1. Click the ⋮ icon of the Edge Device for which you want to check its statistics.
2. Click "Statistics".

   The "Statistics" screen is displayed.

   Note

   Connecting to the Edge Device

   If the remote access is enabled for the Edge Device, you open the UI of the Edge Device by clicking "Connect".

6.5 Adding tags

Tags, that are assigned to Edge Devices, support Edge Device specific configurations. When you install an app on Edge Devices with allocated tags, the keys in the template files will be automatically replaced by its corresponding values from the tags that are allocated to the Edge Device.

You find more information on the keys in the "App configurations (Page 178)" subsection.

Procedure

1. Click the ⋮ icon of the Edge Device for which you want to add tags.
2. Click "Tags".

   The "Tags" screen is displayed.
3. Click "Add tag".

   The "Add Tag" screen is displayed.
4. In the "key" input field, enter the key of the tag.
5. In the "Value" input field, enter the value for the key of the tag.
6. Click "Add".

   The tags are added to the tag list.

6.6 Downloading IEM CA certificates

You can download the CA-chain of the Edge Device to import that CA-chain in the Edge Device UI for securing the Internet browser in which the Edge Device UI is managed.

Procedure

1. Click the ⋮ icon of the Edge Device whose CA-chain you want to download.
2. Click "IEM CA Certificates".

   The CA-chain of the Edge Device is downloaded as "*.json" file to the standard download folder of the Internet browser.

6.7 Managing logs

By clicking the ⋮ icon of an Edge Device and then clicking "Logs", the "Logs" screen of the Edge Device is displayed.

In the "Logs" screen, you check the following:

- Logs of the Edge Device
- Logs of Edge Apps that are installed on the Edge Device

The "Edge Device" tab lists all log files which are related to that specific Edge Device. The "Installed Applications" tab lists all log files which are related to Edge Apps that are installed on that Edge Device.

The date of a log file represents the date when the logs has been uploaded from the Edge Device to the IEM.

Note

Uploading logs

Logs are being uploaded from Edge Devices to the IEM every 24 hours by default. You change the time period in the "Settings > Configuration > Portal" menu in the Edge Device UI.

Downloading log files

By clicking the ⤓ icon, the according log file is downloaded to the standard download folder of your Internet browser.

6.8 Importing certificates

To secure the connection to the Edge Device, you must import the certificates that you also use for the IEM.

Procedure

1. Click the ⋮ icon of the Edge Device for which you want to import certificates.
2. Click "Import Certificate".

   The "Import Certificate" screen is displayed.
3. In the "Private key" section, click "Browse" and select the private key that you also use for the IEM.
4. In the "Certificate" section, click "Browse" and select your certificate that you also use for the IEM.
5. To import the certificates, click either "Import Later" or "Import".

   "Import" imports the certificates immediately. When you click "Import Later", select an import time.
6. After you imported the certificates, refresh the Internet browser of the Edge Device UI.

   The connection is secure now.

6.9 Enabling and disabling remote access

When you click the tile of an Edge Device, you cannot open the Edge Device UI in a new browser tab because the remote access is disabled. To open the Edge Device UI in a new browser tab by clicking the tile of the Edge Device, first you have to enable the remote access to the Edge Device.

Requirement

A relay server has been added.

You find information on how to add a relay server in the "Adding a relay server" subsection in the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)" manual.

Enabling remote access

1. Click the ⋮ icon of the Edge Device for which you want to enable the remote access.
2. Click "Enable Remote Access".

   The "Enable Remote Access" screen is displayed.
3. In the "Expiry Time" input field, set the time for the Edge Device to be enabled for the remote access.

   The maximum enabled remote access time is 10 hours, the minimum time is 2 hours.
4. Click "Enable".

   An enable remote access job is created which you can check in the "Job Status" screen. When the job is completed, you can access the Edge Device UI.

   After the enabled remote access time has passed, the Edge Device is no longer accessible.

Disabling remote access

1. Click the ⋮ icon of the Edge Device for which you want to disable the remote access.
2. Click "Disable Remote Access".

   The "Disable Remote Access" command is only available for Edge Devices which have enabled the remote access.

   The "Disable Remote Access" screen is displayed.
3. Click "Disable".

   A disable remote access job is created.

   When the job is completed, the Edge Device is no longer accessible.

6.10 Removing an Edge Device

Requirement

The Edge Device is onboarded successfully to the IEM but is in "Offline" operating state since minimum 24 hours.

Note

Removing an Edge Device

Removing an Edge Device is only possible, when the Edge Device is offline since minimum 24 hours. Otherwise, the according command to remove the Edge Device is not available. In this case, the color of the Edge Device operating state is grey. Once the Edge Device is removed, you can reconnect the same Edge Device to the IEM. Also, if you want to change the configuration of an connected Edge Device, first you must remove the Edge Device from the IEM and then reconnect the Edge Device with the updated configuration to the IEM.

Procedure

1. Click the ⋮ icon of the Edge Device you want to remove from the IEM.
2. Click "Remove".
3. Confirm the removal by clicking "Remove".

   The Edge Device is removed from the IEM. When you want to reconnect the same Edge Device to the IEM, perform again the onboarding process as described in the "Connecting an Edge Device" section.

6.11 Storing an Edge Device state

Requirement

- The IE State Service is installed in the IEM-OS.

  You find general information on the IE State Service and requirements for storing IED states in the "Industrial Edge State Service (Page 137)" section.

Procedure

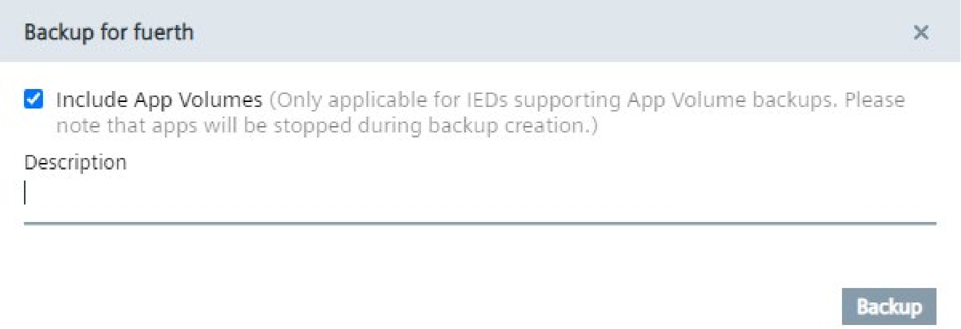
1. Click the ⋮ icon of the Edge Device for which you want to store the IED state.
2. Click the "System Commands > Backup" command.

   Note

   Backup availability

   The "Backup" command is only available if you have the according permissions.

   The "Backup" screen is displayed.

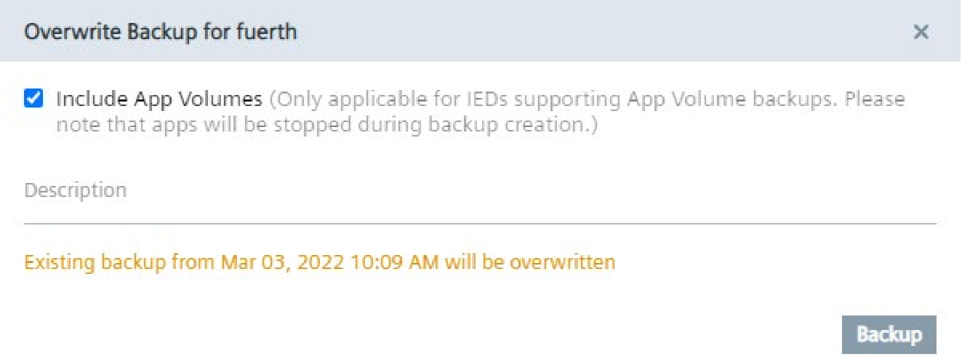
   

   Backup for fuerth

   ☑ Include App Volumes (Only applicable for IEDs supporting App Volume backups. Please note that apps will be stopped during backup creation.)

   Description

   If you already have stored an IED state of this Edge Device, the "Overwrite Backup" screen is displayed.

   Overwrite Backup for fuerth

   ☑ Include App Volumes (Only applicable for IEDs supporting App Volume backups. Please note that apps will be stopped during backup creation.)

   Description

   Existing backup from Mar 03, 2022 10:09 AM will be overwritten

   In this case, the previous IED state will be overwritten when you store a new IED state.

   By default, the "Include App Volumes" checkbox is enabled. By that, app volumes will be also stored, if the Edge Device supports it, when creating the backup.
3. If you do not want to also store app volumes, disable the checkbox.
4. In the "Description" input field, enter a description for the backup.

   The backup description will be displayed for each stored IED state and also when you want to restore an IED state.

5. To store the IED state, click "Backup".

   A backup job is being created and the "Backup" screen is displayed.

6. Click "Job Status".

   The "Job Status" screen is displayed. The status of the backup job is listed under the "Backups" tab.

   After the job is completed, the IED state is stored in the IEM. All stored IED states are listed under "Backups". You can manage all stored IED states as described in the "Backups" subsection.

Note

Storing IED data

App data and IED specific settings will not be stored.

6.12 Restoring an Edge Device state

When performing a restore, the Edge Device will be automatically cleaned up (via "Reset" system command). If an error occurs during the restore, the Edge Device will be cleaned too.

Requirement

- The IE State Service is installed in the IEM-OS.

  You find general information on the IE State Service and requirements for restoring IED states in the "Industrial Edge State Service (Page 137)" section.

- An IED state has been stored.

Procedure

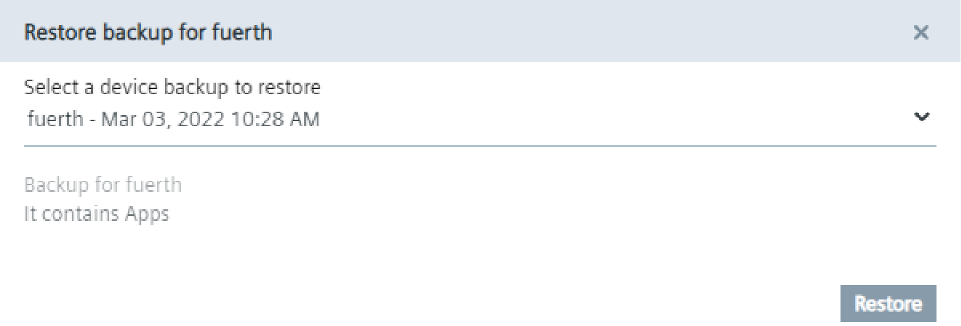
1. Click the ⋮ icon of the Edge Device for which you want to restore an IED state.
2. Click the "System Commands > Restore" command.

   Note

   Restore availability

   The "Restore" command is only available if you have the according permissions.

   The "Restore backup" screen is displayed.



Restore backup for fuerth

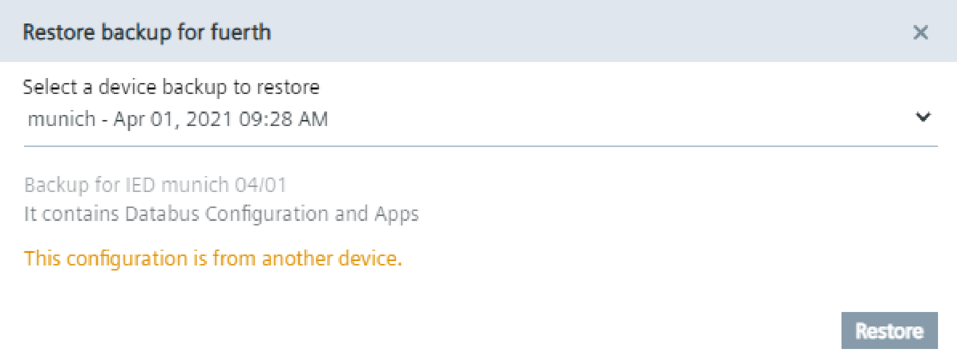
Select a device backup to restore
fuerth - Mar 03, 2022 10:28 AM

Backup for fuerth
It contains Apps

3. From the drop-down list, select the IED state which backup you want to restore.

   The backup description of the stored IED state is displayed below the drop-down list.

   You can also use the stored IED state of a different Edge Device for the target Edge Device.



Restore backup for fuerth

Select a device backup to restore
munich - Apr 01, 2021 09:28 AM

Backup for IED munich 04/01
It contains Databus Configuration and Apps

This configuration is from another device.

4. Click "Restore".

   A restore job is being created and the "Restore" screen is displayed.

5. Click "Job Status".

   The "Job Status" screen is displayed. The status of the restore job is listed under the "Backup" tab.

   After the job is completed, the IED state is restored on the Edge Device.

Note

Restoring IED data

App data and IED specific settings will not be restored. In addition, the IED-OS version may be outdated.

You can manage and also restore IED states as described in the "Backups" subsection.

6.13 Edge Device system commands

You execute a single Edge Device system command by clicking either the 🔧▾ icon or the ⋮ icon of an Edge Device and then selecting the required system command.
The following are the Edge Device system commands:

- Shutdown: Shutdown the selected Edge Devices
- Reboot: Reboot the selected Edge Devices
- Reset: Delete all user data and restore the original configuration from the configuration file
- Hard Reset: Delete all user data and configuration settings of the Edge Device and remove the Edge Device from the IEM
- Firmware Update: If available, update the firmware of selected Edge Devices (only available when you click the 🔧▾ icon)
- Backup: Store IED states of multiple Edge Devices
- Restore: Restore an IED state for multiple Edge Devices

Depending on your permissions, any of the Edge Device system commands are available or not.

By clicking the 🔧▾ icon and selecting 1 of the system commands, the according screen is displayed in which you select the Edge Devices for which you want to execute the system command. You have the possibility to execute the system command immediately or at a later time.

By clicking the ⋮ icon of an Edge Device and selecting 1 of the system commands, an according screen is displayed in which you choose whether to execute the system command immediately or at a later time.

6.13.1 Updating an Edge Device

You find the procedure and additional information on how to update an Edge Device, and other components, in the "Industrial Edge - Update Procedures (https://support.industry.siemens.com/cs/us/en/view/109801947)" manual.

6.13.2 Storing multiple Edge Device states

Requirement

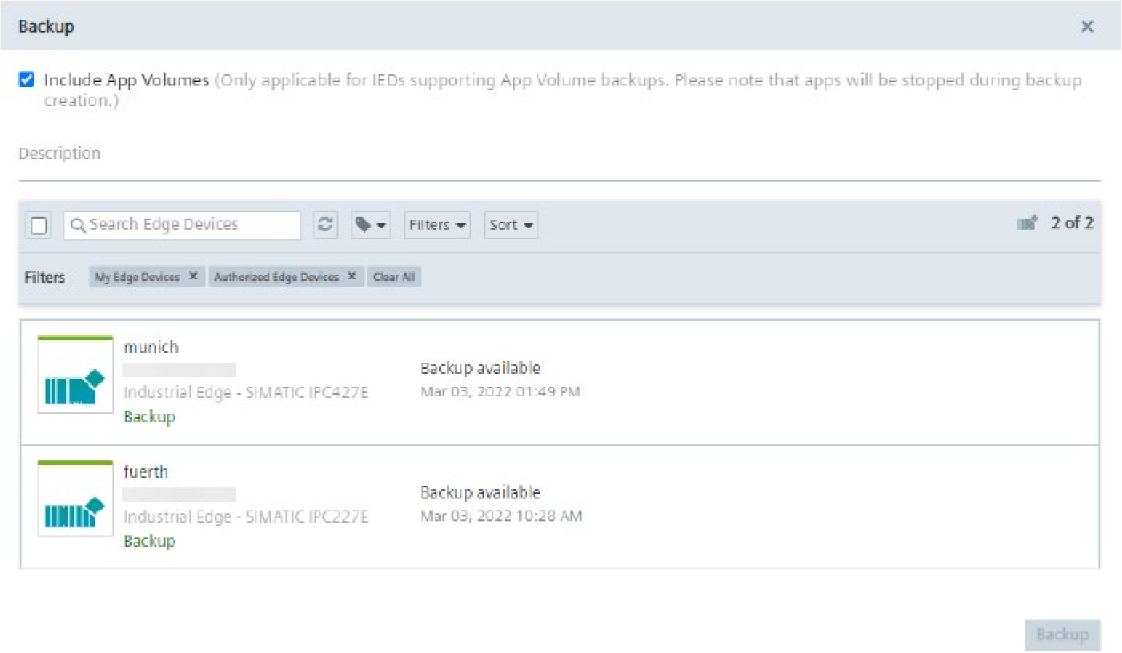
- The IE State Service is installed in the IEM-OS.

  You find general information on the IE State Service and requirements for storing IED states in the "Industrial Edge State Service (Page 137)" section.

Procedure

1. Click the icon and select the "Backup" command.

   The "Backup" screen is displayed.



Backup

☑ Include App Volumes (Only applicable for IEDs supporting App Volume backups. Please note that apps will be stopped during backup creation.)

Description

munich
[redacted]
Industrial Edge - SIMATIC IPC427E
Backup
Backup available
Mar 03, 2022 01:49 PM

fuerth
[redacted]
Industrial Edge - SIMATIC IPC227E
Backup
Backup available
Mar 03, 2022 10:28 AM

   If you have already stored an IED state of an Edge Device, "Backup available" is displayed in the row of the specific Edge Device. If no IED state of an Edge Device has been stored yet, "No backup available" is displayed.

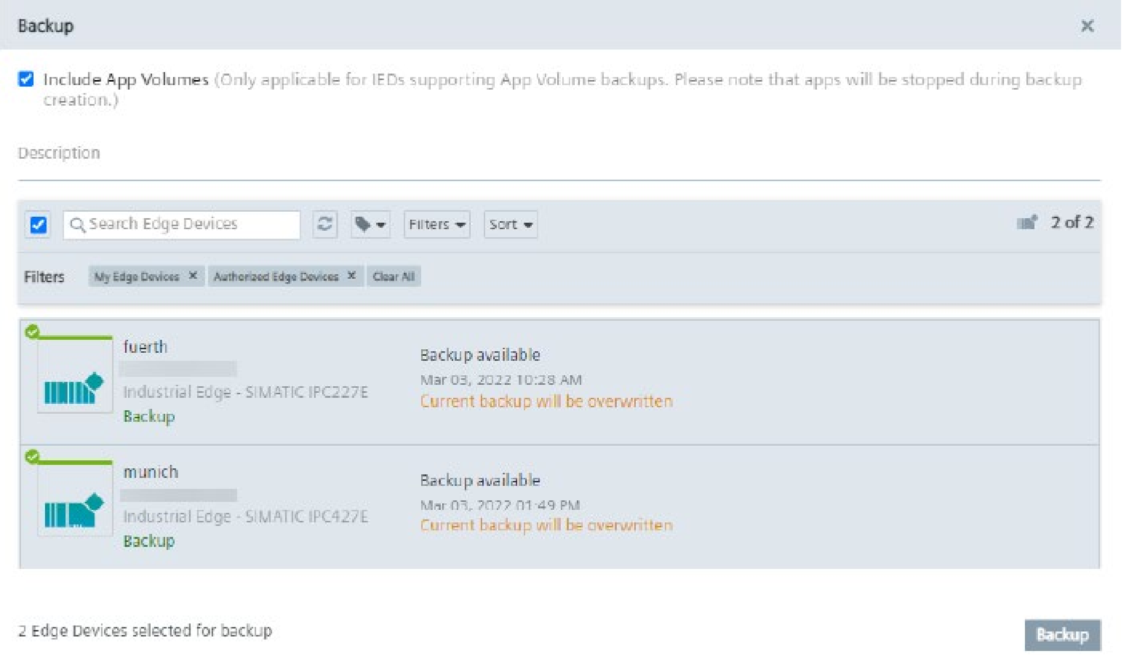
   By default, the "Include App Volumes" checkbox is enabled. By that, app volumes will be also stored, if the Edge Device supports it, when creating the backup.

2. If you do not want to also store app volumes, disable the checkbox.

3. In the "Description" input field, enter a description for the backup, if required.

   The backup description will be displayed for each stored IED state and also when you want to restore an IED state.

4. Select the Edge Devices whose IED states you want to store for a Disaster Strategy.



☑ Include App Volumes (Only applicable for IEDs supporting App Volume backups. Please note that apps will be stopped during backup creation.)

fuerth
Industrial Edge - SIMATIC IPC227E
Backup
Backup available
Mar 03, 2022 10:28 AM
Current backup will be overwritten

munich
Industrial Edge - SIMATIC IPC427E
Backup
Backup available
Mar 03, 2022 01:49 PM
Current backup will be overwritten

2 Edge Devices selected for backup

   Already stored IED states of Edge Devices will be overwritten.

5. Click "Backup".

   A backup job is being created for each Edge Device and the "Backup" screen is displayed.

6. Click "Job Status".

   The "Job Status" screen is displayed. The status of each backup job is listed under the "Backups" tab.

   After the job is completed, the IED state of the selected Edge Device is stored. All stored IED states are listed under "Backups". You can manage all stored IED states as described in the "Backups" subsection.

Note

Storing IED data

For limitations and general information on the IE State Service, refer to the "Industrial Edge State Service (Page 137)" subsection.

6.13.3 Restoring IED states of multiple Edge Devices

When performing a restore, the Edge Device will be automatically cleaned up (via "Reset" system command). If an error occurs during the restore, the Edge Device will be cleaned too.

Requirement

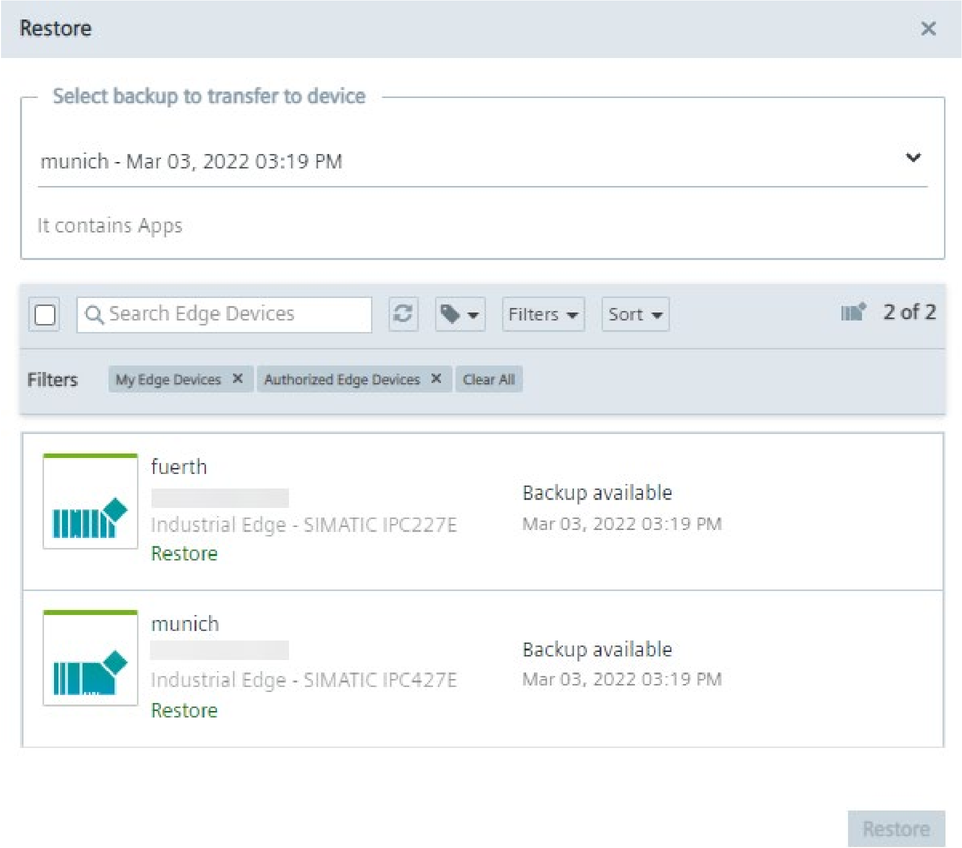
- The IE State Service is installed in the IEM-OS.

  You find general information on the IE State Service and requirements for restoring IED states in the "Industrial Edge State Service (Page 137)" section.
- An IED state has been stored.

Procedure

1. Click the 🔧▾ icon and select the "Restore" command.

   The "Restore" screen is displayed.



Restore

Select backup to transfer to device: munich - Mar 03, 2022 03:19 PM

It contains Apps

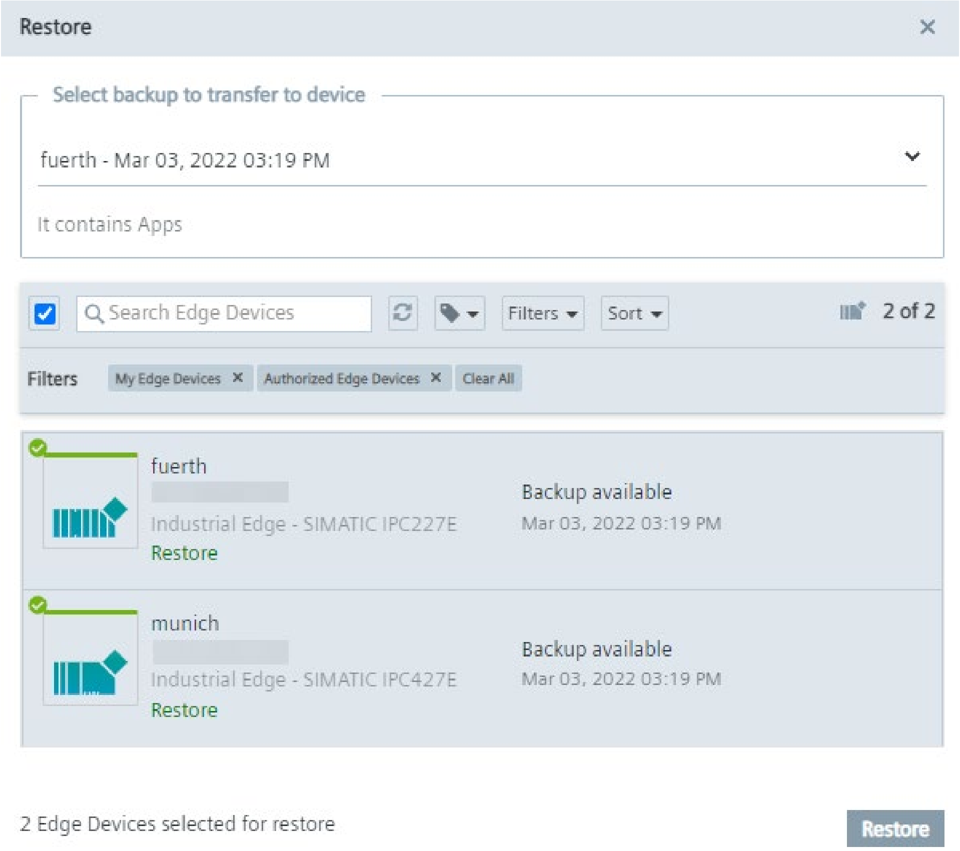
fuerth
Industrial Edge - SIMATIC IPC227E
Backup available
Mar 03, 2022 03:19 PM

munich
Industrial Edge - SIMATIC IPC427E
Backup available
Mar 03, 2022 03:19 PM

2. Select the required IED state from the drop-down list.

   Information on the stored data is displayed below the drop-down list.

3. Select the Edge Devices which you want to restore to the selected IED state.



Restore

Select backup to transfer to device

fuerth - Mar 03, 2022 03:19 PM

It contains Apps

fuerth
[redacted]
Industrial Edge - SIMATIC IPC227E
Restore
Backup available
Mar 03, 2022 03:19 PM

munich
[redacted]
Industrial Edge - SIMATIC IPC427E
Restore
Backup available
Mar 03, 2022 03:19 PM

2 Edge Devices selected for restore

All selected Edge Devices will be restored to the IED state that you have selected from the drop-down list.

4. Click "Restore".

   A restore job is being created for each Edge Device and the "Restore" screen is displayed.

5. Click "Job Status".

   The "Job Status" screen is displayed. The status of each restore job is listed under the "Backups" tab.

   After the job is completed, the corresponding Edge Devices are restored to the selected IED state.

   You can manage and also restore IED states as described in the "Backups" subsection.

Note

Restoring IED data

For limitations and general information on the IE State Service, refer to the "Industrial Edge State Service (Page 137)" subsection.

Backups 7

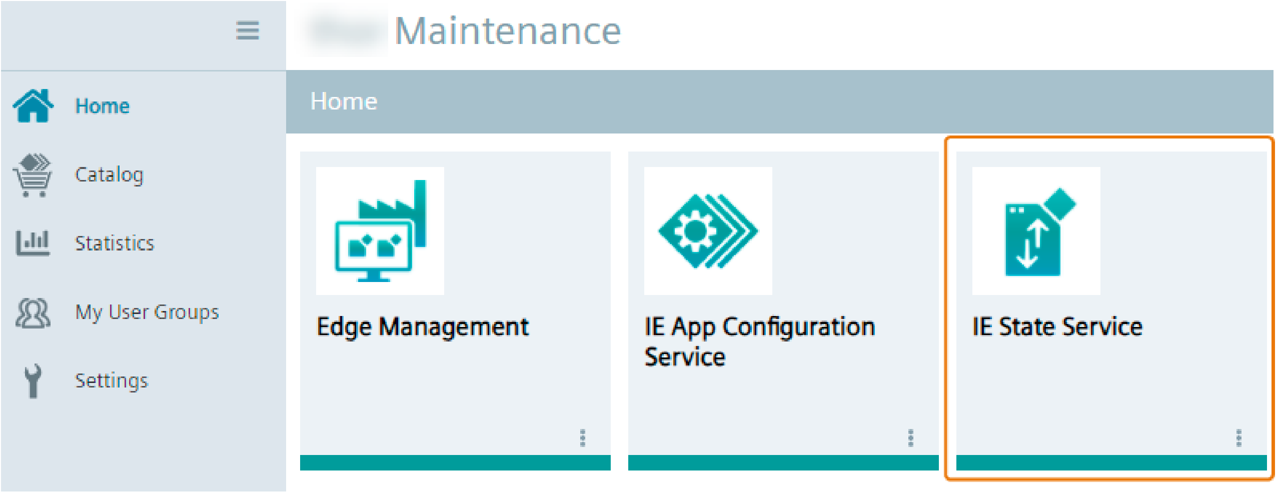
7.1 Industrial Edge State Service

7.1.1 Overview

To minimize the impact during a disaster scenario, the Industrial Edge State Service provides the possibility to implement Disaster Recovery (DR) strategies based on your DR plan respectively requirements. This may include minimizing the down time as well as loss of data. With the IE State Service, you can store the IED state of an Edge Device on the IEM. In case of any occuring errors respectively failures in the Edge Device, you can choose and restore a desired stored IED state on the Edge Device. Only 1 IED state per Edge Device can be stored in the IEM.

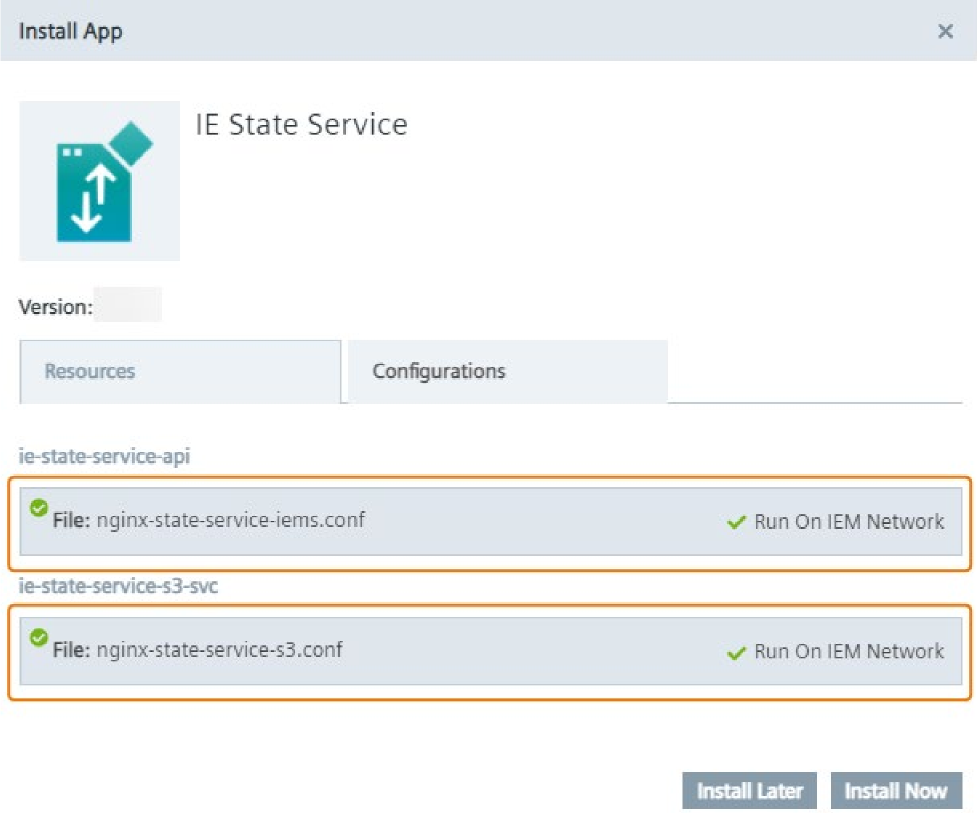
You can store and restore an IED state of 1 Edge Device as described in the following subsections or store and restore IED states for multiple Edge Devices as described in the "Edge Device system commands (Page 132)" subsection.

After you have successfully installed the IE State Service, the app is listed in the "Home" screen of your Maintenance UI.



7.1.2 Installation

The installation of the IE State Service (IESS) will be automatically initiated in your IEM-OS during the first set up of the system. During the installation process, select and ensure that the available resource files in the "Resources" tab are activated.



Install App

IE State Service

Version:

ie-state-service-api

File: nginx-state-service-iems.conf ✓ Run On IEM Network

ie-state-service-s3-svc

File: nginx-state-service-s3.conf ✓ Run On IEM Network

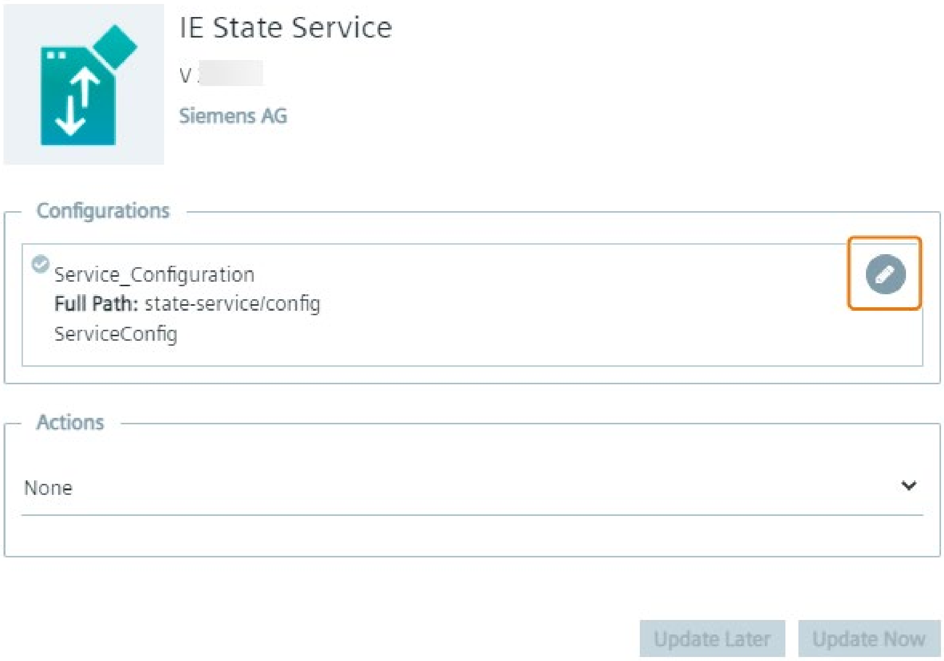
Furthermore, you have the possibility to configure the IESS in the "Configurations" tab which includes the storage size and the provided monitoring service.

7.1.3 Configuration

Note

Siemens recommends adjusting the configuration upon the initial installation of the IESS because only changes to the monitoring service will be applied during an update of the IESS or an update of the IESS configuration.

To adjust the IESS configuration during its installation or during an update of the IESS, click the edit button.



IE State Service
V
Siemens AG

Configurations

Service_Configuration
Full Path: state-service/config
ServiceConfig

Actions

None

7.1.3.1 Storage size

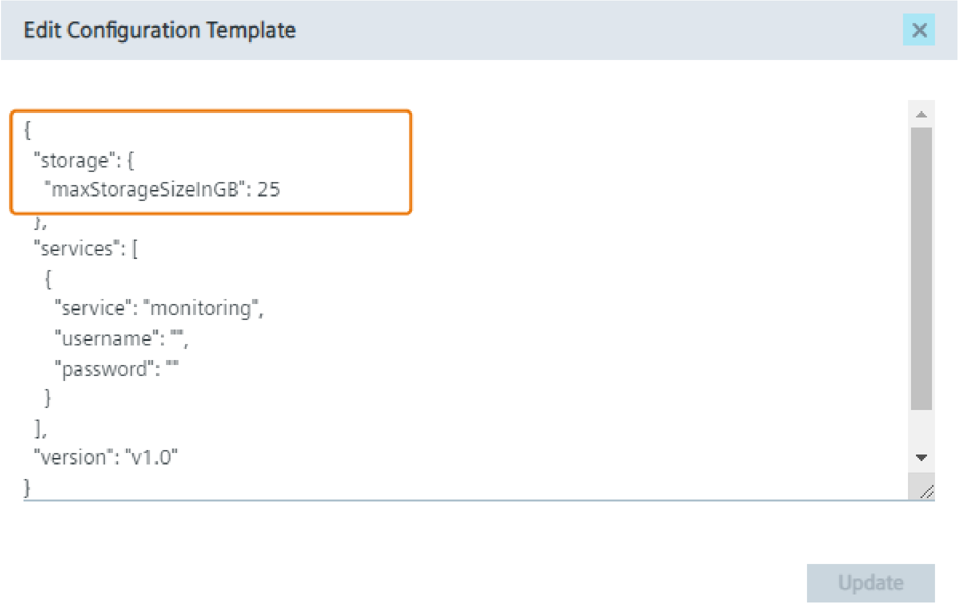
By default, the IE State Service reserves 25 GB of storage size. Based on your demand, it is possible to adjust this value in the configuration template.

Note

It is only possible to adjust the storage size upon the initial installation of the IESS. If it is necessary to adjust the storage size afterwards, you must reinstall the IESS. Be aware that all existing backups will be removed during this process.

Note

You also have the possibility to add additional storage to the IEM as described in the "Adding additional storage to the IEM (Page 41)" subsection.



Edit Configuration Template

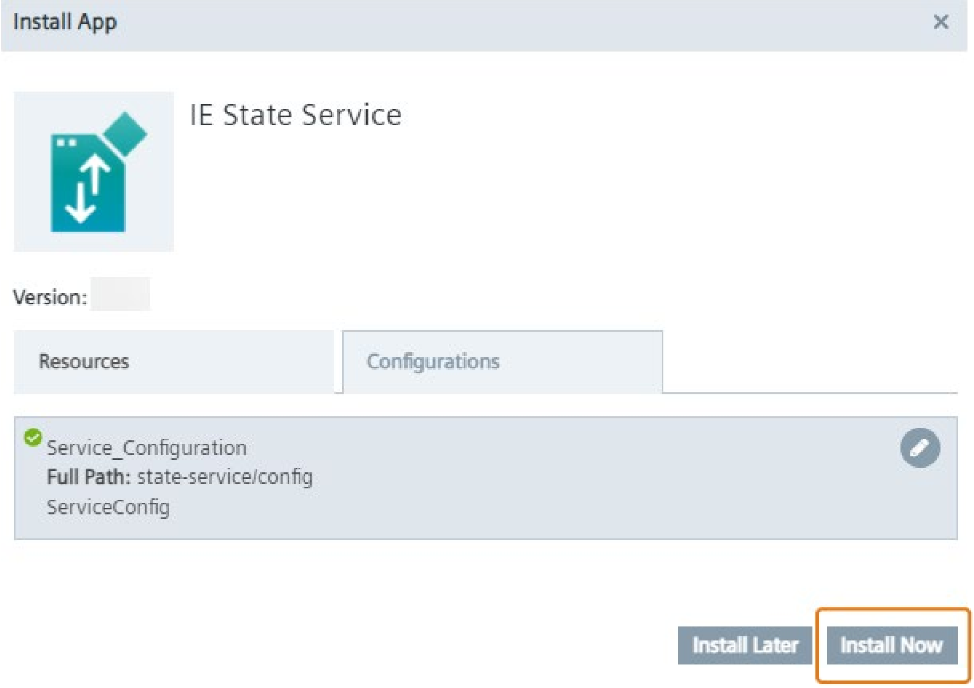
```
{
 "storage": {
  "maxStorageSizeInGB": 25
 },
 "services": [
  {
   "service": "monitoring",
   "username": "",
   "password": ""
  }
 ],
 "version": "v1.0"
}
```

To change the IE State Service storage size, enter your required value in the "maxStorageSizeInGB" input field.

Note

If an invalid value is entered, for example more disk space than available, the IE State Service will not start. This error will be displayed in the cluster logs downloadable in the Maintenance UI.

Save the changes by clicking "Update" and install the IE State Service by clicking "Install Now".



Install App

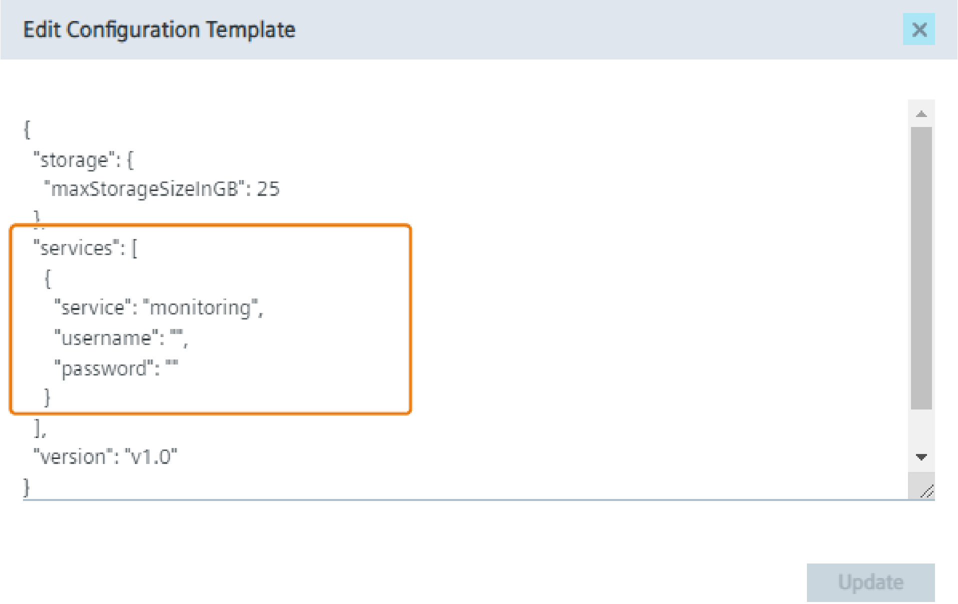
IE State Service

Version:

Service_Configuration
Full Path: state-service/config
ServiceConfig

7.1.3.2 Monitoring service

The monitoring service enables metrics tracking for more detailed service information. To enable the monitoring service, you must configure a basic authentication mechanism in the configuration template.



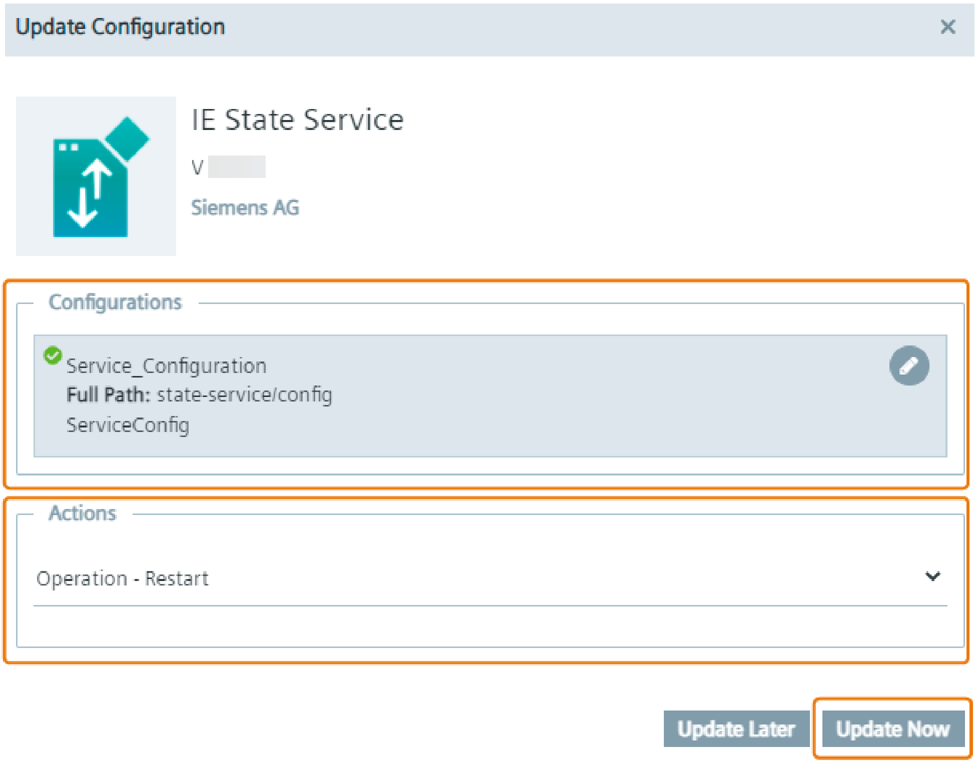
```
{
 "storage": {
  "maxStorageSizeInGB": 25
 },
 "services": [
  {
   "service": "monitoring",
   "username": "",
   "password": ""
  }
 ],
 "version": "v1.0"
}
```

Enter a username and a strong password.

Note

If username and password are empty respectively not set, the monitoring service will not be available.

Save the changes by clicking "Update" and select the configuration. If you update the IESS configuration, you must also select "Operation - Restart" in the "Actions" drop-down list for the IESS to implement the changes that you made to the configuration.



Update Configuration

IE State Service

V [redacted]

Siemens AG

Configurations

Service_Configuration
Full Path: state-service/config
ServiceConfig

Actions

Operation - Restart

This is not required when you install or update the IESS itself.

Click "Install Now" or "Update Now" respectively. After successful installation of the IE State Service respectively after successfully restarting the IE State Service, open the metrics tracking under "https://<portal-url>/state-service/api/v1/metrics".

When you open the metrics, you must enter the credentials that you set in the configuration. The metrics can be integrated with monitoring solutions, for example Prometheus.

Metrics information

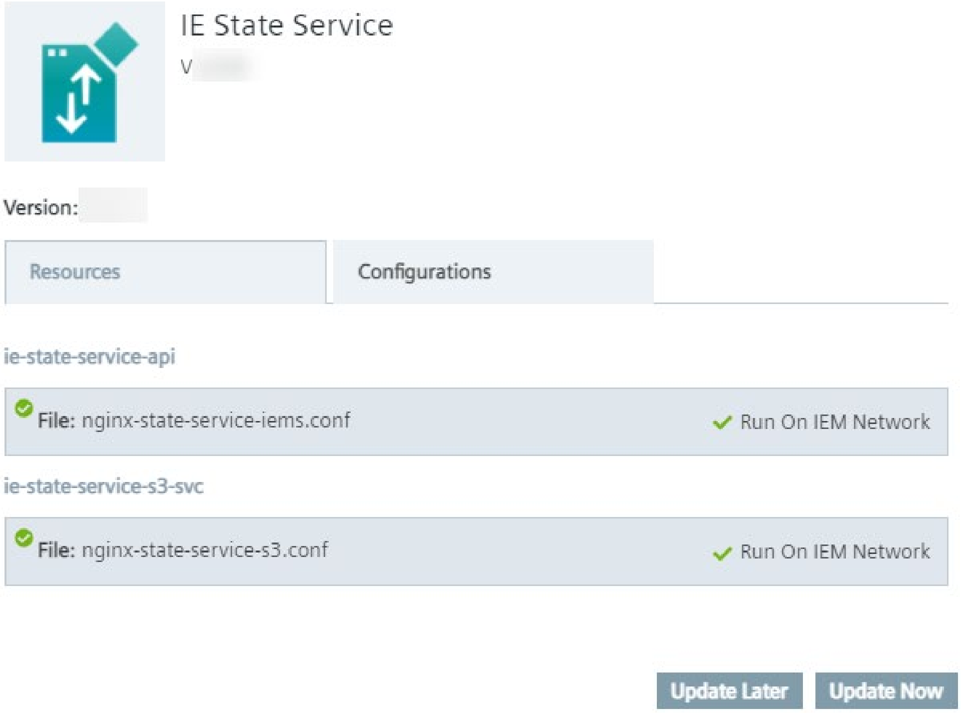
The following are examples of information given inside the metrics.

Key	Description
process_uptime_seconds	Time in seconds since the process is running
state_service_store_requests_count	Number of store requests
state_service_restore_requests_count	Number of restore requests
state_service_targets_requests_count	Number of resource requests
state_service_store_requests_error_count	Number of store requests returning an error
state_service_config_storage_size	Maximum configured storage size for IE State Service backups
state_service_storage_size	Storage size for IE State Service backups.

7.1.4 Updating the IE State Service

If you update your IEM, in which the IE State Service was not installed to a newer version, you must install the IE State Service manually (Page 150) from the catalog in the Maintenance UI.

To update or check if an update for the IE State Service is available, click the ⋮ icon and then click the "Check Update" command. If an update is available, the "Update Application" screen is displayed. The current app version is displayed below the app name, the app version you update to is displayed below the app icon. Select respectively ensure that the available resource files in the "Resources" tab are activated.



IE State Service
V

Version:

Resources | Configurations

ie-state-service-api

File: nginx-state-service-iems.conf ✓ Run On IEM Network

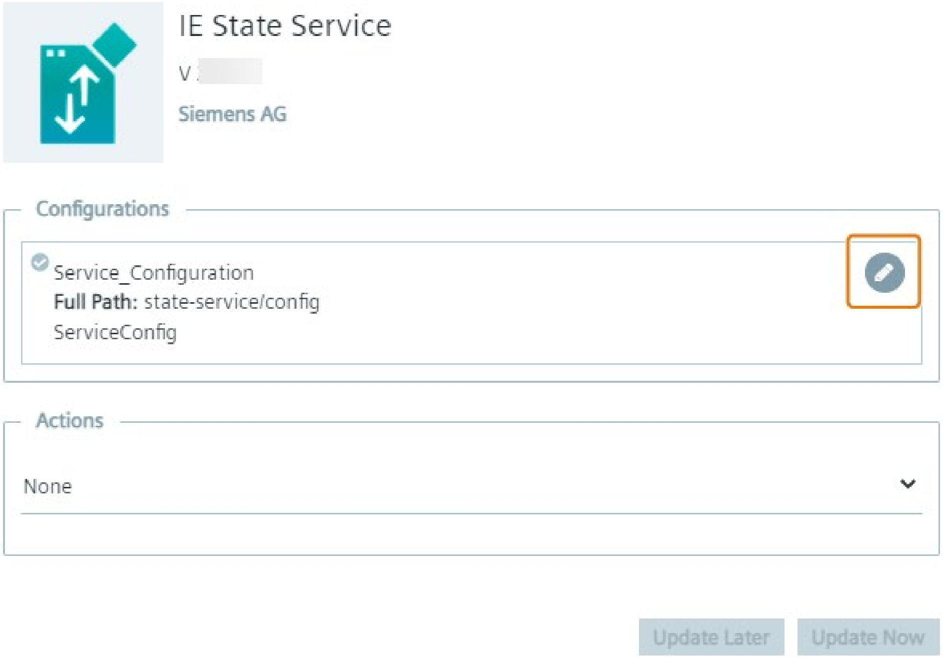
ie-state-service-s3-svc

File: nginx-state-service-s3.conf ✓ Run On IEM Network

If required, you can also make further adjustments in the "Configurations" tab. For detailed information, refer to the "Configuration (Page 139)" subsection.

7.1.5 Updating the configuration

If the IESS is already installed, you can edit the configuration at a later time by clicking "Update Configuration" in the Maintenance UI. To edit the configuration, click the edit button.



IE State Service

V

Siemens AG

Configurations

Service_Configuration
Full Path: state-service/config
ServiceConfig

Actions

None

You find information on how to update the configuration in the "Configuration (Page 139)" subsection.

7.1.6 Functionality

Requirements for storing an IED state

- The IE State Service is installed in the IEM-OS.
- You have the permission to store an IED state.

Note

Permissions

Only the owner and users who are added to the "edgedevices.co-admin" admin group role of the specific Edge Device have permissions to store an IED state.

Note

Resiliency

Resiliency is the ability of the IE State Service to ignore errors that occurred during store execution. For example, non-existent resources can be skipped.

Requirements for restoring an IED state

- The IE State Service is installed in the IEM-OS.
- You have the permission to restore an IED state.
- When you restore an IED state of a specific Edge Device Type to an Edge Device of a different Edge Device Type, ensure that the hardware specifications of the stored Edge Device Type match the hardware specifications of the target Edge Device Type.

Note

If the amount of maximum running apps on the target Edge Device is exceeded by the backup, not all apps will be started during the restore process.

Storable resources

The following table shows the resources that can be stored (and restored) as well as the resources that are not stored in an IED state:

Resources	Included in the IED state	Not included in the IED state
Apps	• Apps running on the IED (App ID will be persisted)	• The *.app file is not persisted
App volumes	App volumes of the following volume types: • Host • Logs • Configs • Auth Service	• App volumes of the following volume types: – TMPFS – Openpipe – Socket – Internal – Data Storage – Events Service • Volume files with the following file mode: – ModeNamedPipe: Named pipe (FIFO) – ModeDevice: Device file – ModeCharDevice: Unix character device, when ModeDevice is set – ModeSocket: Unix socket domain – ModeIrregular: Non-regular file
App configurations	• Versioned: Configuration ID • Unversioned: Configuration file • Templated and Schema-based: Configuration ID and modifications	• Versioned: Configuration file • Templated and Schema-based: Configuration file

Resources	Included in the IED state	Not included in the IED state
System App configurations	• System App configurations which are available during the moment of the store operation • The configuration will be stored and used during the restore process without any Edge Device specific settings such as Edge Device name	System Apps will not be deployed upon restore, app resources are required to be used for that
App states	App state (running/stopped)	-

Note

To successfully store app volumes, all apps are being stopped temporary and will be restarted after the backup creation.

Note

Apps are the basis for every backup. Therefore, if there are no apps that can be stored, no backup will be created.

Restore process in detail

By default, when you restore a previously created IED state in the IEM, all resources in the created IED state will be selected to restore. That means, the IE State Service checks whether all resources stored in the created IED state can be restored. The IE State Service will not start the restore process and responds with an error message when 1 of the following applies:

- App is not published anymore
- App is deleted
- App version is not available anymore
- System App Configurator is not available
- Edge Device does not support backup and restore for app volumes

The status message displays the resource which caused the error.

If any of the resources cannot be restored, the restore process will result in an error. In this case, the Edge Device will not be reset.

If all resources can be restored, the IE State Service starts the restore process. The IE State Service triggers an Edge Device reset to clean up the state of the Edge Device. After the Edge Device is reset, the restore conditions will be checked again and the restore process will continue. If any of the resources fail during the restore process, the restore process ends with the "Error" status message. The Edge Device will be reset again. If all resources succeed, the restore process will be completed with the "Success" status message.

Jobs on the Edge Device

During the store and restore process, different jobs can be triggered on the Edge Device.

Job on the Edge Device	Trigger time
Reset	• Prior to restore process (to have an empty state) • After an error during the restore process • In case of an error prior to restore process, reset will not be triggered
App installation	During restore process
Edge Device Backup	During store process
Edge Device Restore	During restore process

Job messages

When storing or restoring an IED state, the following job messages can occur for the respective jobs:

Operation	Job message	Description
Store	In progress	• Store is in progress
Store	Success	• Store was successful • All required resources have been stored
Store	Partially succeeded	• Store was partially successful • No specific resources were selected during the store operation and some resources were unsuccessfully stored • You can check the stored resources of a partially succeeded backup in the "Backups" section of that respective backup (tile view)
Store	In cancelation	• Store is being canceled
Store	Canceled	• Store has been canceled • Incomplete backups are cleaned up
Store	Error	• Store has failed • A detailed error message including error reason is displayed
Restore	In progress	• Restore is in progress
Restore	Success	• Restore was successful • All required resources have been restored
Restore	In cancelation	• Restore is being canceled
Restore	Canceled	• Restore has been canceled • The Edge Device will be reset
Restore	Error	• Restore has failed • A detailed error message about the resource status is displayed

Note

The jobs on the Edge Device (Job Status - System) are subtasks that are triggered by the IE State Service and have direct influence on the status of the backup or restore job (Job Status - Backups). Therefore, a failure of the subtasks usually leads to a failure of the superior job. However, notice that a backup job (Job Status - Backups) can be completed and partially successful despite of a fail of the "Edge Device Backup" job (Job Status - System), for example due to a time out. In this case, the failed subtasks represents an unsuccessfully stored resource within the backup job.

7.1.7 Limitations on IE State Service

Following are the limitations on the IE State Service.

Storage size

As described in the "Configuration (Page 139)" subsection, it is only possible to set the storage size during the installation of the IESS. Any later change requires an uninstall of the IESS which also results in the deletion of all available backups.

Compatibility

IE State Service Version	IEDK & IEM Version	Limitation
> V2.5.0	IEDK > V1.5.0-3 IEM > V1.4.6	If apps were stored while being stopped, they will be installed in stopped state. Running apps will run again.
< V2.5.0	IEDK < V1.7.0-4 IEM < V1.6.3	Store and restore of app volumes is not available
< V2.2.0	IEDK < V1.5.0-3 IEM < V1.4.6	Store and restore of the app's state is not available

Apps

- Apps which are not available respectively which are removed from the catalog of the IEM cannot be restored, the operation will result in an error.
- Users who do not possess the "management.admin.co-admin" role in the IEM are only able to restore backups containing apps when the needed app version the latest available version in the catalog of the IEM is.

App configurations

- For IEM V1.0 and V1.1, app configurations of the "unversioned configuration" type are not included in an IED state and will be omitted during storing respectively restoring.
- App configurations of the "unversioned configuration" type from IEM V1.0 or V1.1 are not getting restored when performing a restore operation in newer IEM versions.
- Instead of restoring configuration file names of the "unversioned configuration" type, configuration IDs are used as file names.
- App configurations which are not available respectively which are removed from the app cannot be restored, the operation will result in an error.

User and roles

- Only the owner and the Co-Admin of the Edge Device can initiate a store or restore process.
- The initiating user must possess the right permission to gain access to all target resources. The initiator must be for example the owner or co-owner of projects containing apps which are installed on the Edge Device on which the store or restore operation is performed.
- To restore backups containing apps with an older version than the latest available version in the catalog of the IEM, the initiating user must be member of an admin group that posses the "management.admin.co-admin" role.

Edge Devices

- The settings (proxy, system settings, users) on the Edge Device itself will be neither stored nor restored.
- During the backup and restore process of app volumes, apps running on the Edge Device will be stopped automatically. If you manually start apps through the Edge Device UI during the backup or restore process, errors might occur resulting in no properly backed up respectively restored app volumes. To avoid this, do not manually start apps during the backup or restore process.

Backups

Backups are related to Edge Devices. If an Edge Device was hard reset or deleted from the IEM, the backup cannot correlate to the Edge Device. Only a connection between the ID of the Edge Device and the performed backup is established which is only visible for admin users.

Therefore, if you want to restore an IED state of an Edge Device that is not existent anymore, the user who is triggering the restore operation must have the "edgedevices.state.store" respectively "edgedevices.state.restore" permissions and the "Admin" role in the IEM. This limitation is since only admin users have access to all IED states, even if Edge Devices are not onboarded anymore. As workaround, the Edge Device can be shared with an admin user who can restore the chosen IED state on that Edge Device.

Available information

In addition to the requirements to have the permissions to either store or restore an IED state, the following table shows the available information that are displayed by the IE State Service depending on the user permissions:

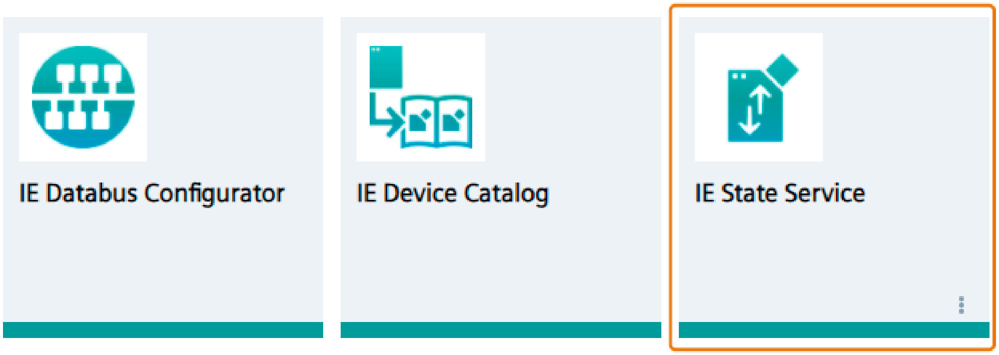
User	IED states	Status	Storable resources
Authenticated user	No IED states	No status	All storable resources
User with the "edgedevices.state.store" / "edgedevices.state.restore" permission	All IED states from Edge Devices for which the user is authorized	Every status associated with Edge Devices for which the user is authorized	All storable resources
Edge Device owner	All IED states from Edge Devices which the user owns	Every status associated with Edge Devices which the user owns	All storable resources
Admin user of the IEM	All IED states within the system	No status	All storable resources

7.1.8 Installing the IE State Service manually

The following procedure is only requried for installing the IE State Service on an existing IEM V1.0 or V1.1 or after you updated an existing IEM V1.0 or V1.1 without installed IE State Service to a newer version.

Procedure

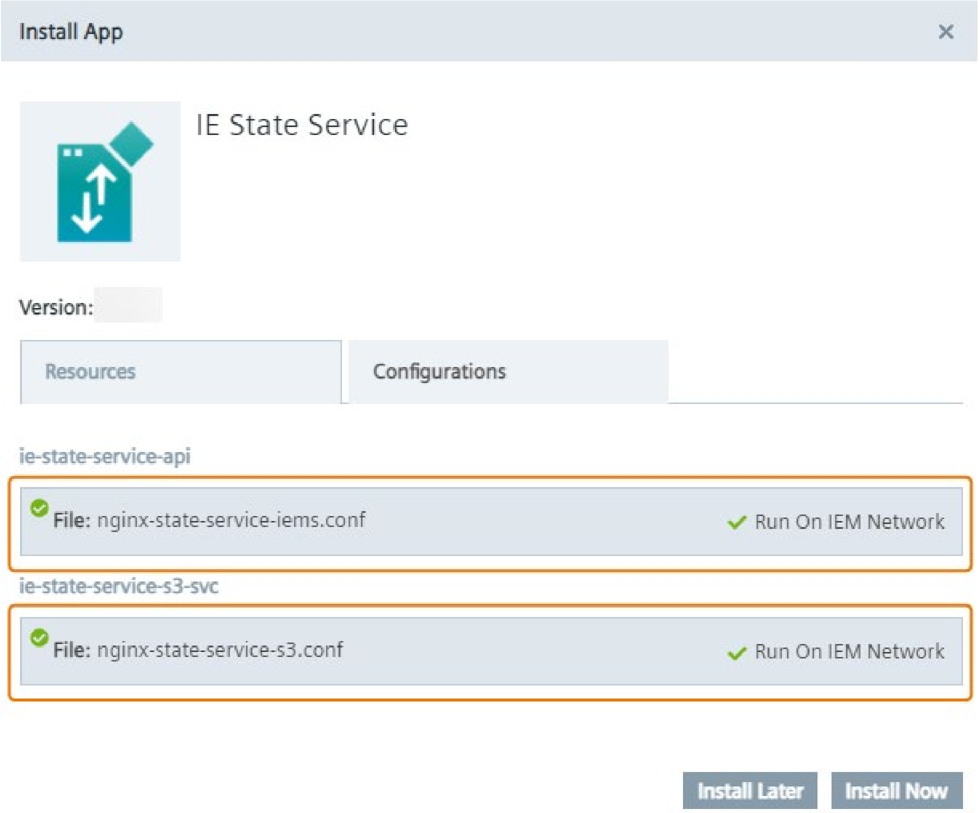
1. Open and log into the Maintenance UI.
2. In the navigation menu, click "Catalog".
3. Click the "IE State Service" app.



The "Install App" screen is displayed.

The app version you install is displayed below the app icon.

4. Ensure that the available resource file is activated.



Install App

IE State Service

Version:

ie-state-service-api

File: nginx-state-service-iems.conf ✓ Run On IEM Network

ie-state-service-s3-svc

File: nginx-state-service-s3.conf ✓ Run On IEM Network

5. If required, enable the monitoring service of the IE State Service in the "Configurations" tab.

   You find the procedure on enabling the monitoring service and further information on the service in the "Monitoring service" subsection.

6. Click "Install Now" to install the app.

   An installation job is created. After the job is completed, the IE State Service is successfully installed in your IEM-OS. You can now store and restore IED states.

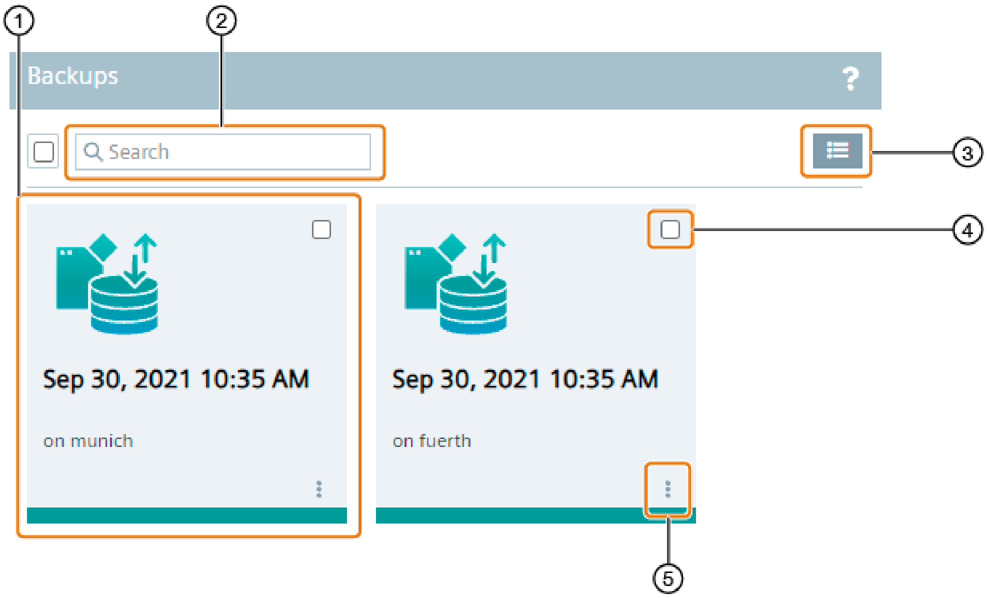
7.2 Overview

Requirement

To use the "Backups" menu item and its functionalities, the IE State Service must be installed in the IEM-OS.

Stored IED states

The "Backups" screen lists all stored IED states that can be again used for restoring an IED state. The tile view of the "Backups" screen is displayed as follows for example:



① Stored IED state containing following information:

- Backup date and time
- Target Edge Device

② Search bar: Enter a keyword to search for an IED state and press <Enter>

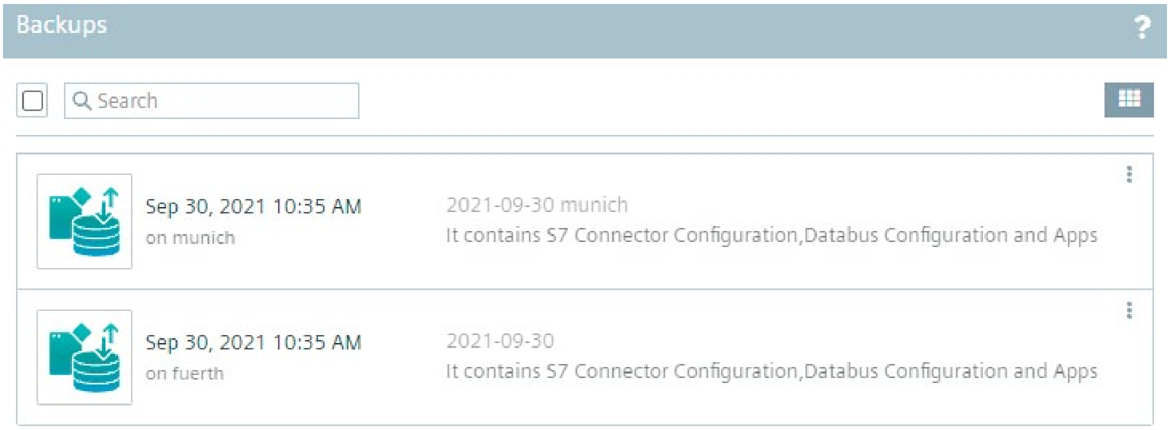
③ Switch to list view and back to tile view

④ Select respective IED state

⑤ IED state commands

When you move the cursor over a tile, the backup description and information on the stored data will be displayed as tooltip.

By clicking the ☰ icon, you switch to the list view, as displayed below for example:



Sep 30, 2021 10:35 AM
on munich
2021-09-30 munich
It contains S7 Connector Configuration,Databus Configuration and Apps

Sep 30, 2021 10:35 AM
on fuerth
2021-09-30
It contains S7 Connector Configuration,Databus Configuration and Apps

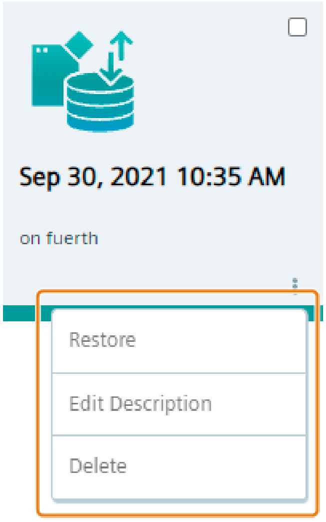
A stored IED state in the list view contains by default the backup description and information on the stored data in its row.

Deleting multiple IED states

When you select 1 or more IED states, the 🗑 icon is enabled through which you delete the selected IED states.

7.3 IED state commands

By clicking the ⋮ icon, the IED state commands are displayed.



Following commands are available:

- Restore: Restore Edge Devices to this stored IED state
- Edit description: Add, update or delete a description
- Delete: Delete the IED state

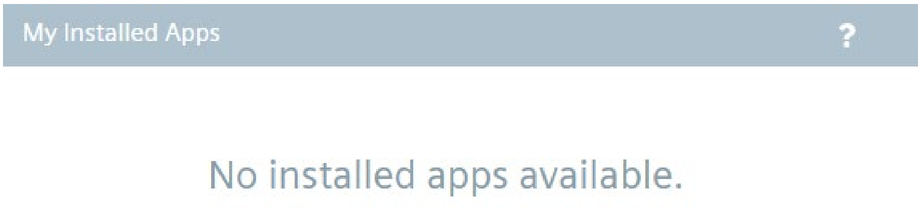
My Installed Apps

8

8.1 Overview

The "My Installed Apps" screen gives you an overview of all apps that are installed on your onboarded Edge Devices. Also, you manage and get additional information of these apps.

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



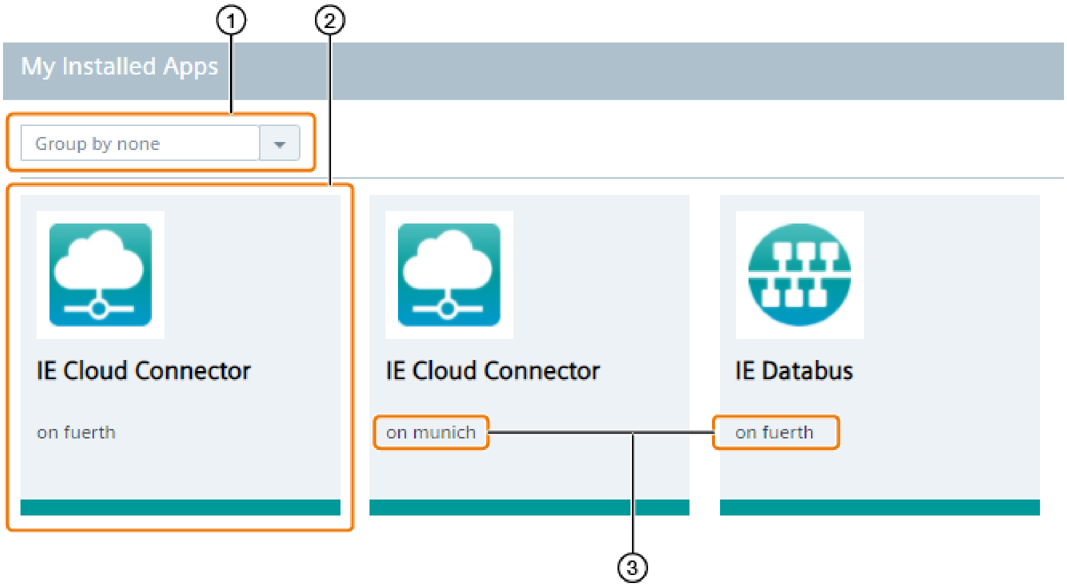
My Installed Apps

No installed apps available.

Once you have installed 1 or more apps on an Edge Device, the installed apps are displayed and you can switch between a non-grouping view of the installed apps and a grouped by Edge Devices view.

Grouped by none view

When you select "None" from the drop-down list, all installed apps are not grouped but just listed and are displayed as follows for example:



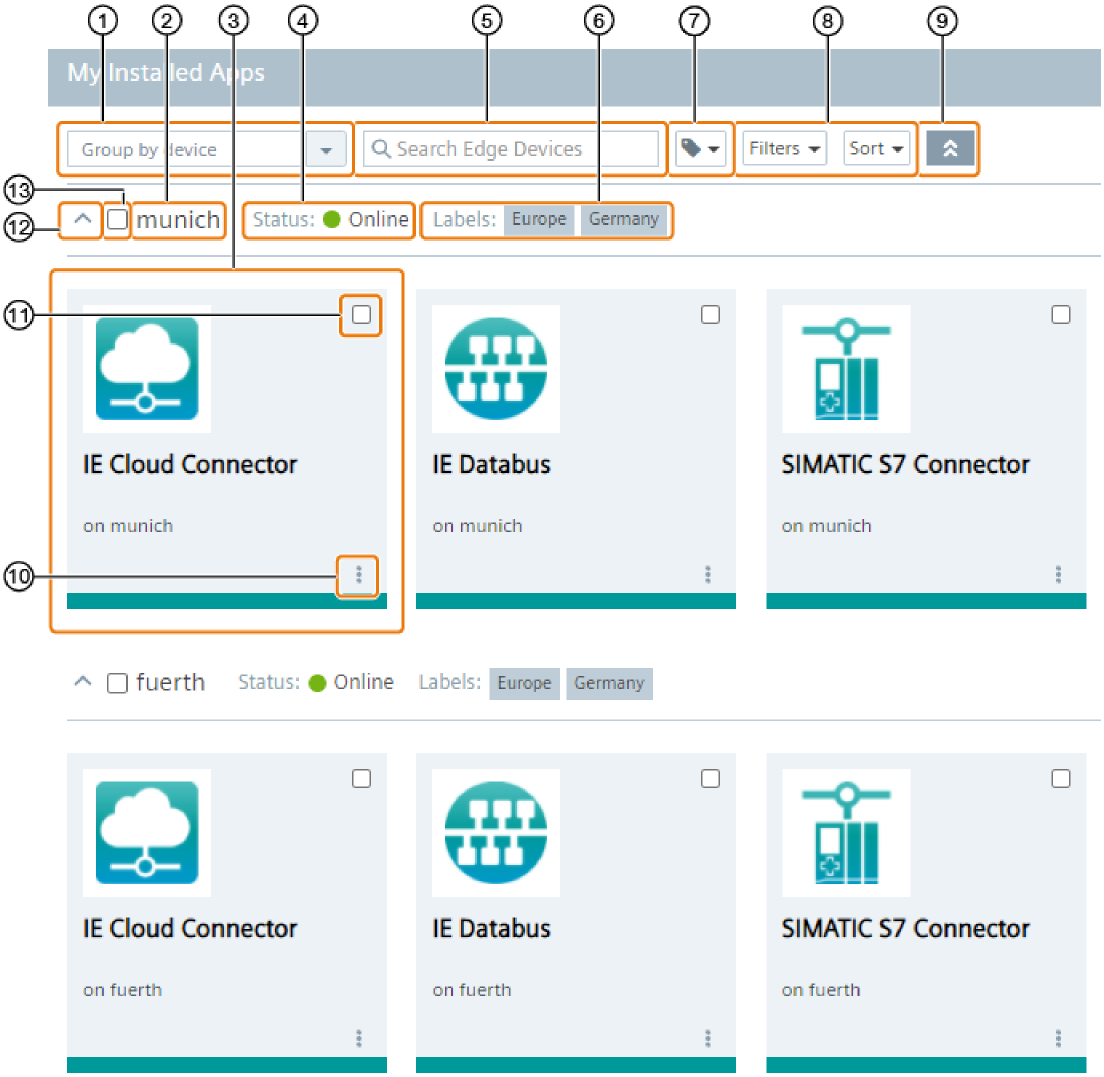
① Switch between grouped by Edge Devices view and grouped by none view

② Installed app

③ Edge Device on which the app is installed

Grouped by Edge Devices view

When you select "Device" from the drop-down list, the installed apps are grouped by the Edge Devices on which they are installed and are displayed as follows for example:



① Switch between grouped by Edge Devices view and grouped by none view
② Edge Device on which the app is installed
③ Installed app
④ Status of the Edge Device
⑤ Search for Edge Devices
⑥ Labels assigned to the Edge Device
⑦ Search for labels assigned to Edge Devices
⑧ Filter and sort grouped by Edge Device view
⑨ Hide and display all installed apps
⑩ Check app events and update and delete app configurations
⑪ Select respective app

⑫ Hide and display all installed apps on the respective Edge Device

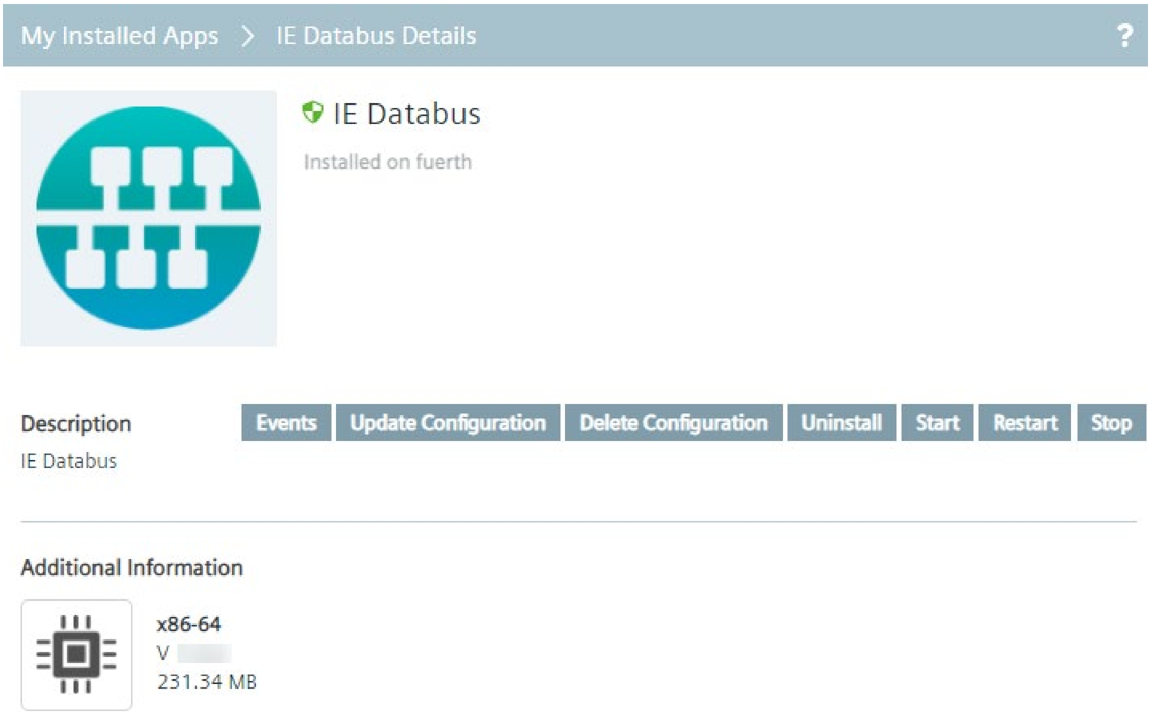
⑬ Select all apps installed on the respective Edge Device

8.2 Managing an app

Grouped by none view

When you click the tile of an app, you open the app details in which you manage the installed app on the specific Edge Device.

The following figure shows the details of the "IE Databus" app as an example:



My Installed Apps > IE Databus Details

IE Databus

Installed on fuerth

Description

IE Databus

Additional Information

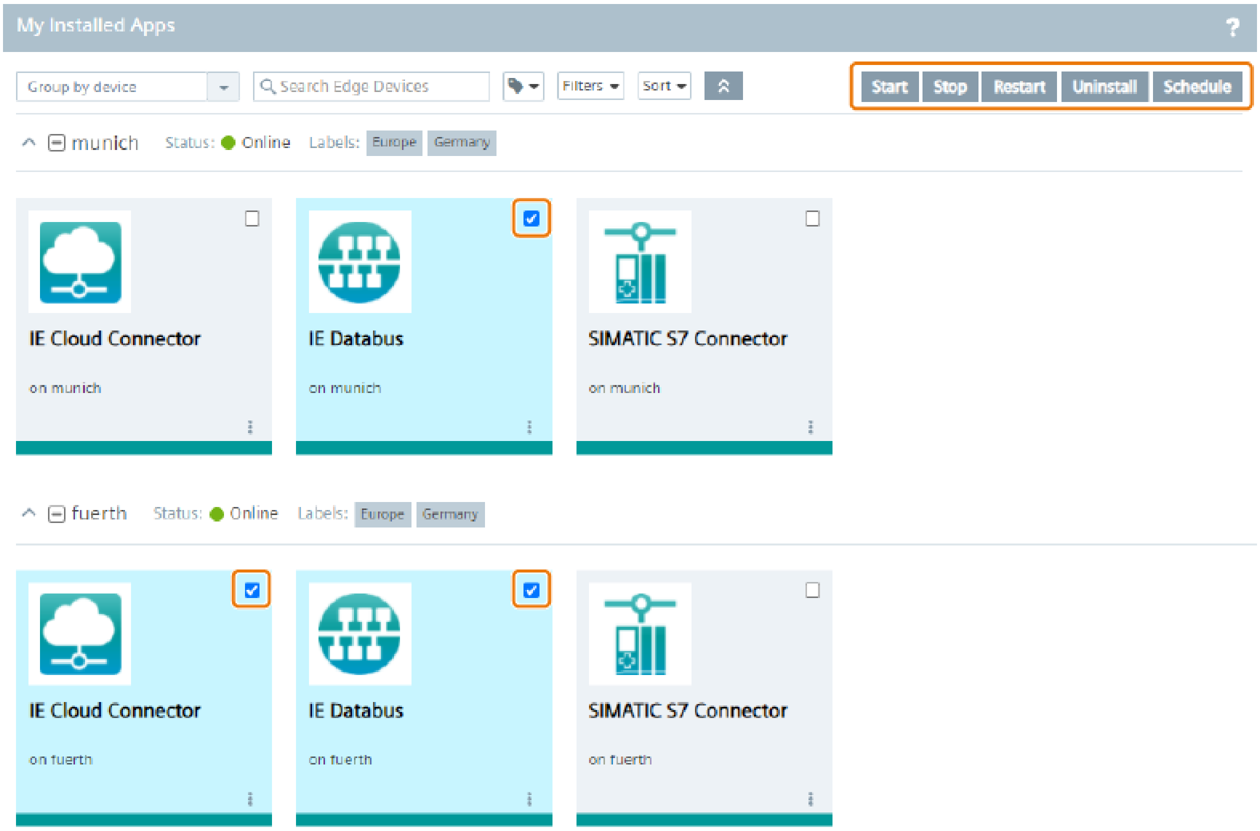
x86-64

V

231.34 MB

Grouped by Edge Devices view

When you select minimum 1 app by clicking the check box of the app, buttons to manage the app are enabled.



In this way, you can manage more than 1 app at once and you can also schedule, for example, the restart of all selected apps at a specific time.

Available options

To manage your app, the following options are available:

- Events: Display system events when you subscribe to the "Event Service" during the creation of the app version in the IE App Publisher
- Update Configuration: Update, edit or select an other app configuration of the app on the specific Edge Device
- Delete Configuration: If you have created several app configurations, delete app configurations of the app on the specific Edge Device
- Uninstall: Uninstall the app from the specific Edge Device
- Start: Start the app on the specific Edge Device
- Restart: Restart the running app on the specific Edge Device

- Stop: Stop the running app on the specific Edge Device
- Schedule: Schedule an app job of selected apps (only available in the grouped by Edge Devices view)

You can execute the options immediately or at a later required time.

8.3 Scheduling an app job

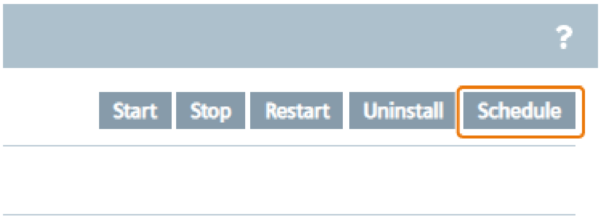
Requirement

Minimum 1 app has been installed on an Edge Device.

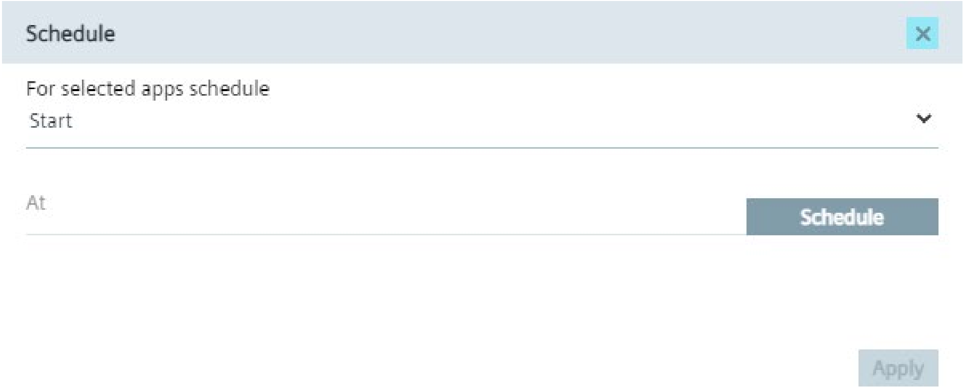
Procedure

1. Switch to the grouped by Edge Devices view.
2. Select all apps by clicking their respective check boxes for which you want to schedule a job.

   Buttons to manage the app are displayed.
3. Click "Schedule".

   The "Schedule" screen is displayed.

   
   Schedule

   For selected apps schedule: Start

   At

4. From the drop-down list, select the job you want to schedule.

   The following app jobs are available:

   – Start
   – Stop
   – Restart
   – Uninstall
5. Click "Schedule" and select a schedule date and time.
6. Click "Apply".
7. To finally schedule the job, click "Apply".

   An according job is created and will be started at the scheduled time.

Data Connections 9

9.1 Overview

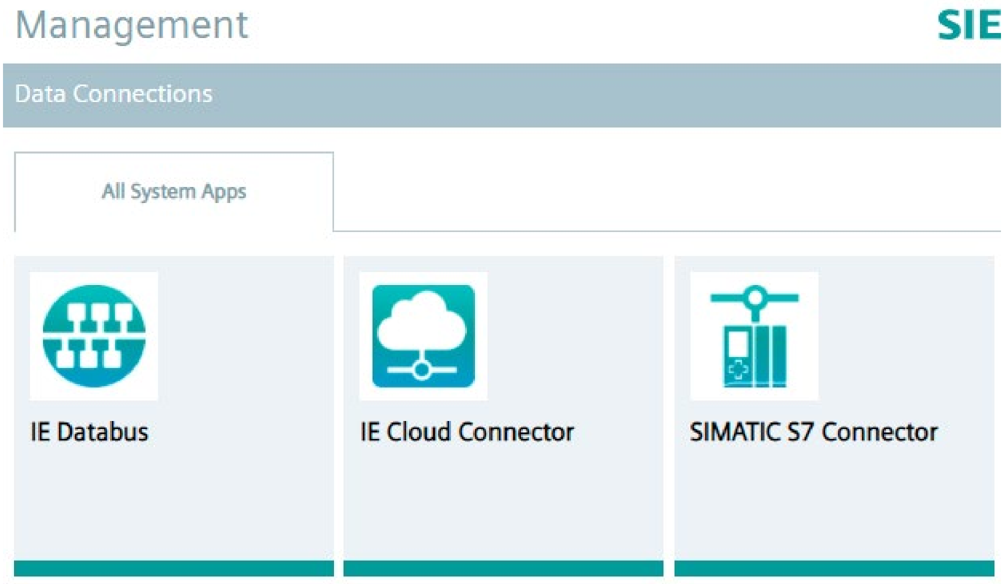
From the "Data Connections" menu item, you launch the "IE Databus" System App as well as apps that are configured by a configurator or that have an external URL as endpoint.

Note

Apps with an external URL as endpoint

When creating an app version in the IE App Publisher, you can set an external URL as redirection endpoint. By launching the app, the respective endpoint will be opened. You find more information on external endpoints, and in general on app redirections, in the "App Redirection" section in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109804060)" manual.

If you install configurators in the Maintenance UI and load the respective runtime app into the catalog of the Management UI, the "Data Connections" screen is displayed as follows for example.



Apps that have an external URL as endpoint are also displayed in this screen.

Once one of these apps is installed on an Edge Device, you can launch the respective app on that Edge Device.

9.2 Launching apps

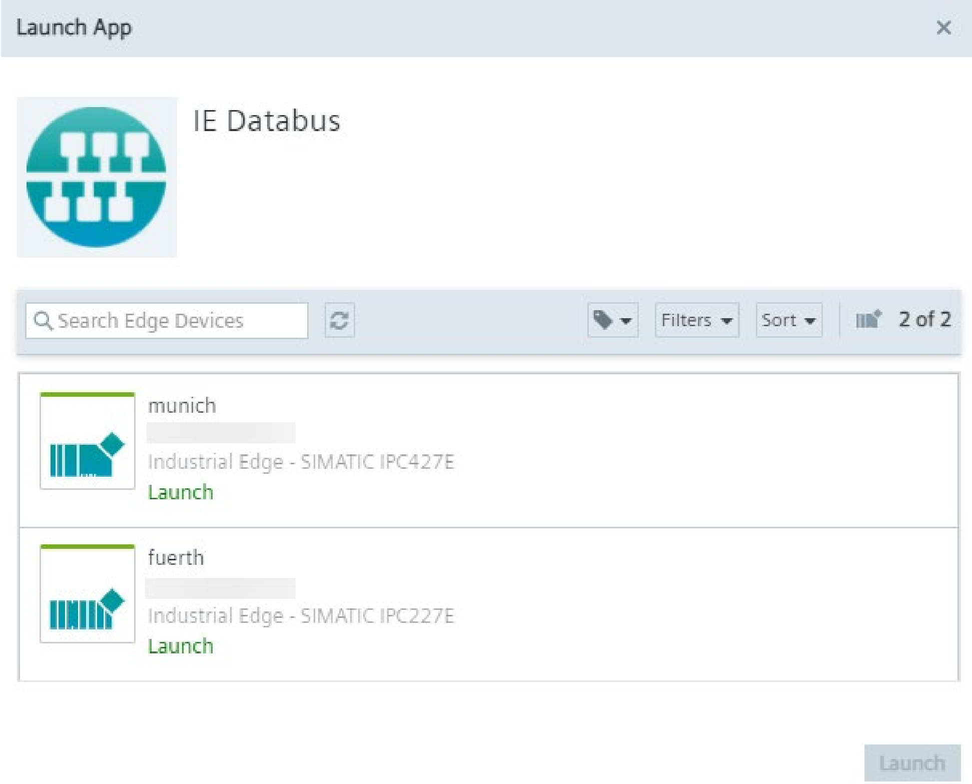
Requirement

- The configurator is installed in the Maintenance UI.
- The respective runtime app is installed on an Edge Device.

Procedure

1. Click the tile of the app, in this example the "IE Databus" System App.

   The "Launch App" screen is displayed.



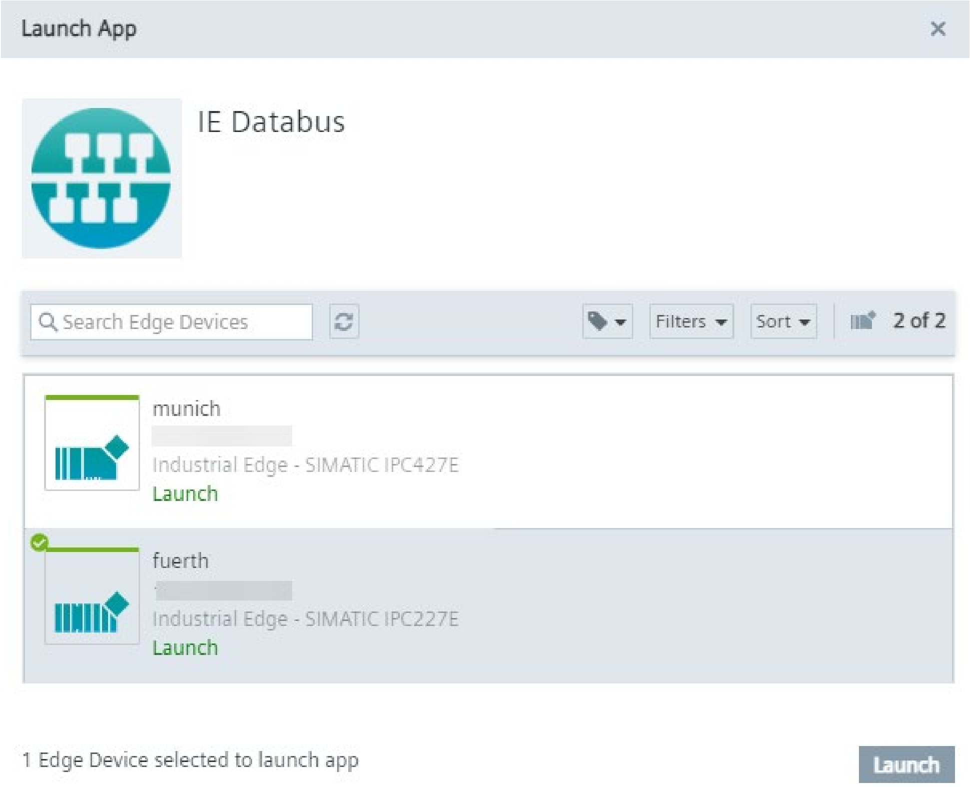
Launch App

IE Databus

munich
Industrial Edge - SIMATIC IPC427E
Launch

fuerth
Industrial Edge - SIMATIC IPC227E
Launch

2. Select the Edge Device on which the app is installed.



munich
[redacted]
Industrial Edge - SIMATIC IPC427E
Launch

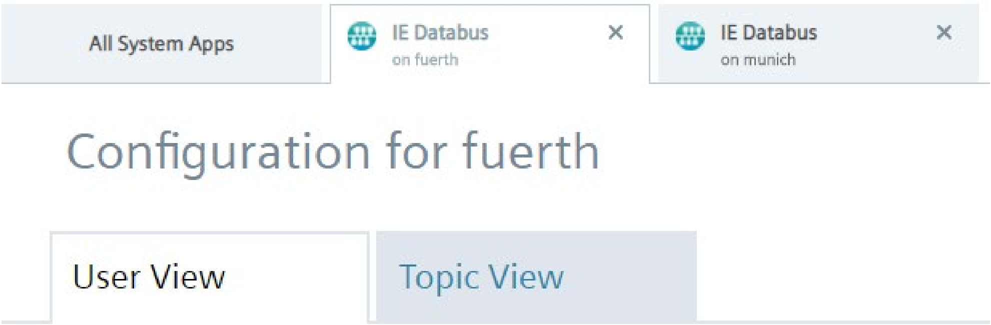
fuerth
[redacted]
Industrial Edge - SIMATIC IPC227E
Launch

1 Edge Device selected to launch app

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

3. Click "Launch".

The app is launched and will be opened in a new tab inside the "Data Connections" screen. The tab displays the app name and the respective Edge Device.



In that way, you can open several apps on different Edge Devices and swicth between the apps through the tabs.

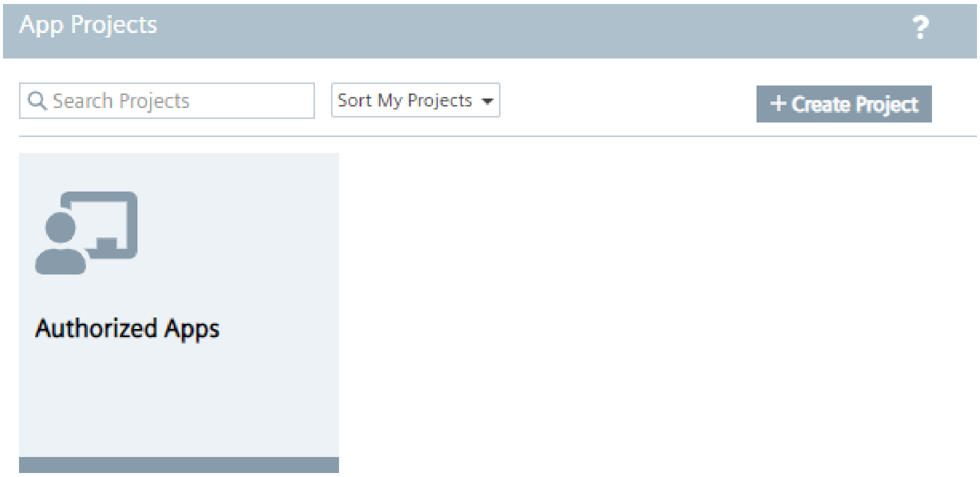
App Projects 10

10.1 Overview

To use your self developed apps in the IEM, you can publish your apps to projects in the "App Projects" menu item.

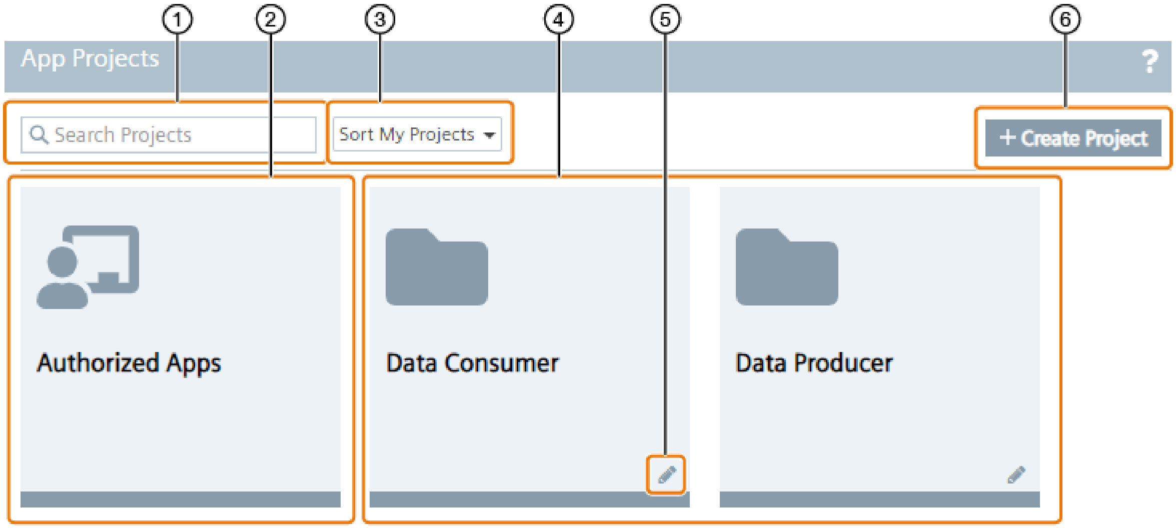
In the "App Projects" screen, you get an overview about all created projects inclusive all assigned apps to each project, and an overview about shared apps.

The layout of the "App Projects" screen varies depending on whether or not you have already created a project. If you have created no projects yet, only the "Authorized Apps" folder is displayed as follows:



The "Authorized Apps" folder, which is created by default, contains apps that have been shared with you.

Once you have created minimum 1 project, the screen is displayed as follows for example:



① Search for projects
② "Authorized Apps" folder with shared apps inside
③ Sort the projects
④ Created projects
⑤ Edit project
⑥ Create new project

Projects are presented via folders. When you select a folder, you can check the created apps in this project. You can also create new apps inside the projects.

Note

Publishing app versions from the IE App Publisher

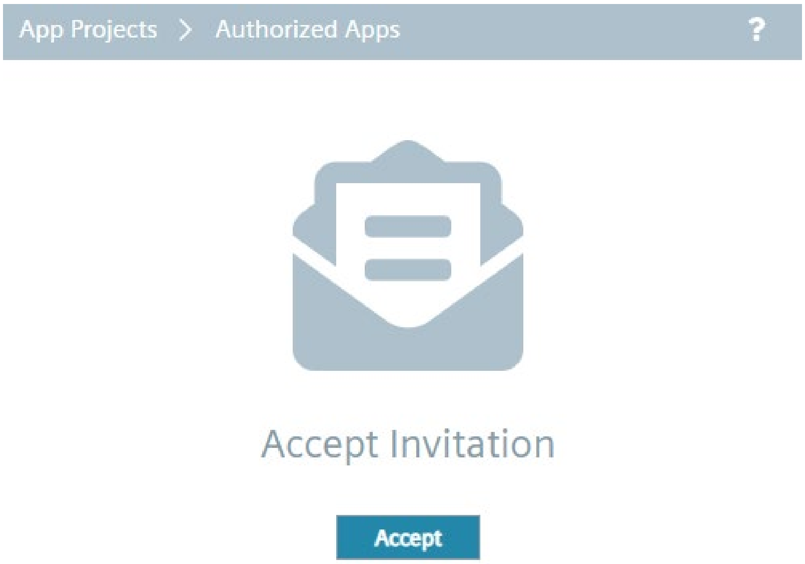
If you want to publish an app version from the IE App Publisher to a project, first you must create the project in the IEM. After you have created the project in the IEM, you can publish the created app version from the IE App Publisher to the IEM.

10.2 Authorized Apps

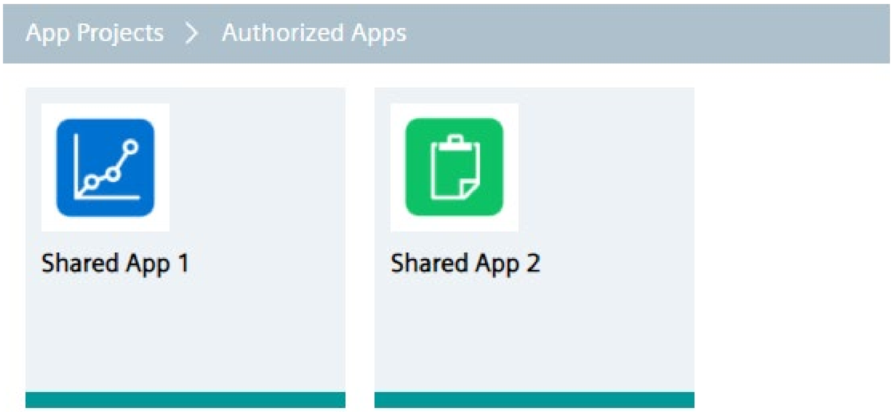
10.2.1 Overview

The "Authorized Apps" folder shows you all foreign apps that are shared with you from a foreign project.

If no apps have been shared with you yet, the "Authorized Apps" screen is displayed as follows:



Once apps have been shared with you, the "Authorized Apps" screen is displayed as follows for example:



By clicking the app tile, the app details are displayed. Depending on the permissions assigned to the project, several operations are available or not. Project members for example can edit app versions or display app keys. The available permissions are listed in the "Roles (Page 212)" subsection.

Note

Contributing to a project

When you contribute to another app from a foreign project, you must first pull the images from the previous app version in the IE App Publisher before submitting a new app version.

10.2.2 Joining other projects

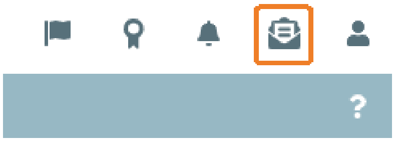
To join another project, the owner of the respective project must invite you to the project and must send you an invitation code. This invitation code enables you to join the shared project.

Requirement

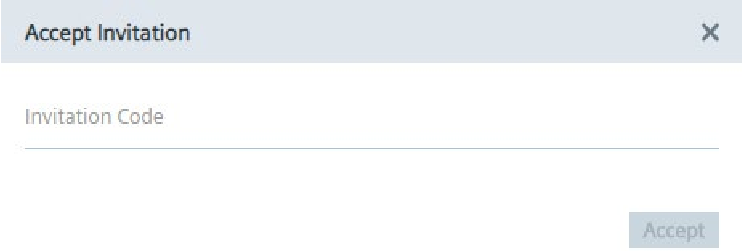
You have received the invitation code.

Procedure

1. In the top-right corner, click the icon to accept an invitation.



The "Accept Invitation" screen is displayed.



Accept Invitation

Invitation Code

2. In the "Invitation Code" input field, enter the invitation code that you received from the owner of the project.
3. Click "Accept".

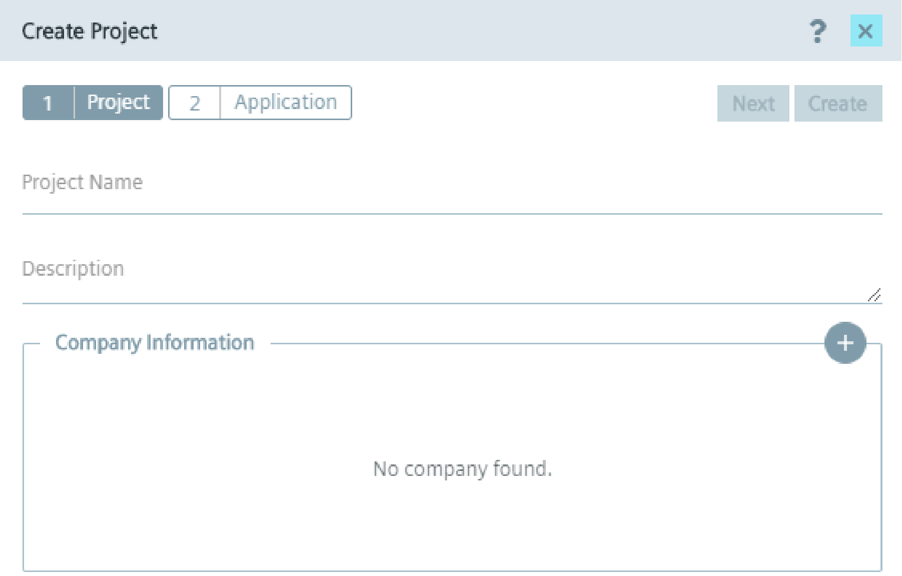
   If the invitation code is valid, all apps that are assigned to the project are now available.

10.3 Creating a project

Procedure

1. Click "Create Project".

   The "Create Project" screen is displayed.



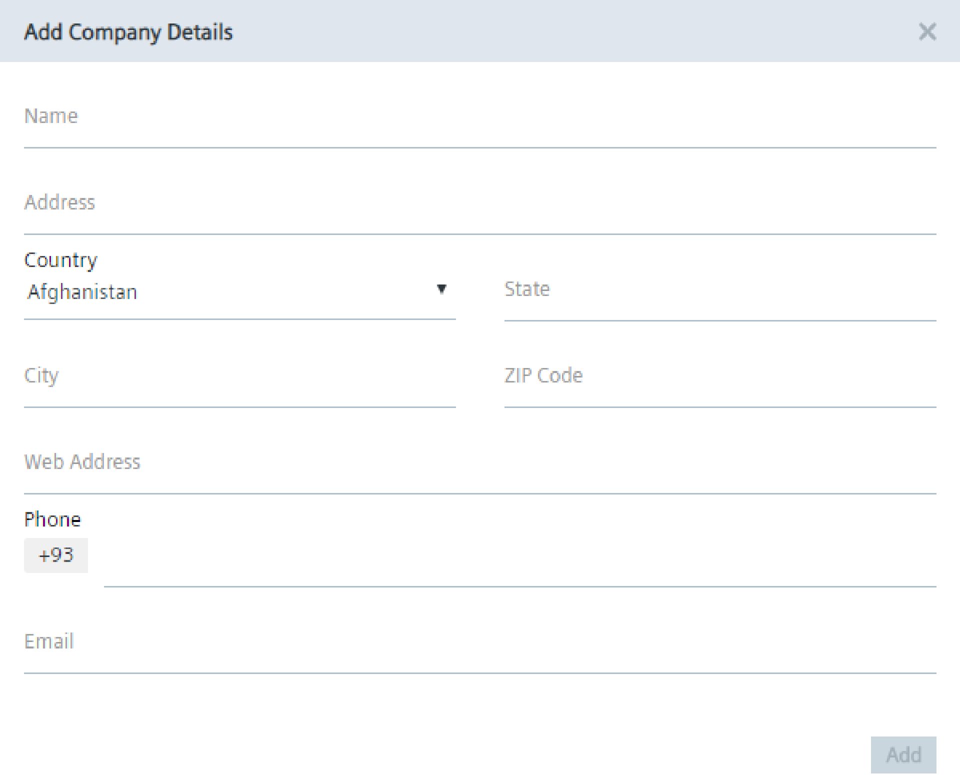
Create Project

No company found.

2. In the "Project Name" input field, enter the name of the project.
3. In the "Description" input field, enter the description of the project.

4. To add information about the company respectively the publisher, click the ⊕ icon.

   The "Add Company Details" screen is displayed.



Country
Afghanistan ▾

Phone
+93

5. Enter the company specific information.
6. To complete the company information, click "Add"
7. Click "Create".

   The project is created.

Note

Creating an app in the project

If you want to directly create an app and add the app to the project, click "Next" instead of "Create". In the following screen, create the app according to the "Creating an app - Parameters (Page 174)" subsection.

10.4 Editing a project

When you click the ✎ icon inside the project tile, the "Edit Project" screen is displayed.

In this screen, you edit the following parameters of the project:

- Project name
- Description
- Company information

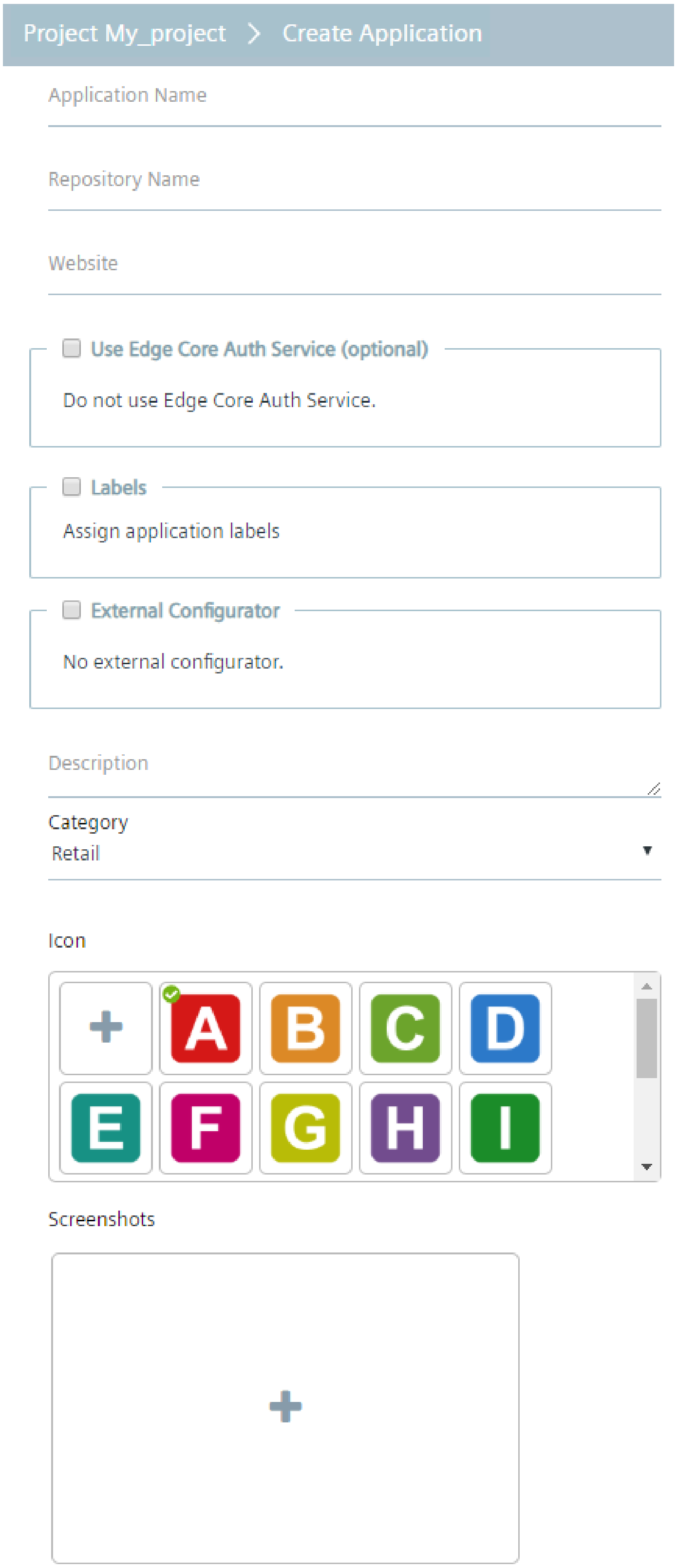
To save your changes, click "Update". By clicking "Delete", you delete the project from the IEM.

10.5 Creating an app

Procedure

1. Select the folder in which you want to create an app.
2. Click "Create Application".

   The "Create Application" screen is displayed.



Project My_project > Create Application

Application Name

Repository Name

Website

□ Use Edge Core Auth Service (optional)

Do not use Edge Core Auth Service.

□ Labels

Assign application labels

□ External Configurator

No external configurator.

Description

Category
Retail ▼

Icon

Screenshots

3. Configure your app according to the "Creating an app - Parameters (Page 174)" subsection.
4. After configuring the app, click "Create".

   The app is created in the project.

   When you click the tile of the created app, the app details are displayed. Notice, that no versions of the app are available. You create and upload the versions of the app in the IE App Publisher.

10.5.1 Creating an app - Parameters

Parameter	Description
Application Name	App name
Repository Name	• Tag images with the repository name on the IEM registry • The IEM stores the image in the registry by tagging it with <IEM-IP>/<repo-name>/<image-name> • Additionally represents the top folder in which the *.app file is put • Only lower-case alphanumeric characters are valid
Website	Website of the company
Use Edge Device Auth Service (optional)	• Enable the authorization service to access the app for multiple users • When enabled, choose 1 of the available types for users to access the app
Labels	• Assign labels to the app • You find more information on assigning labels to the app in the "Assigning labels (Page 175)" subsection
External Configurator	• Possibility to use an external app configuration • When enabled, enter the URL of the external configurator via which you configure the app you want to install • You find more information on the external configurator in the "Enabling the external configurator (Page 176)" subsection
Description	App description
Category	Category of the app
Icon	• App icon • Select a given icon or upload an own icon by clicking the plus icon
Screenshots	• Adding screenshots to the app by clicking the plus icon • The screenshots are displayed in the app details

Note

App and repository names

App and repository names are unique. You can just use them once in your IEM.

10.5.2 Assigning labels

By default, all new apps have no labels assigned to them. You have the possibility to assign 1 or more labels to several apps. In that way, you group your apps.

Procedure

1. In the "Create Application" screen, select the "Labels" check box.

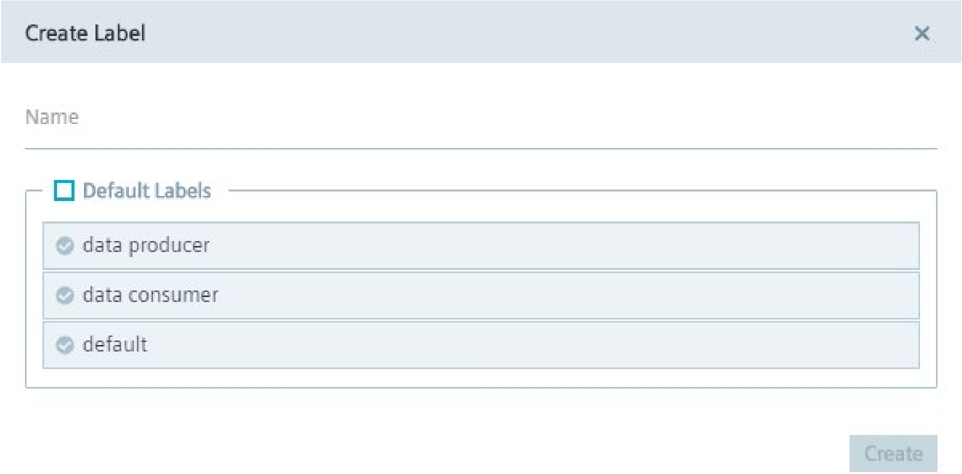
   The ⊕ icon is enabled.

2. Click the ⊕ icon.

   The "Assign Labels to Application" screen is displayed.

3. To create a new label, click "Create Label".

   The "Create Label" screen is displayed.



Create Label ×

Name

□ Default Labels

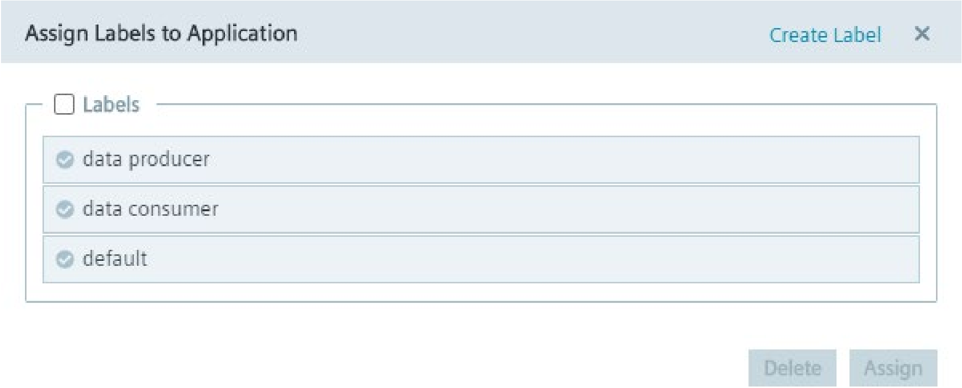
- data producer
- data consumer
- default

   By default, the "data producer", "data consumer" and "default" labels are available.

4. Click either 1 or more of the default labels or enter the name for a new label in the "Name" input field.

5. Click "Create".

   The selected labels respectively the newly created label is added to the label list.



Assign Labels to Application

□ Labels

- data producer
- data consumer
- default

6. Select the labels that you want to assign to the app.

   By clicking the "Labels" check box, all labels are selected.

   Note

   Deleting labels

   By selecting a label and clicking "Delete", the label is deleted.

7. Click "Assign".

   The labels are added to the "Create Application" screen. When you finish creating the app, the labels are assigned to the app.

10.5.3 Enabling the external configurator

When you install or update an app, the "External Configurator" option allows other services, that are hosted on the same domain, to configure the app that you want to install.

Procedure

1. When you create an app, select the "External Configurator" check box.

   The "Redirect URL" input field is enabled.

2. In the "Redirect URL" input field, enter the URL of the service respectively external configurator via which you configure the app you want to install.

   For example, if you want to use the IE App Configuration Service to render the app configuration when installing the app, enter "/acs" in the input field.

   Note

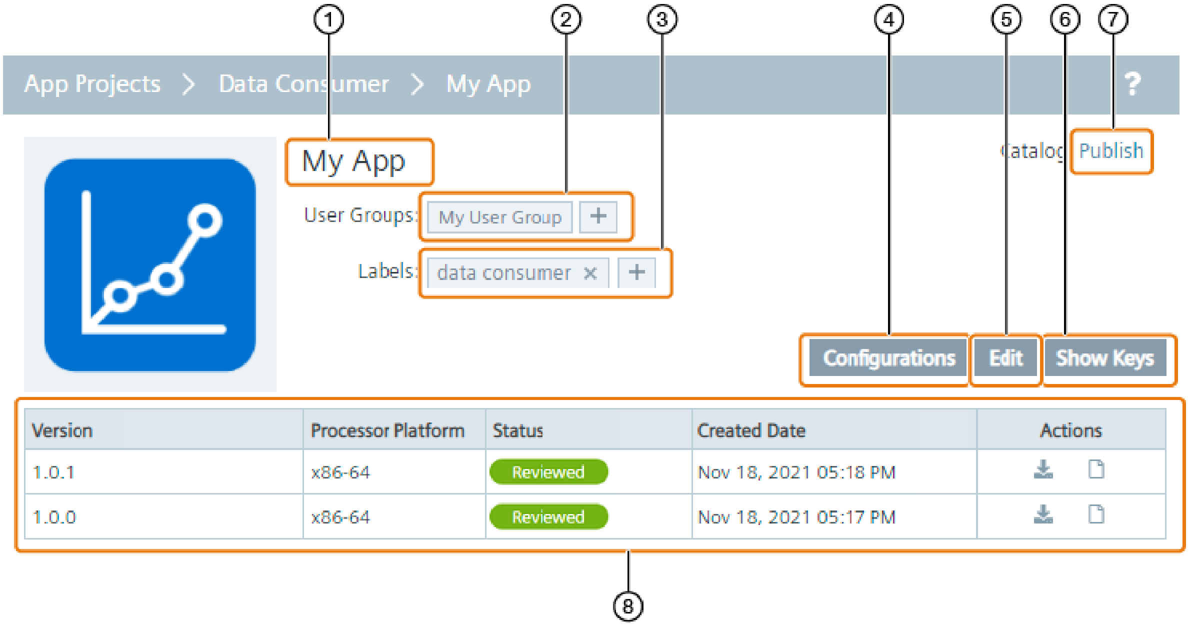
   Requirements for using the IE App Configuration Service

   To use the IE App Configuration Service when installing an app, the following is required from app side:

   - The "Redirect URL" input field when enabling the "External Configurator" check box must be entered with "/acs".
   - The "JSON Schema" check box must be enabled during the creation of the app configuration.

10.6 App details

When you click the tile of an app, the app details are displayed as follows for example:


①
②
③
④
⑤
⑥
⑦
App Projects > Data Consumer > My App
?
My App
User Groups: My User Group +
Labels: data consumer × +
Catalog
Publish
Configurations
Edit
Show Keys
⑧

Version	Processor Platform	Status	Created Date	Actions
1.0.1	x86-64	Reviewed	Nov 18, 2021 05:18 PM	⤓ 🗋
1.0.0	x86-64	Reviewed	Nov 18, 2021 05:17 PM	⤓ 🗋

① App name

② User groups:

- User groups in which the app is assigned to
- Assign app to other existing user groups

③ Labels:

- Assigned labels
- Remove labels from the app
- Create and assign new labels to the app

④ Add and manage app configurations

⑤ Edit app

⑥ Display app ID and secret keys

⑦ Publish app versions to the catalog in the Management UI

⑧ Version table with following information:

- Version: Published versions of the app from the IE App Publisher to the IEM
- Processor Platform: Platform of the published versions
- Status: Status of app versions
- Created Date: Date and time of uploaded app versions
- Actions:
  - ⤓ : Install app version
  - ⊘ : Remove app version from the catalog in the Management UI, if previously published via ⑦
  - 🗋 : Check Docker-compose file

10.7 App configurations

10.7.1 Creating configurations

By adding 1 or more app configurations, you create several configuration possibilities for the app. When you have several configurations for an app, you can choose, when you install the app on the Edge Device, which configuration suits the best for the selected Edge Device and for the app tasks.

Procedure

1. Click the tile of the app in the respective folder for which you want to create an app configuration.

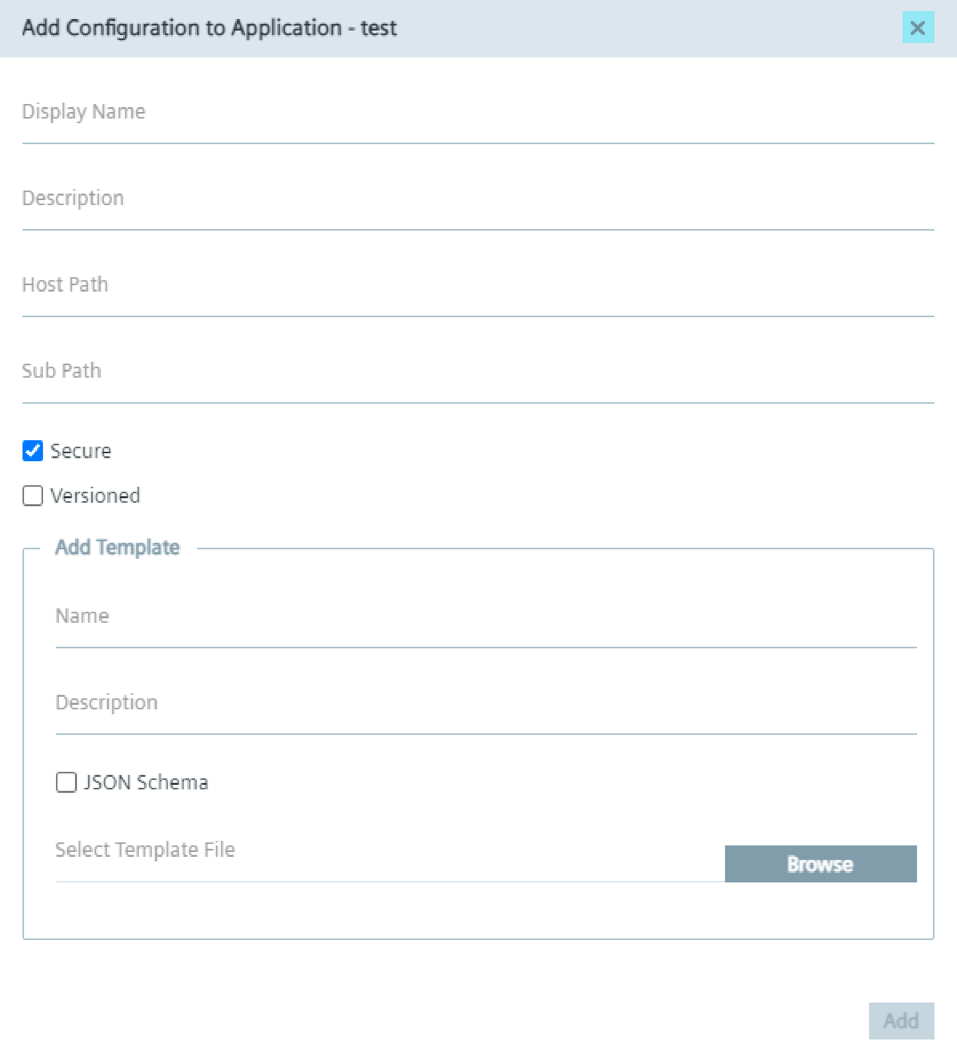
   The app details are displayed.

2. Click "Configurations".

   The "Configuration" screen of the app is displayed. If you already created any app configurations, all configurations for the selected app are listed in the drop-down list.

3. To create a new app configuration, click "Add Configuration".

   The "Add Configuration to Application" screen is displayed.



Add Configuration to Application - test

Display Name

Description

Host Path

Sub Path

☑ Secure

☐ Versioned

Add Template

Name

Description

☐ JSON Schema

Select Template File

You have the possibility to create several app configurations. You find information on the available app configurations and how to create these configurations in the following subsections.

10.7.2 Available app configurations

App configurations are either app versioned or Edge Device specific.

App versioned configurations

To add versioned configurations, select the "Versioned" check box in the "Add Configuration to Application" screen. Versioned configurations are only based on specific configuration files that you upload for each version of an app.

Edge Device specific configurations

To add Edge Device specific configurations, disable the "Versioned" check box in the "Add Configuration to Application" screen. For Edge Device specific configurations, you have the following types:

- Templates
- File uploads

Templates are either *.text or *.json based configuration files. In case of *.txt based configuration files, the configuration file supports the configuration for Edge Devices with allocated tags. Any key that you add to the template based configuration file in the format ""##$<KEY>$##" is replaced by its value that you have allocated to the Edge Devices through the created tags. App configurations that base on *.json template files are being used to configure and install the app via the IE Application Configuration Service. You find more information on the IE Application Configuration Service in the "IE Application Configuration Service (Page 185)" subsection.

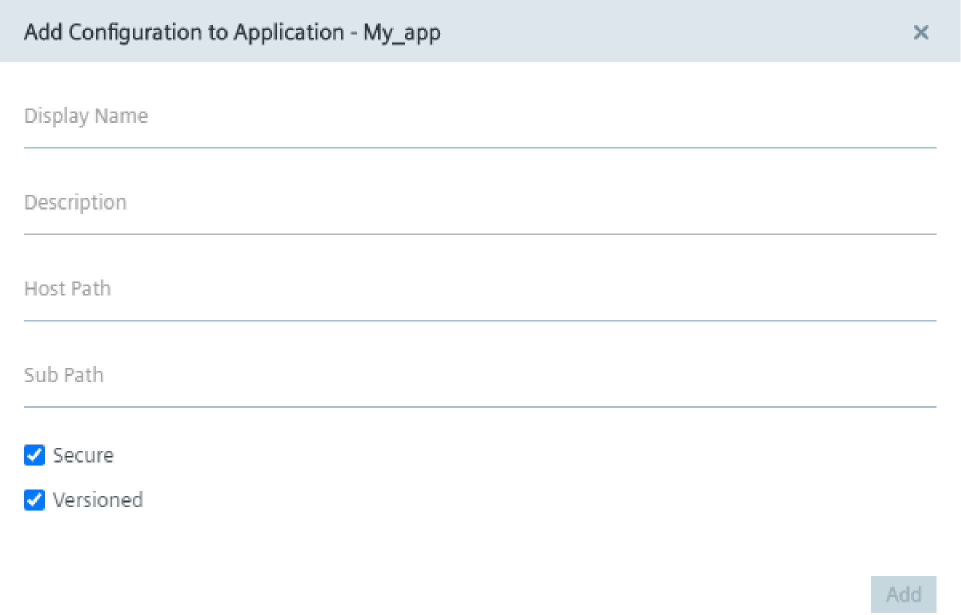
File upload configurations are based on configuration files that you upload. These configurations depend on the Edge Device on which you want to install the app.

10.7.3 Versioned configuration file

Uploading versioned configuration file

1. In the "Add Configuration to Application" screen, select the "Versioned" check box.

   The "Add Template" section is disabled.



Add Configuration to Application - My_app

Display Name

Description

Host Path

Sub Path

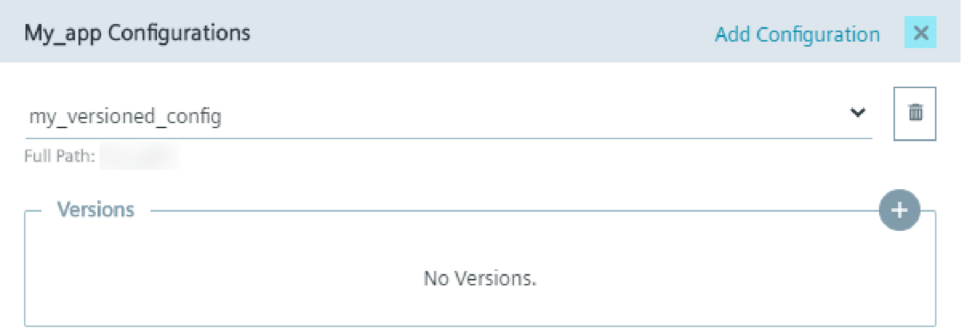
☑ Secure

☑ Versioned

2. Fill out the parameters of the screen according to the "Add configuration to app - Parameters (Page 184)" subsection.

3. Click "Add".

   The versioned configuration is added to the drop-down list in the configurations screen of the app.



my_versioned_config

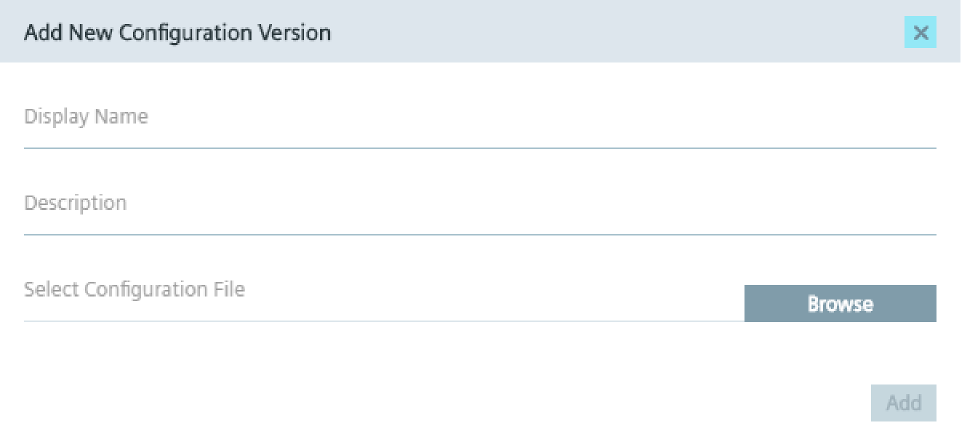
Full Path: [redacted]

No Versions.

   The created configuration still does not have any version related configuration file.

4. To add a required file to a specific version, click the + icon.

   The "Add New Configuration Version" screen is displayed.



5. Enter the name of the version and the description in the according input fields.
6. Click "Browse" and select the required configuration file for the version.
7. Click "Add".

   The version including the related configuration file are added to the version list in the configurations screen of the app.

Deleting versioned configuration

By clicking the 🗑 icon, you delete the version from the version list.

Downloading versioned configuration

By clicking the ⤓ icon, you download the configuration file to the standard download folder of your Internet browser.

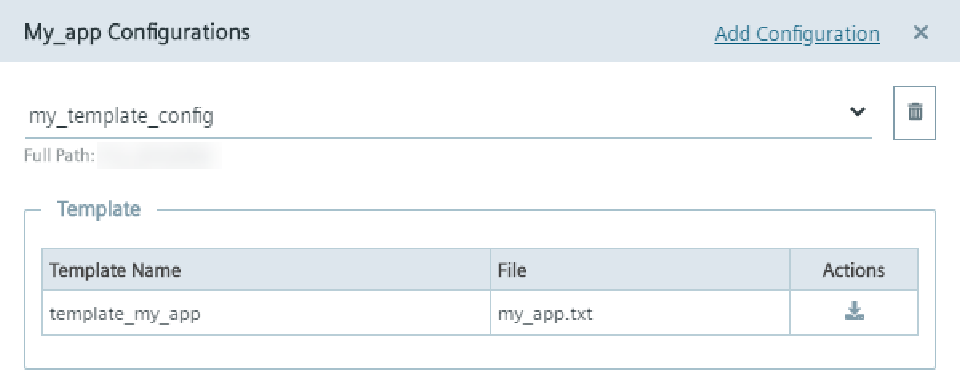
10.7.4 Template based configurations

Adding template based configurations

1. In the "Add Configuration to Application" screen, disable the "Versioned" check box.

   The "Add Template" section is enabled.
2. In the "Name" and "Description" input fields under the "Add Template" section, enter the name and the description of the template.
3. If the template based configuration file you want to use is in the "*.json" format, enable the "JSON Schema" check box.
4. To add the template file, click "Browse" and select the template based configuration file.
5. Fill out the rest of the screen according to the "Add configuration to app - Parameters (Page 184)" subsection.
6. Click "Add".

   The template based configuration is added to the configuration possibilities in the configurations screen of the app.



My_app Configurations

my_template_config

Full Path: [redacted]

Template

Template Name	File	Actions
template_my_app	my_app.txt	⬇

You can download the template file again by clicking the ⬇ icon.

Editing the template based configuration file

When you later install the app, you can edit the template based configuration file.

To edit the template based configuration file, click the edit icon of the template based configuration in the "Install app" screen. To save your changes, click "Update".

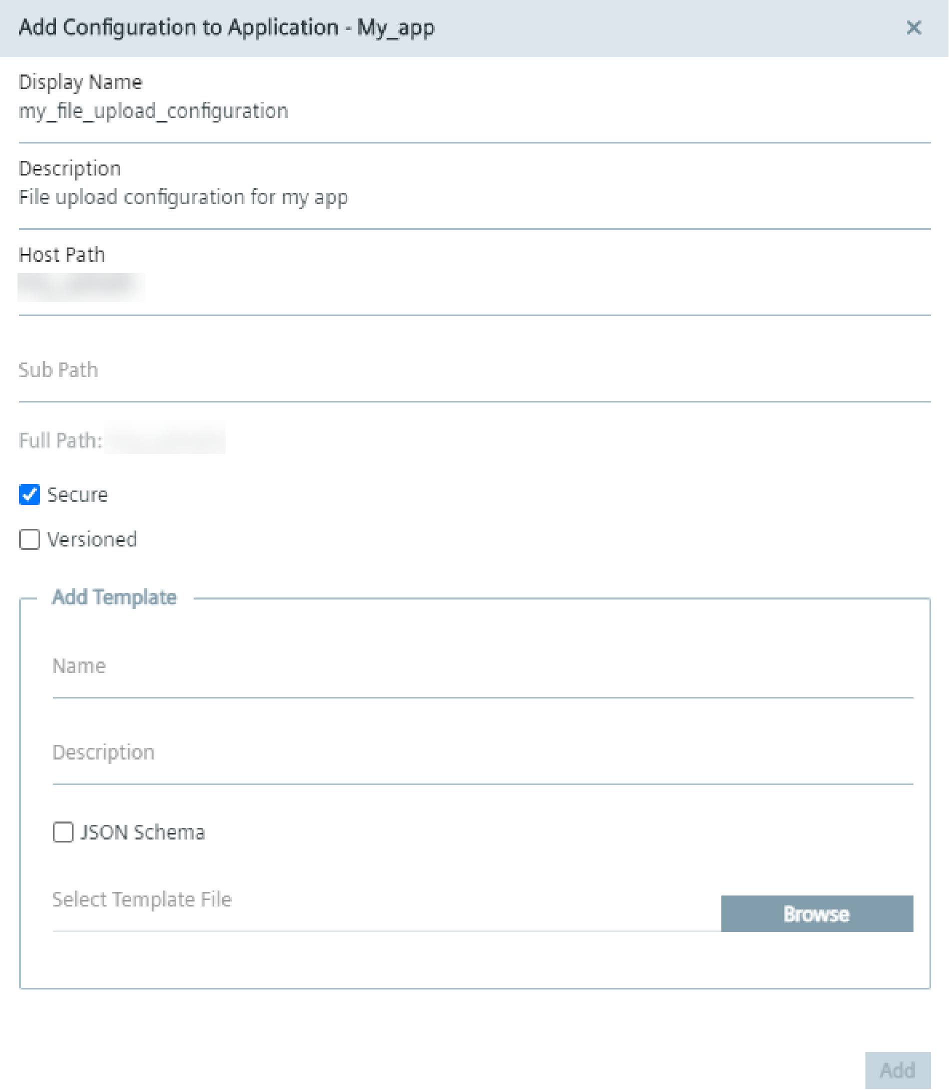
10.7.5 File upload configurations

Adding file upload configurations

1. In the "Add Configuration to Application" screen, disable the "Versioned" check box.

   The "Add Template" section is enabled.

2. Fill out the rest of the screen according to the "Add configuration to app - Parameters (Page 184)" subsection without entering the information in the "Add Template" section.



Add Configuration to Application - My_app

Display Name
my_file_upload_configuration

Description
File upload configuration for my app

Host Path
[redacted]

Sub Path

Full Path: [redacted]

☑ Secure

☐ Versioned

Add Template

Name

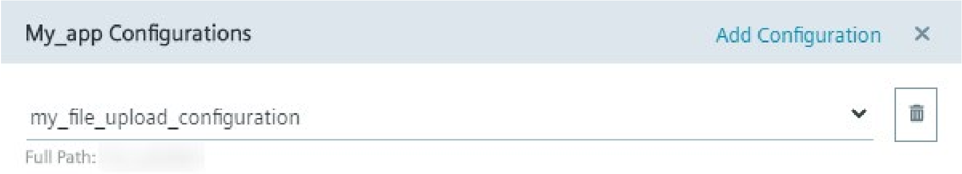
Description

☐ JSON Schema

Select Template File

3. Click "Add".

   The configuration is added to the configuration possibilities in the configurations screen of the app.


My_app Configurations

my_file_upload_configuration

Full Path:

When you later install the app, select the configuration and upload the required configuration file.

10.7.6 Add configuration to app - Parameters

The following are the parameters when creating an app configuration:

Parameter	Description
Display Name	• Name of the configuration • Mandatory input field
Description	• Description of the configuration • Mandatory input field
Host Path	• Mounted volume path that is configured in the "*.yaml" configuration file of the app • Mandatory input field
Sub Path	• Relative path • Optional input field
Secure	• Enable secured configuration • When you select the "Secure" check box, the uploaded configuration files are stored encrypted on the IEM • When you download the configuration files, they are again decrypted
Versioned	• Enable versioned configuration
Name	• Name of the template based configuration • Only available when versioned configuration is disabled
Description	• Description of the template based configuration • Only available when versioned configuration is disabled
JSON Schema	• Enable check box if template based configuration file is in *.json format • Only available when versioned configuration is disabled
Select Template File	• Browse template based configuration file • Only available when versioned configuration is disabled

The following are restrictions for the uploaded configuration files:

App configuration	File size	File type
Versioned configuration file	10 MB	• *.txt • application/octet-stream
Template based configuration file	10 MB	• *.txt • application/octet-stream
File upload configuration	10 MB	• *.txt • application/octet-stream

10.7.7 IE Application Configuration Service

10.7.7.1 Overview

The IE Application Configuration Service (ACS) provides the possibility to configure an app during the app installation or during the update by rendering a configuration specific UI. This UI is defined by schemes and is just available for template based app configurations.

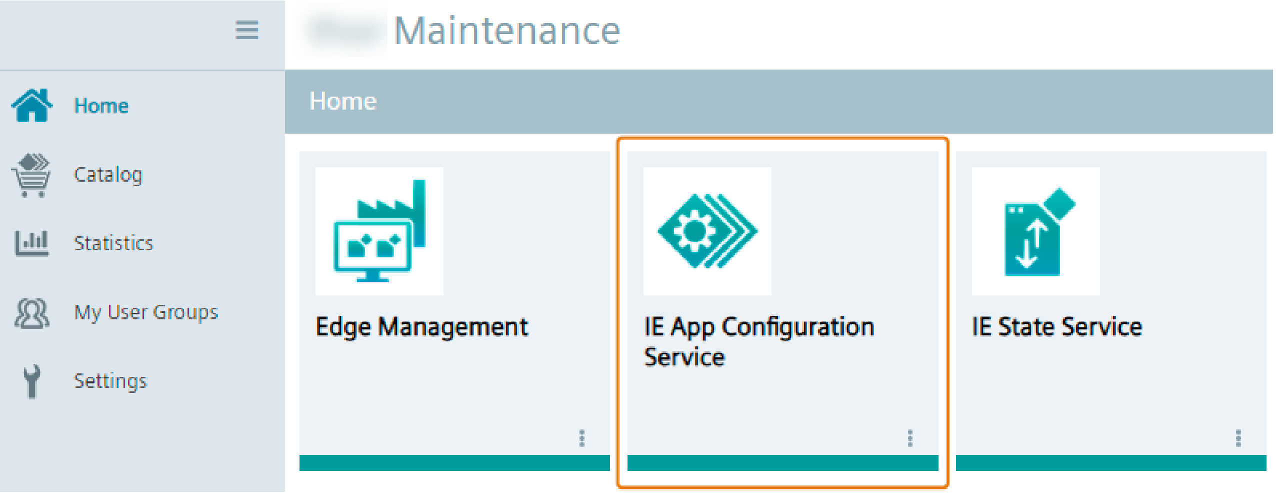
Using the IE ACS

To use the IE ACS in the Industrial Edge Management, the IE ACS must be installed in the IEM-OS. When the IE ACS is installed, the IE ACS will be used during the app configuration, either when you install a new app via the IE ACS (Page 195)in the IEM or when you update the configuration of an already installed app via the IE ACS (Page 202)in the IEM. If the IE ACS is not installed, template based app configurations are proceeded as described in the "Template based configurations (Page 182)" subsection.

If you want to provide app configurations that are compatible with the IE ACS, refer to the "Integration of IE ACS compatible app configurations (Page 189)" subsection.

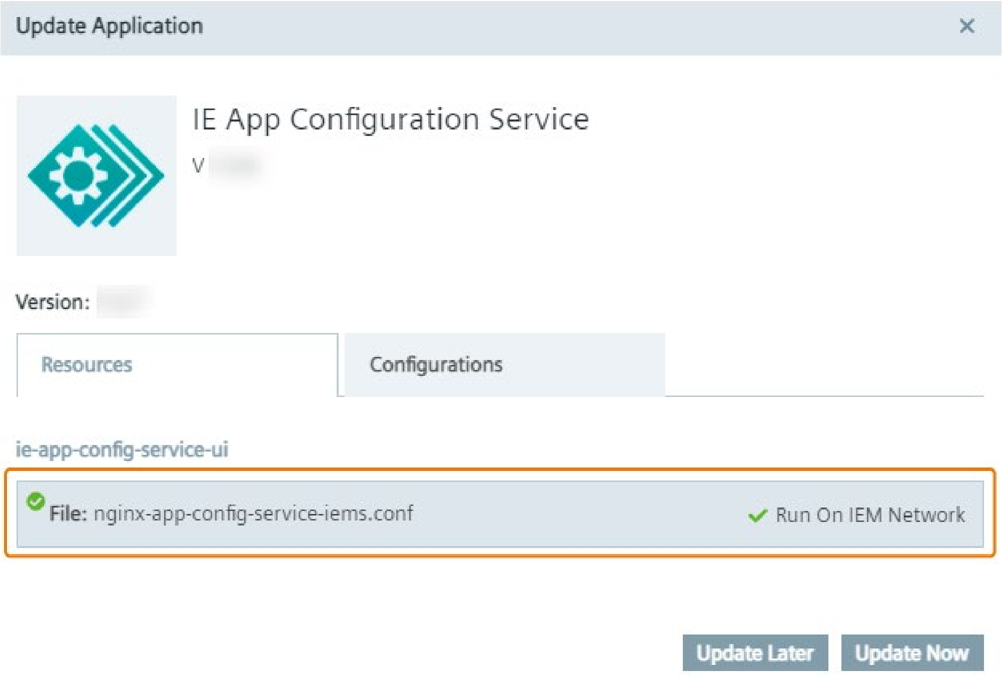
Installation and update

If you set up a complete new IEM, the IE ACS will be installed automatically in your IEM-OS. In that case, you find the "IE App Configuration Service" app in the "Home" screen of your Maintenance UI.



If you update your IEM V1.0 or V1.1, in which the IE ACS was not installed, to a newer version, you must install the IE ACS manually (Page 187)from the catalog in the Maintenance UI.

To update or check if an update for the IE ACS is available, click the ⋮ icon and then click the "Check Update" command. If an update is available, the "Update Application" screen is displayed. The current app version is displayed below the app name, the app version you update to is displayed below the app icon. Select respectively ensure that the available resource file in the "Resources" tab is activated.



File: nginx-app-config-service-iems.conf ✓ Run On IEM Network

Update the app by clicking "Update Now".

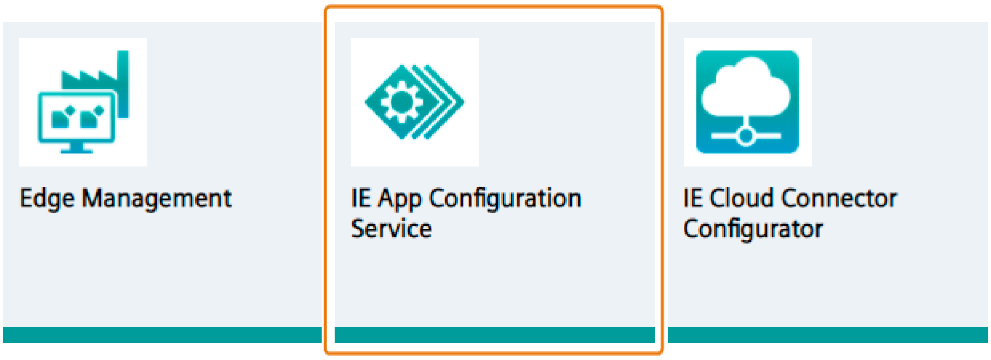
10.7.7.2 Installing the IE App Configuration Service manually

The following procedure is only requried for installing the IE ACS on an existing IEM V1.0 or V1.1 or after you updated an existing IEM V1.0 or V1.1 without installed IE ACS to a newer version.

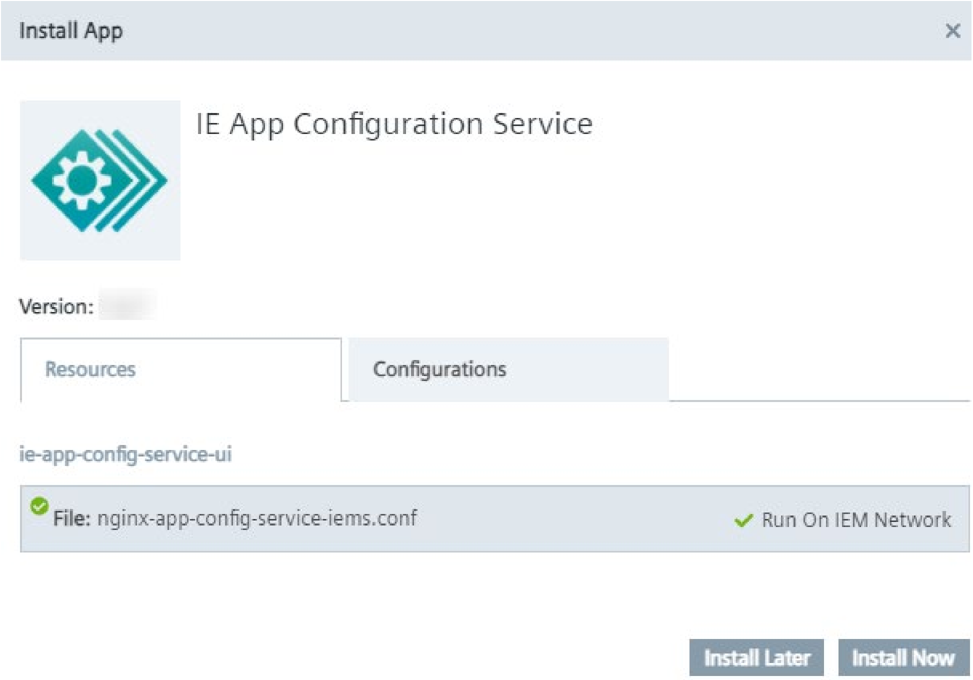
Procedure

1. Open and log into the Maintenance UI.
2. In the navigation menu, click "Catalog".

3. Click the "IE App Configuration Service" app.



The "Install App" screen is displayed.



Install App

IE App Configuration Service

Version: [redacted]

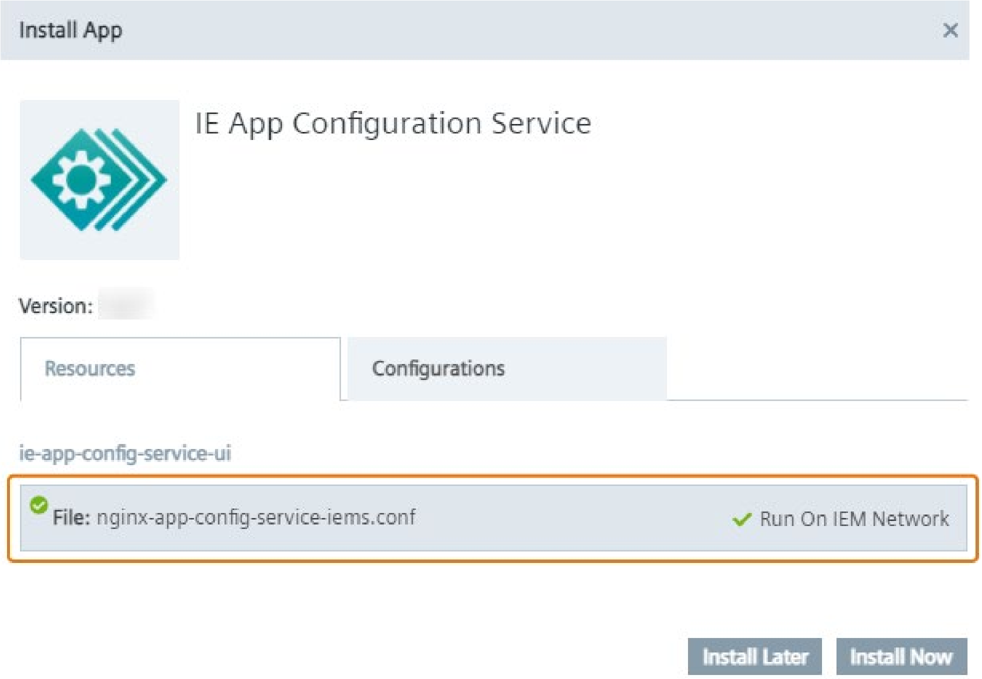
ie-app-config-service-ui

File: nginx-app-config-service-iems.conf

✓ Run On IEM Network

The app version you install is displayed below the app icon.

4. Ensure that the available resource file is activated.



Install App

IE App Configuration Service

Version:

Resources | Configurations

ie-app-config-service-ui

File: nginx-app-config-service-iems.conf ✓ Run On IEM Network

5. Without selecting any configurations click "Install Now" to install the app.

   An installation job is created. After the job is completed, the IE App Configuration Service is successfully installed and ready for usage.

10.7.7.3 Integration of IE ACS compatible app configurations

To add a configuration to your app, that is compatible with the IE ACS, you must first provide a schema which describes your configuration options and rendering. You can later use this schema as a *.json based template configuration when adding app configurations to your app.

Requirements to add an IE ACS compatible app configuration

- App must contain minimum 1 template based configuration with UI schema and data schema.
- During the creation of the app in the IEM, the "Redirect URL" input field when enabling the "External Configurator" (Page 176) check box must be entered with "/acs".
- During the creation of the app configuration, the "JSON Schema" check box must be enabled.

  Only template based configurations with enabled "JSON Schema" check box and with "/acs" entered external configurator are compatible with the IE ACS.

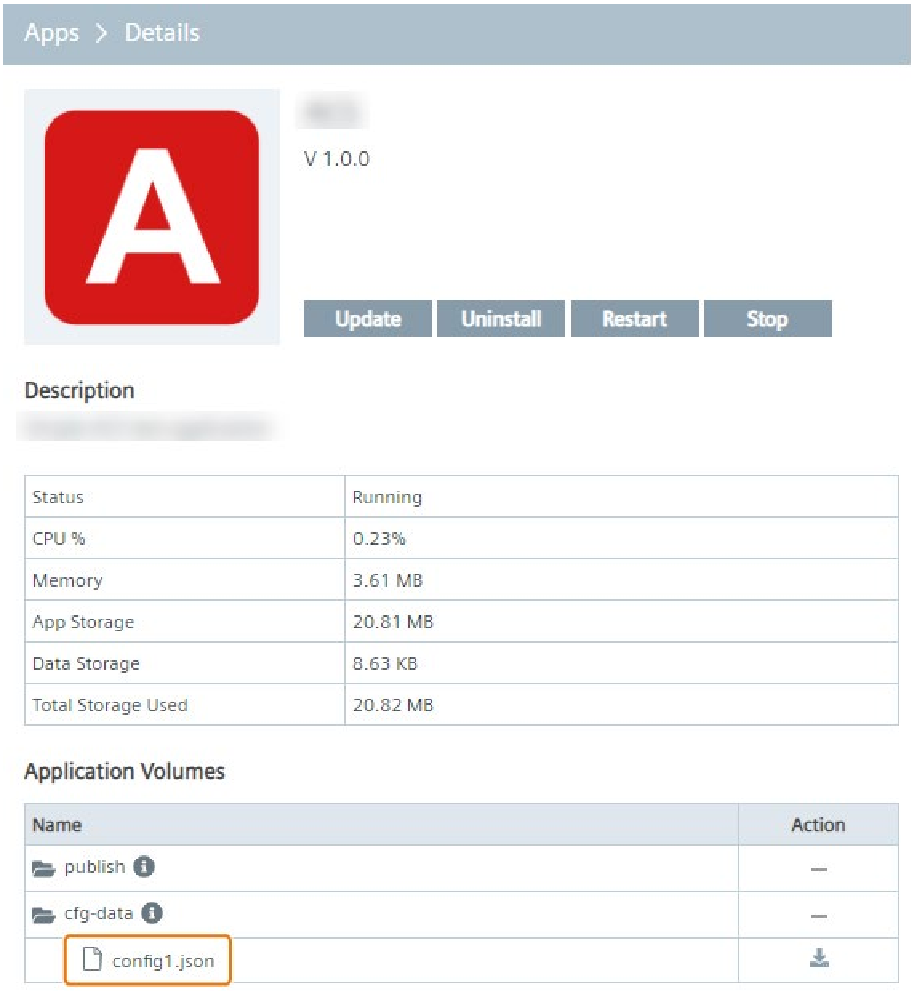
  You can also find information regarding the IE ACS compatibility in conjunction with the IE App Publisher in the "Configuring an Edge App" section in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

10.7.8 Downloading and checking app configuration

Procedure

1. Open the Edge Device UI in which the app has been installed.
2. In the "Apps" screen, click the ⋮ icon of the required app.
3. Click "More Info".

   The app details are displayed. The configuration is displayed under "Application Volumes".



Status	Running
CPU %	0.23%
Memory	3.61 MB
App Storage	20.81 MB
Data Storage	8.63 KB
Total Storage Used	20.82 MB

Application Volumes

Name	Action
publish	–
cfg-data	–
config1.json	⤓

4. To download the app configuration, click the ⤓ icon.

   The configuration file is downloaded to the standard download folder of your Internet browser. You can now again check the configuration file.

10.8 Installing an app from my projects

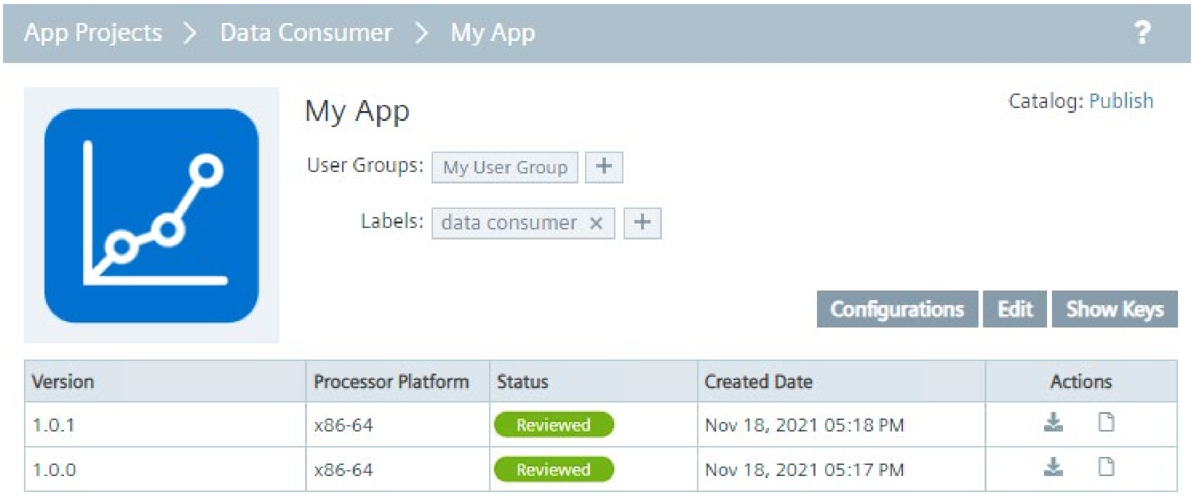
Requirement

- The app version has been published to the IEM.
- Minimum 1 Edge Device is running in the IEM.

Procedure

1. Click the tile of the app you want to install.

   All available versions of the app are displayed.



My App

Catalog: Publish

User Groups: My User Group +

Labels: data consumer ✕ +

Version	Processor Platform	Status	Created Date	Actions
1.0.1	x86-64	Reviewed	Nov 18, 2021 05:18 PM	⤓ 🗋
1.0.0	x86-64	Reviewed	Nov 18, 2021 05:17 PM	⤓ 🗋

Note

Verified Edge Apps

With the signature of an Edge App, the Edge App is trusted and verified by Siemens. Verified Edge Apps are marked with the 🛡 icon after the version.

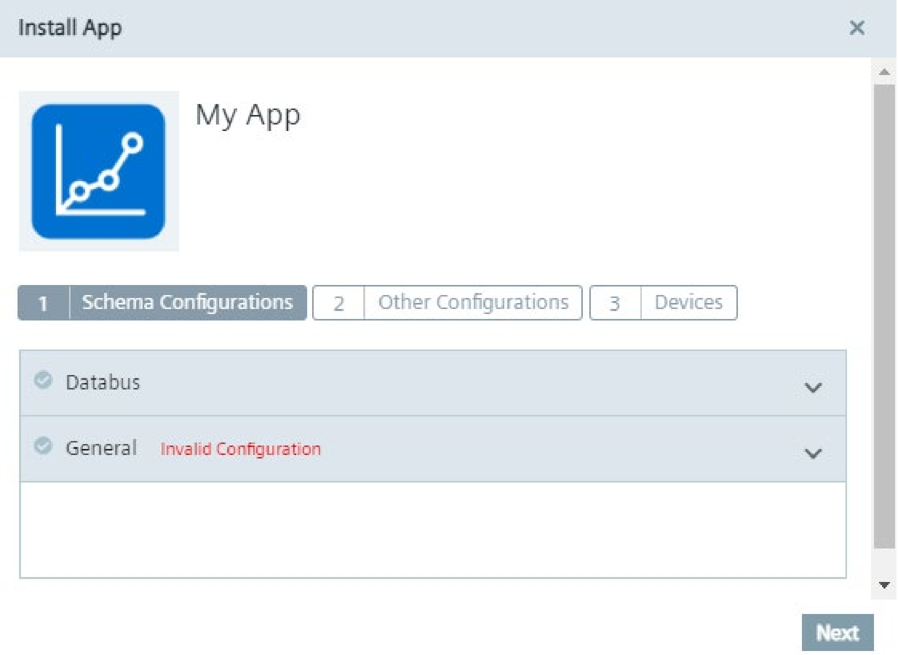
2. Install the required app version by clicking the ⤓ icon under "Actions" of the corresponding version.

   The "Install App" screen is displayed.

   The layout of the screen depends on whether or not the app contains template based *.json configuration files and hence is compatible with the IE ACS. If the app contains template based *.json configuration files, the app configuration is rendered by the IE ACS in the "Schema Configurations" tab. If the app does not contain template based *.json configuration files, the "Schema Configurations" tab is disabled. Instead, you choose the required app configuration in the "Configurations" tab.

3. Select the app configurations, if required, that you want to use for installing the app.

   In case the IE ACS is being used, select the required app configurations in the "Schema Configurations" tab and click "Next" twice. For each configured template based configuration, an according drop-down menu is represented, in this example 2 template based configurations "Databus" and "General".



Each configuration can be selected by clicking the check mark. You find more information and an example on installing an app via the IE ACS in the "Installing an app via the IE ACS (Page 195)" subsection.

In case the IE ACS is not being used, select the app configurations, if required, that you want to use for installing the app in the "Configurations" tab and click "Next".

If you do not need an app configuration to install the app, click "Next" without selecting a configuration.

Note

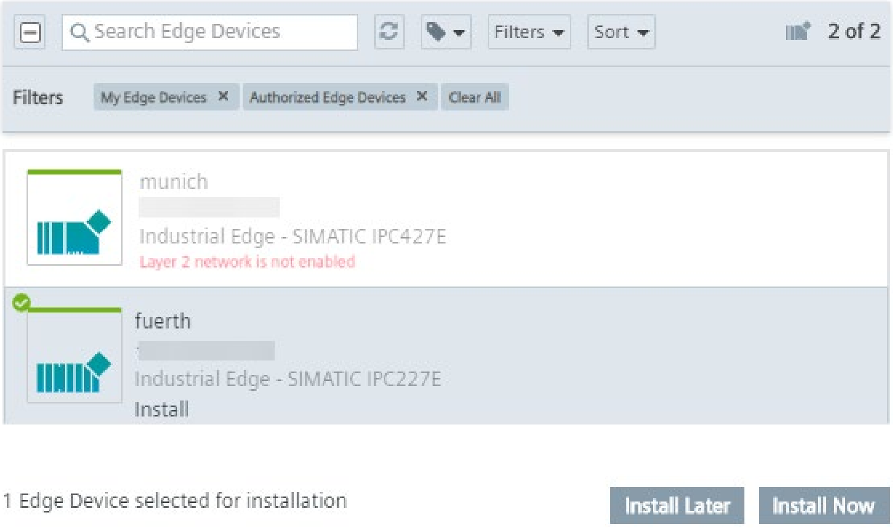
Required configurations

To identify the required configurations when installing an app, check the installation instructions in the documentation of the specific Edge App.

4. Select the Edge Device on which you want to install the app.

   You can select several Edge Devices to install the app to.

   You cannot install Edge Apps that require a Layer 2 (L2) network access on Edge Devices that do not support such a L2 network access.

   munich
   [redacted]
   Industrial Edge - SIMATIC IPC427E
   Layer 2 network is not enabled

   fuerth
   [redacted]
   Industrial Edge - SIMATIC IPC227E
   Install

   1 Edge Device selected for installation

   If you need to install apps that require a L2 network access, you must perform a Hard Reset of the Edge Device and re-onboard the Edge Device with L2 network access (see "Creating the Edge Device configuration file" subsection in the "Industrial Edge Device - Operation (https://support.industry.siemens.com/cs/us/en/view/109783785)" manual).

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

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

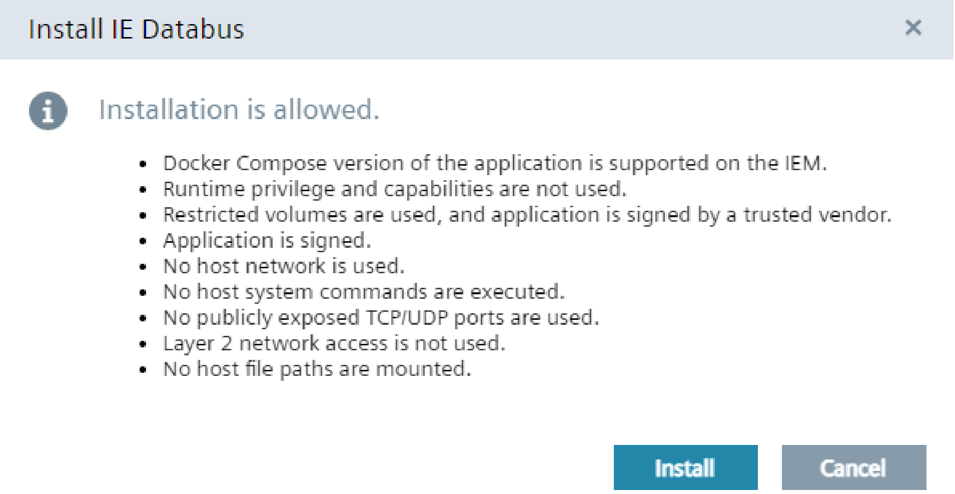
   Note

   Installation date and time

   When you select "Install Later", a calendar and the local system time is displayed for selecting the installation date and time.

   The "Install" screen is displayed which shows capabilities and services which will be used by the app. Depending on the Edge App, the installation is allowed, allowed with warnings or blocked.

   – If the installation is allowed without any warnings, the screen is displayed as follows for example:



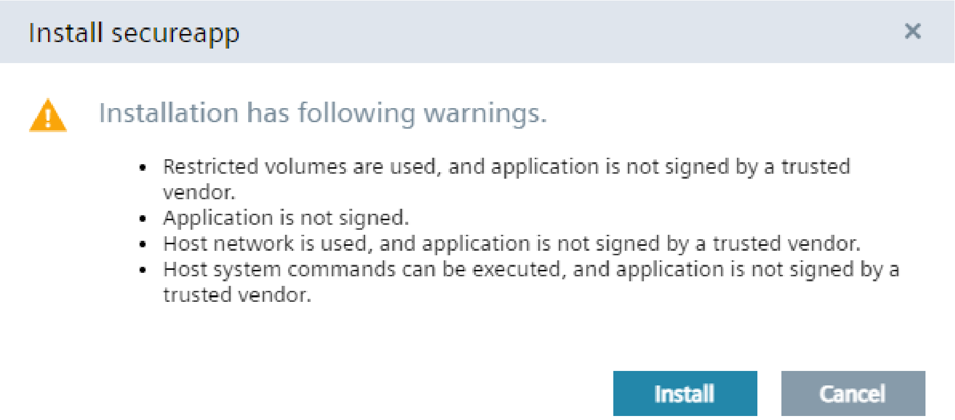
Install IE Databus

Installation is allowed.

- Docker Compose version of the application is supported on the IEM.
- Runtime privilege and capabilities are not used.
- Restricted volumes are used, and application is signed by a trusted vendor.
- Application is signed.
- No host network is used.
- No host system commands are executed.
- No publicly exposed TCP/UDP ports are used.
- Layer 2 network access is not used.
- No host file paths are mounted.

   By clicking "Install", the app will be installed.

   – If the installation is allowed but indicates several warnings, the screen is displayed as follows for example:



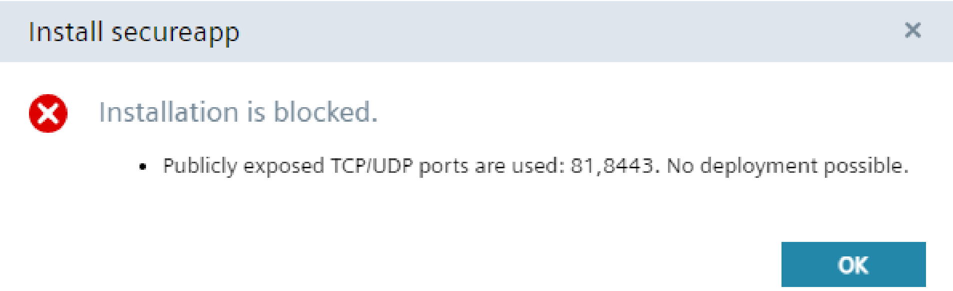
Install secureapp

Installation has following warnings.

- Restricted volumes are used, and application is not signed by a trusted vendor.
- Application is not signed.
- Host network is used, and application is not signed by a trusted vendor.
- Host system commands can be executed, and application is not signed by a trusted vendor.

In this case, check the warnings. If the warnings are neglectable and you still want to install the app, click "Install". Otherwise, click "Cancel".

– If the installation is blocked due to security risks for example, the screen is displayed as follows:



Install secureapp

Installation is blocked.

- Publicly exposed TCP/UDP ports are used: 81,8443. No deployment possible.

In this case, you cannot install the app.

6. To install the app, click "Install".

   The app is being installed. You can check the installation status in the "Job Status" menu item.

   Note

   Installation of apps

   The installation time of apps vary depending on (but not limited) network conditions, hardware specifications of each Edge Device or size of the apps.

See also

Privileged and network mode (Page 204)

App configurations (Page 178)

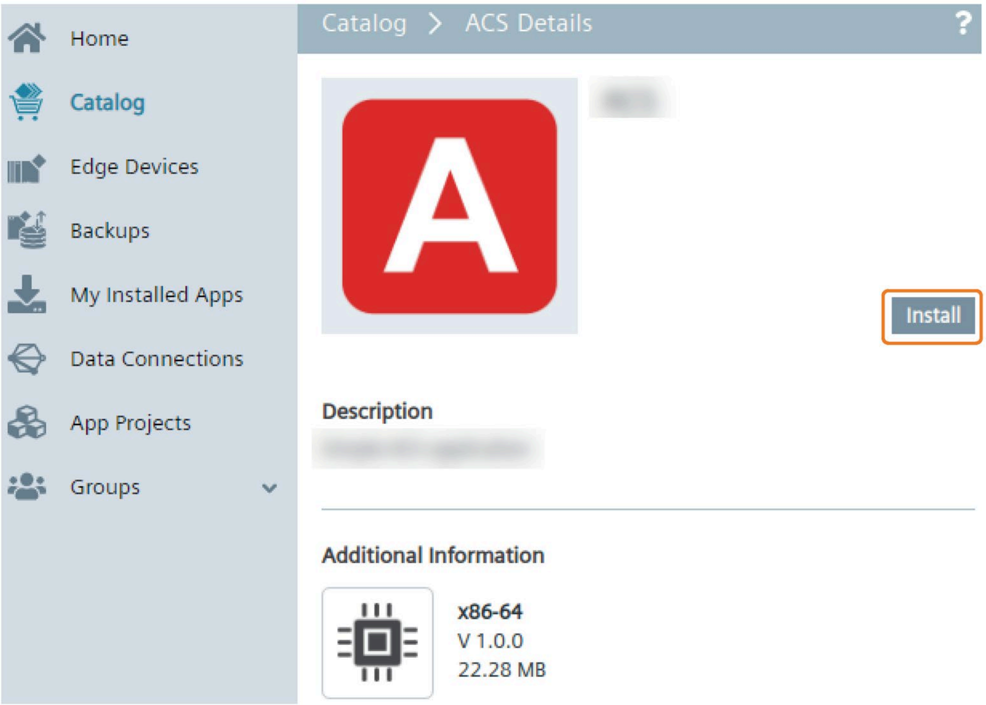
10.8.1 Installing an app via the IE ACS

Requirement

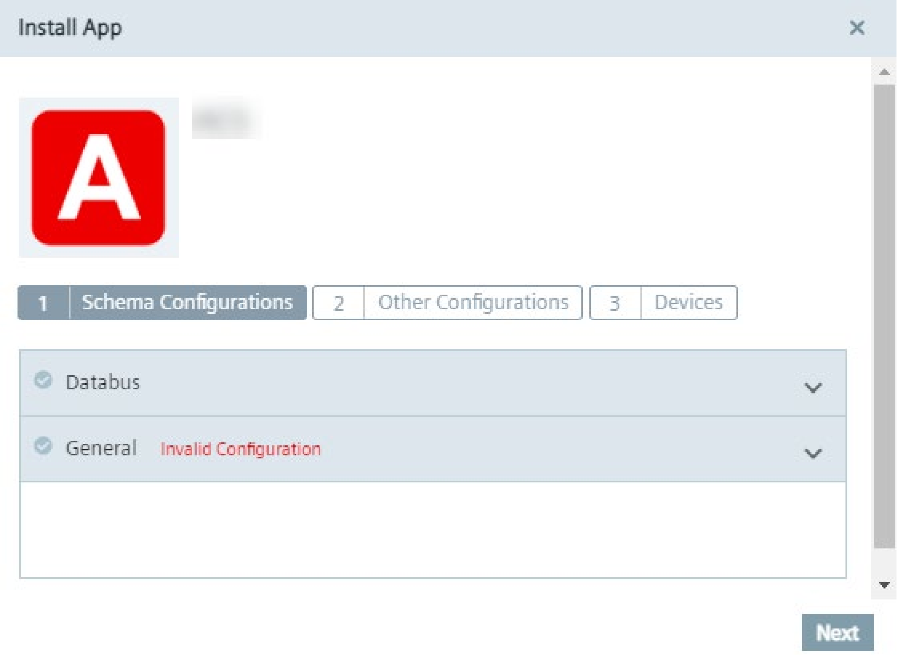
- IE ACS must be installed in the IEM-OS.
- App configuration is compatible with the IE ACS.

Procedure

1. When you want to install an app via the IE ACS, either from the catalog or from your own projects, click "Install".



The "Install app" screen is displayed.

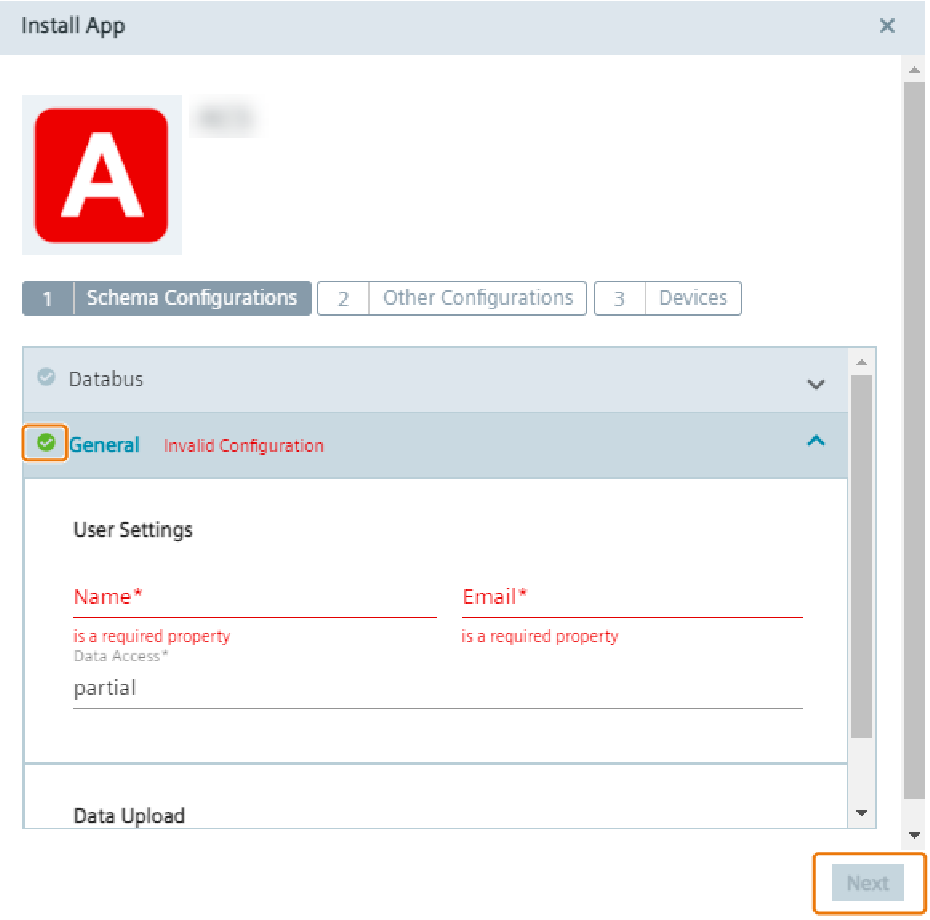


The above figure shows the rendered IE ACS. For each configured template based configuration, an according drop-down menu is represented, in this example 2 template based configurations "Databus" and "General". Each configuration can be selected by clicking the check mark.

2. To use an app configuration, click the according check mark.

   If a configuration is selected, the configuration will be used for installing the app. It is possible to select more than 1 valid app configurations.

   If a configuration is not valid, because for example some mandatory parameters are missing, the according configuration displays the "Invalid Configuration" error. If you select an app configuration that displays the "Invalid Configuration" error, the "Next" button gets disabled.



   In that case, you cannot install the app. If you want to use this configuration, you must fill in the missing parameters.

   Note

   Installation without a configuration

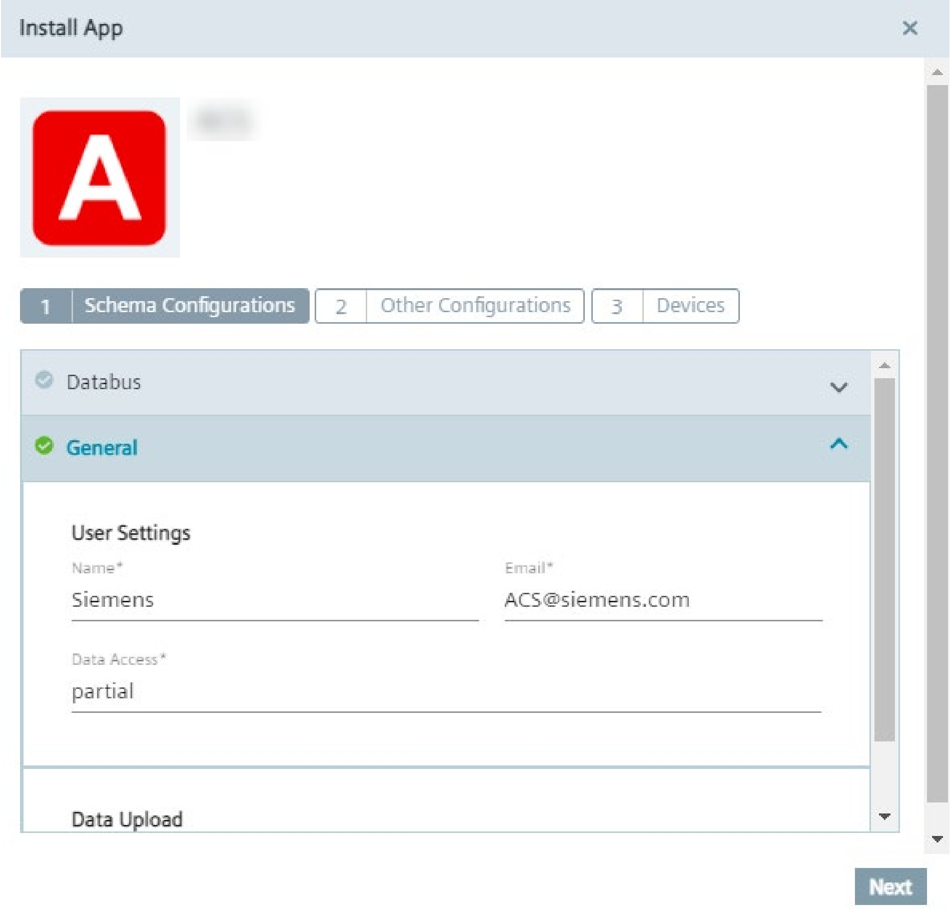
   It is also possible to install the app without a configuration. In that case, click "Next" without selecting a check mark.

3. To display detailed information and the mandatory parameters, click the respective drop-down menu.

   Mandatory parameters are marked as required properties.

4. Fill in the missing mandatory parameters.

   The "Next" button is enabled again.



User Settings

Name*
Siemens

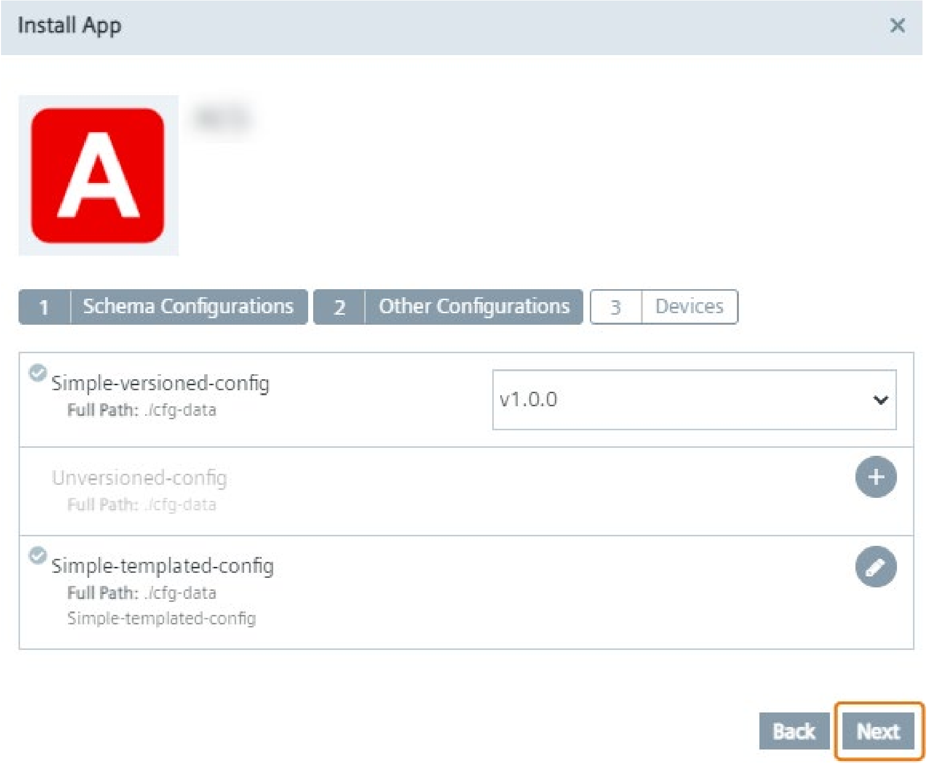
Email*
ACS@siemens.com

Data Access*
partial

Data Upload

5. Click "Next".

6. If the app also contains app configurations other than template based *.json files, click again "Next" without selecting an other configuration.



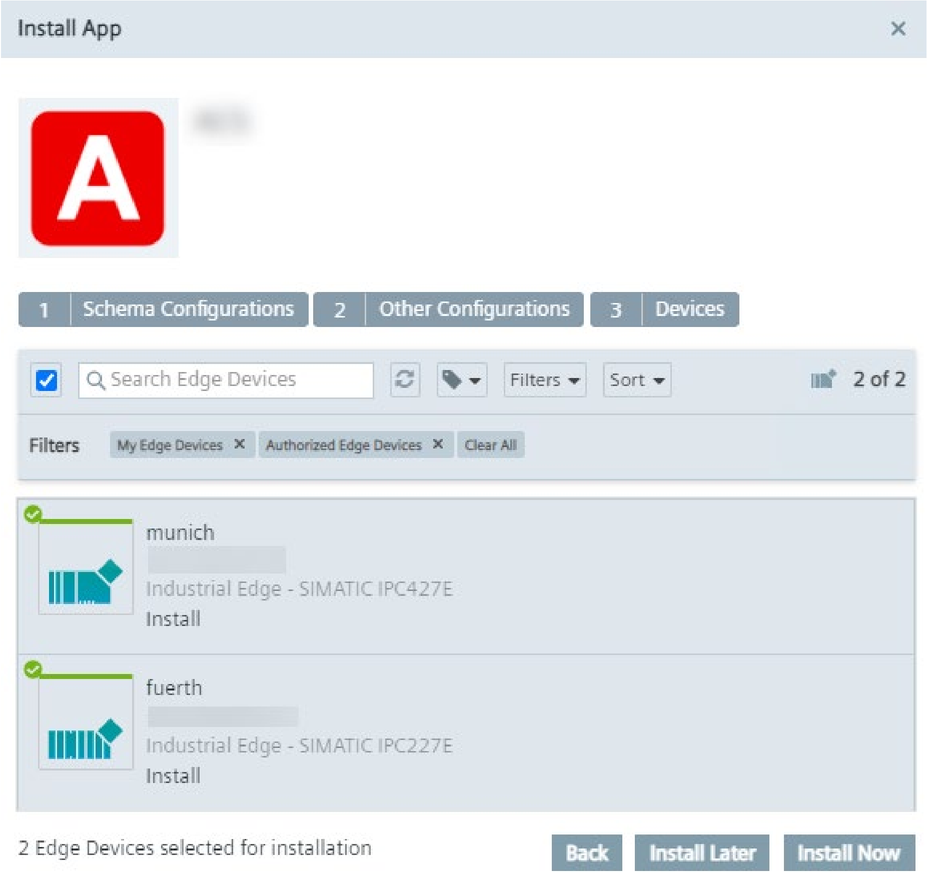
Install App

Simple-versioned-config
Full Path: ./cfg-data
v1.0.0

Unversioned-config
Full Path: ./cfg-data

Simple-templated-config
Full Path: ./cfg-data
Simple-templated-config

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



munich
Industrial Edge - SIMATIC IPC427E
Install

fuerth
Industrial Edge - SIMATIC IPC227E
Install

2 Edge Devices selected for installation

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

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

   Note

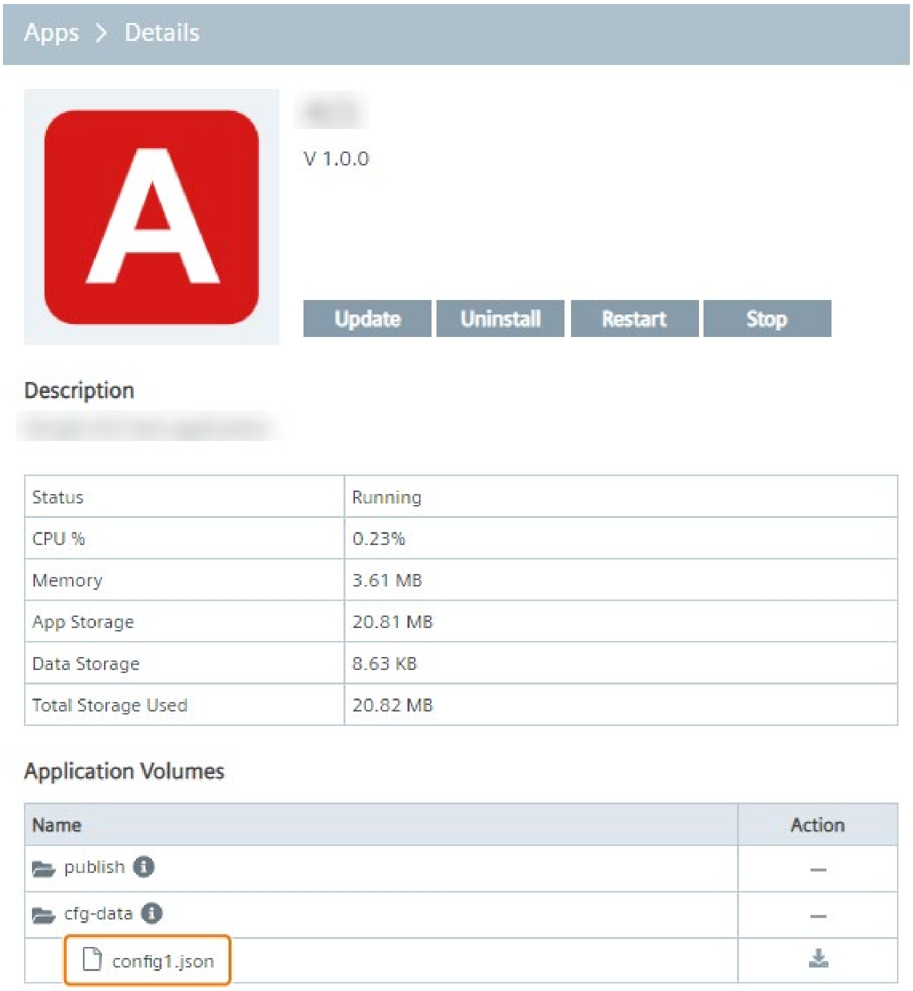
   Installation date and time

   When you select "Install Later", a calendar and the local system time is displayed for selecting the installation date and time.

   The "Install" screen is displayed which shows capabilities and services which will be used by the app. The layout of the screen depends on the Edge App which you can check in the "Installing an app from my projcts (Page 191)" subsection.

9. To install the app, click "Allow".

   The app is being installed now or at the selected date and time. After the installation is completed, you can find and check the selected app configurations in the application volumes section under the app details.



Status	Running
CPU %	0.23%
Memory	3.61 MB
App Storage	20.81 MB
Data Storage	8.63 KB
Total Storage Used	20.82 MB

Application Volumes

Name	Action
publish	—
cfg-data	—
config1.json	

Note

IE ACS not installed but used in the app

If the IE ACS is not installed but enabled in the app, the default configuration options for template based configurations are used.

10.9 Updating an app configuration via the IE ACS

Requirement

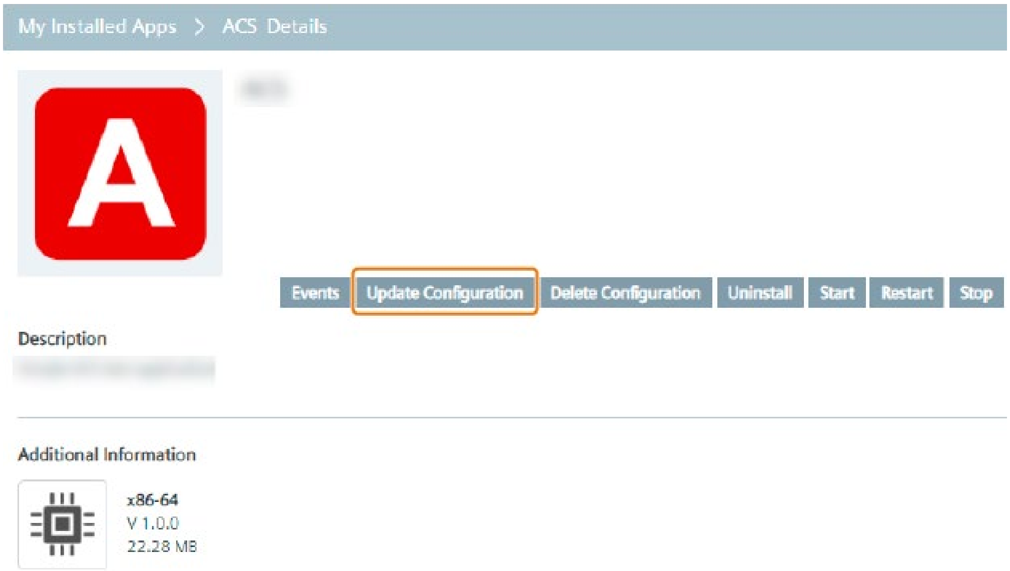
- IE ACS must be installed in the IEM-OS.
- App configuration is compatible with the IE ACS.

Procedure

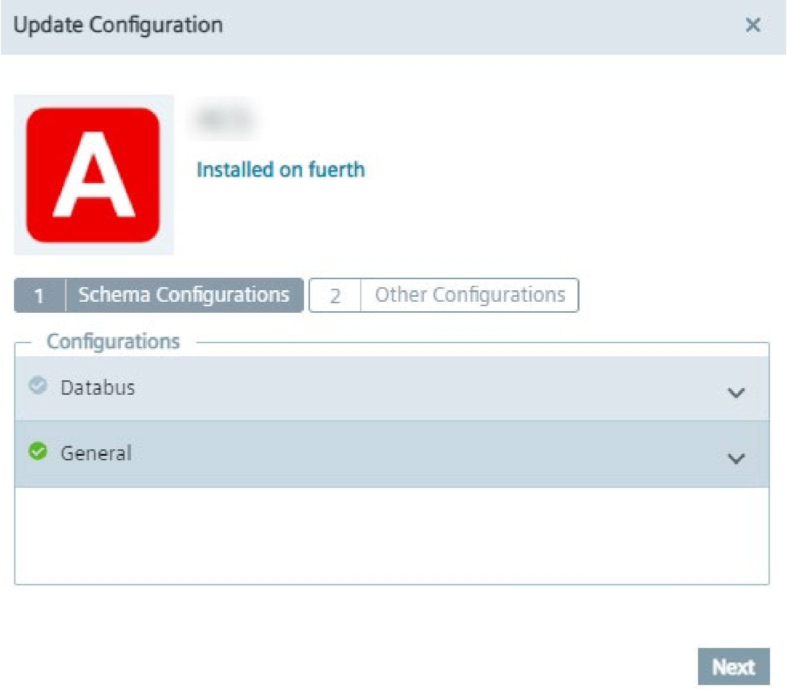
1. In the Management UI, navigate to "My Installed Apps".
2. Click the respective app tile.

   The details screen is displayed.

3. In the details screen of the app, click "Update Configuration".



The "Update Configuration" screen of the app is displayed. When the IE ACS is installed and the IE ACS is enabled in the app, the IE ACS is rendered again. The IE ACS displays the configuration state which was used when the app has been installed. When an app configuration was configured and selected during the installation of the app, the respective app configuration is preselected.



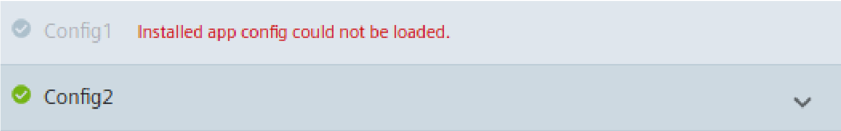
4. Update the app configuration as needed.

5. When all app configurations are valid, click "Next".
6. Click "Update".

   The app configuration has been updated. You can find and check the updated app configurations again in the application volumes section under the app details.

Errors

If problems occur when fetching configuration information from the IEM, this is indicated in the ACS. In this case, the respective configuration is disabled and an error message is displayed, as displayed in the following figure for example:



Config1 Installed app config could not be loaded.

Config2

In this case, you can only interact with the second configuration.

10.10 Privileged and network mode

When you create an app or a new version of an app in the IE App Publisher, you have the possibility to choose the privileged or the network mode.

When you install an app, the privileged and the network mode are important because they allow the app additional privileges.

Privileged mode

The privileged mode allows app services to access root resources. Some services in the *.yaml configuration file of the app request to run in privileged containers. Privileged containers have all root capabilities of the host which allows them to access resources which are not accessible in ordinary containers. For example, if a service requires direct hardware access or uses the host's kernel functions, you must enable the privileged mode.

Network mode

The network mode allows apps to run on the host network. When you enable the network mode for an app, the app container shares the host's networking namespace and the container does not get its own IP address. For example, if you run a container which binds to port 80 and you use the network mode, the container is available on port 80 on the host's IP address.

10.11 Updating Edge Apps via the IE App Publisher

If you want to update an app via the IE App Publisher, you must create a new app version in the IE App Publisher.

For this, you must first import the current version of the app to the IE App Publisher, if the app is not there yet. Then in the IE App Publisher, you create a new version of the required app. After you created the new version of the app, you upload the version to the IEM. From there, you install the new app version on the required Edge Devices.

The following procedures describe the import of an app to the IE App Publisher and the upload of a new app version to the IEM. You find the procedure on how to create a new version of the app in the "Creating an Edge App version" subsection in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

10.11.1 Importing an Edge App to IE App Publisher

If the app is not yet available in the Industrial Edge App Publisher, you must first import the current version of the app to the Industrial Edge App Publisher.

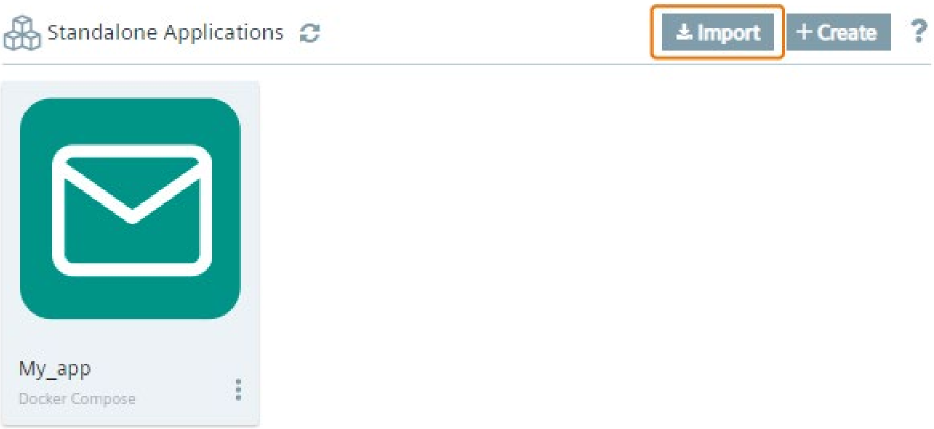
If the app is already available in the Industrial Edge App Publisher, proceed with creating a new version of the app in the Industrial Edge App Publisher as described in the "Creating an Edge App version" subsection in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

Requirement

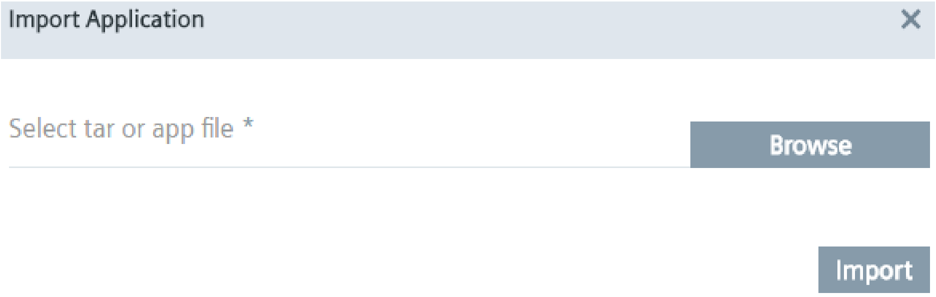
- The IE App Publisher is installed on the PC.
- The Edge App is downloaded and available in the "*.app" file format.
- You are a registered user in the IEM.
- You have created minimum 1 project in the Management UI of the IEM.
- The IEM is running.

Procedure

1. Launch the IE App Publisher.
2. Under the "Standalone Applications" section, click "Import".



The "Import Application" screen is displayed.



3. Click "Browse" and select the required Edge App in the "*.app" file format.
4. Click "Import".

   When the import was successful, an according message is displayed. The app is now available in the "Standalone Applications" section.
   Now, create a new version of the app in the IE App Publisher as described in the "Creating an Edge App version" subsection in the "Industrial Edge App Publisher - Operation (https://support.industry.siemens.com/cs/us/en/view/109780392)" manual.

10.11.2 Uploading an Edge App to the IEM

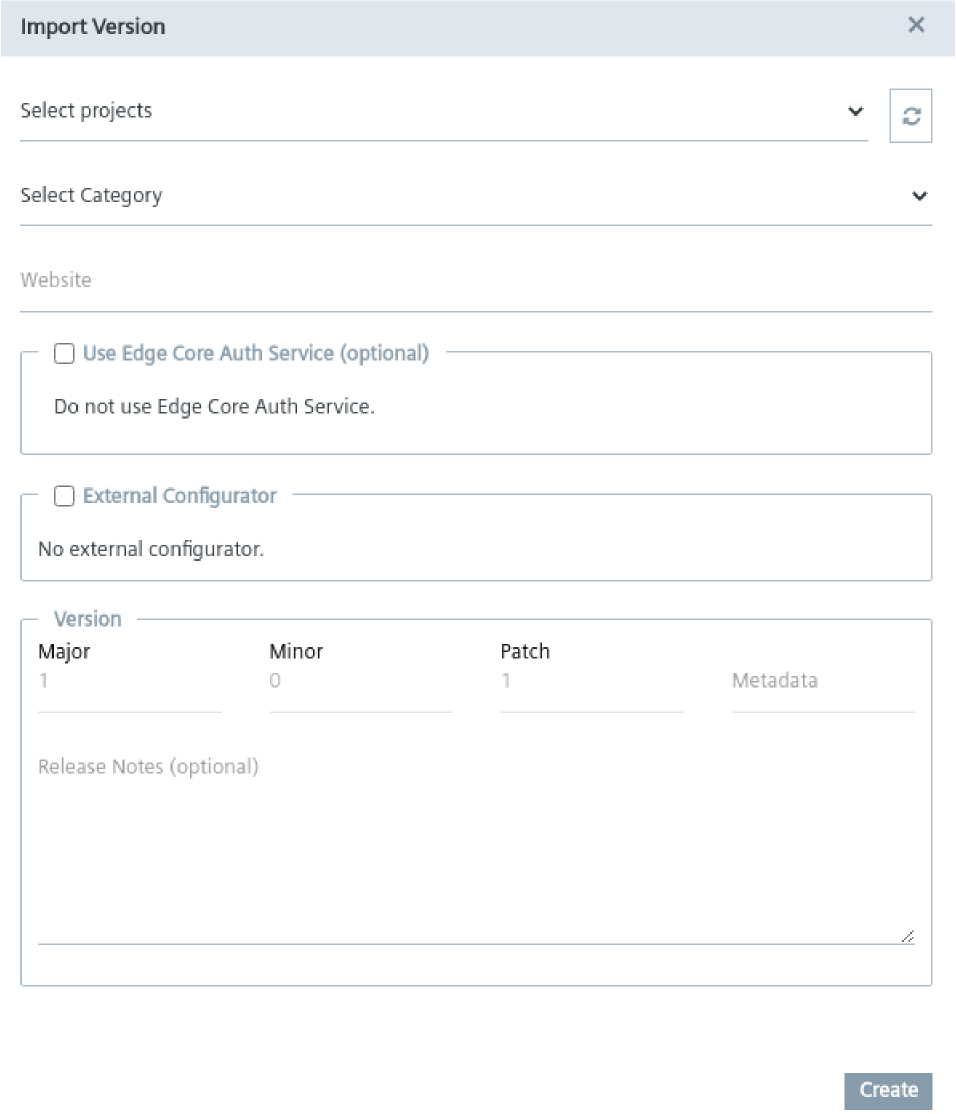
Requirement

- The new app version has been created.
- You must be a registered user in the IEM in which you want to upload the app.
- The IE App Publisher is connected to the IEM in which you want to upload the app.
- The IE App Publisher is connected to a Docker Engine.

Procedure

1. Click the tile of the app under the "Standalone Applications" section that you want to upload to the IEM.
2. Click the ↗ icon under "Actions" of the new version.
3. Select "My Project".

   The "Import Version" screen is displayed.



□ Use Edge Core Auth Service (optional)

Do not use Edge Core Auth Service.

□ External Configurator

No external configurator.

Version

Major	Minor	Patch	Metadata
1	0	1	

Release Notes (optional)

4. Select the project that you created in the Management UI of the IEM from the "Select projects" drop-down list.
5. Select the required category from the "Select Category" drop-down list.
6. Enter the website of the app publisher in the "Website" input field, for example www.siemens.com.

7. If necessary, enable the "Use Edge Core Auth Service" check box.

   You find more information on this option in the "Creating an app - Parameters (Page 174)" subsection.

8. If necessary, enable the "External Configurator" check box and enter the URL of the external app configurator.

   You find more information on the external configurator in the "Enabling the external configurator (Page 176)" subsection.

9. If required, add release notes to the app version under "Release Notes".

10. Click "Create".

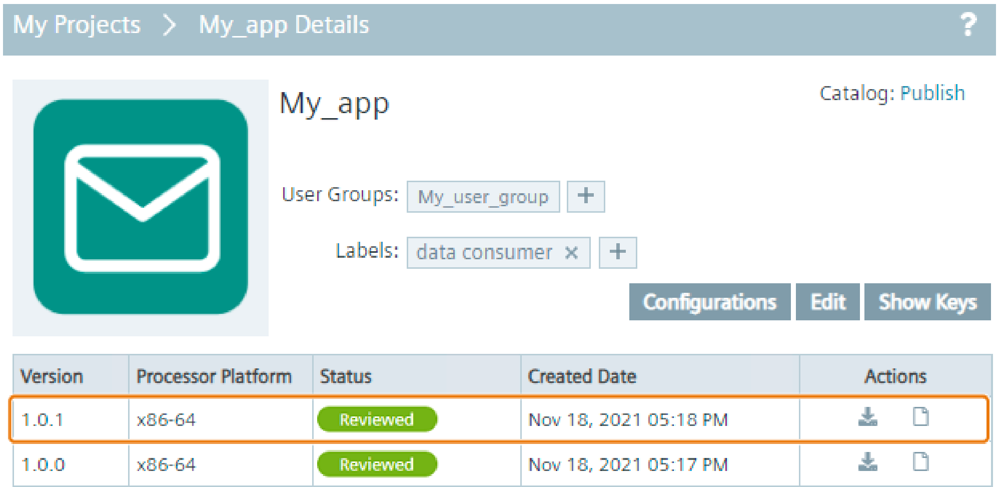
    The app version is created and the app is now listed in the IE App Publisher under the "My Projects" section of the according project.

11. Click the tile of the app under the "My Projects" section in the IE App Publisher.

12. Click Start Upload of the newly created version.

    The app version is being uploaded to the IEM. When the upload was successful, an according message is displayed.

    The app version is now available in the Management UI under "App Projects".



My_app

Catalog: Publish

User Groups: My_user_group +

Labels: data consumer × +

Version	Processor Platform	Status	Created Date	Actions
1.0.1	x86-64	Reviewed	Nov 18, 2021 05:18 PM	
1.0.0	x86-64	Reviewed	Nov 18, 2021 05:17 PM	

You can now install the updated app on an Edge Device as described in the "Installing an app from my projects (Page 191)" subsection.

Groups

11

11.1 My User Groups

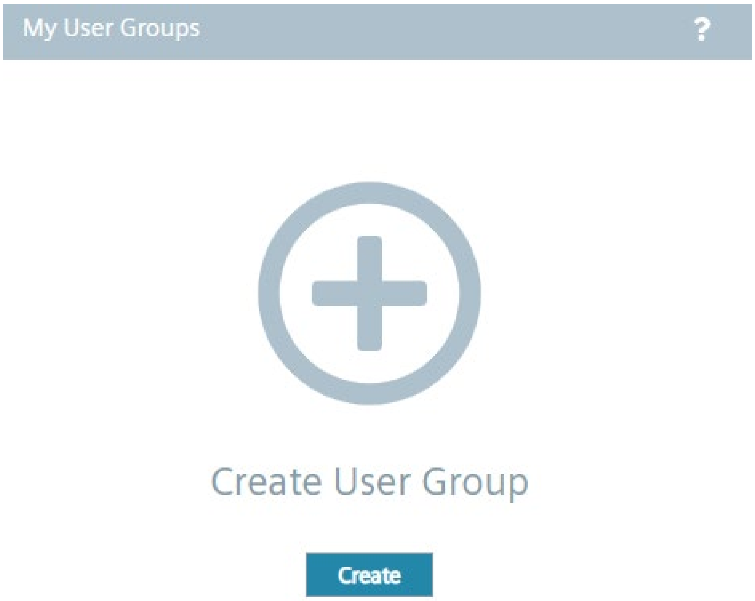
11.1.1 Overview

User groups enable access to private apps. In the "Groups > My User Groups" screen you create your own user groups and add new users to these groups. In that way, you share your private apps with members of the group.

After inviting new users to a user group, all members can develop any apps within this user group in parallel and share the apps. Depending on the permissions you give other group members, the members are, for example, just allowed to deploy apps on their Edge Devices or they contribute new apps and new versions of existing apps to your user group.

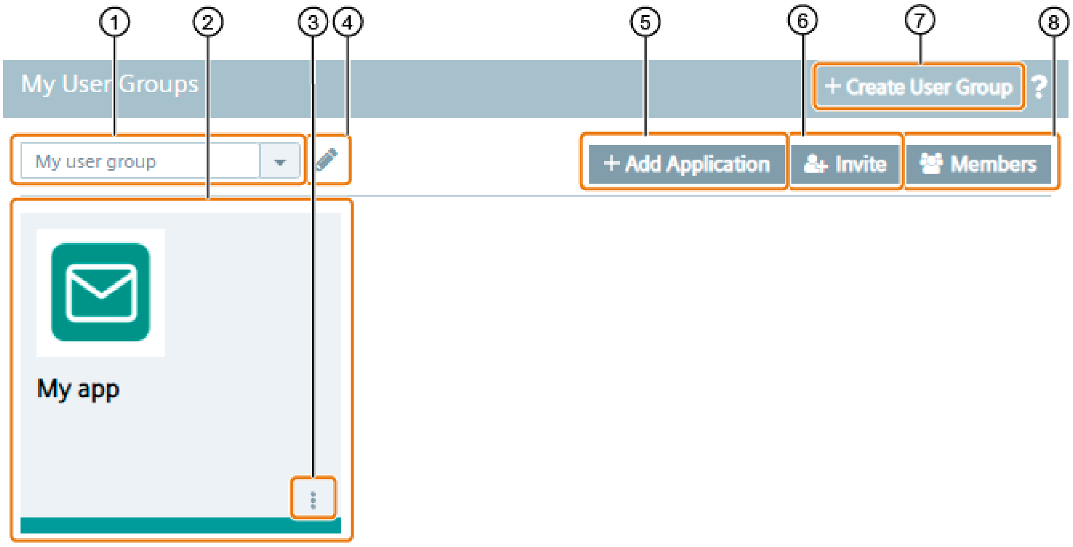
The layout of the "My User Groups" screen varies depending on whether or not you have already created an user group.

If you have created no groups yet, the "My User Groups" screen is displayed as follows:



Once you have created an user group and added apps to the user group, the "Create User Group" button is displayed on the right of the title bar of the "My User Groups" screen and the "Add Application" button is enabled.

The following figure shows an example with already added apps:



① Drop-down list of existing user groups

② Assigned apps to the user group

③ Editing apps in the user group

④ Editing the in ① selected user group

⑤ Assign an app to the user group

⑥ Invite new members to the user group

⑦ Create a new user group

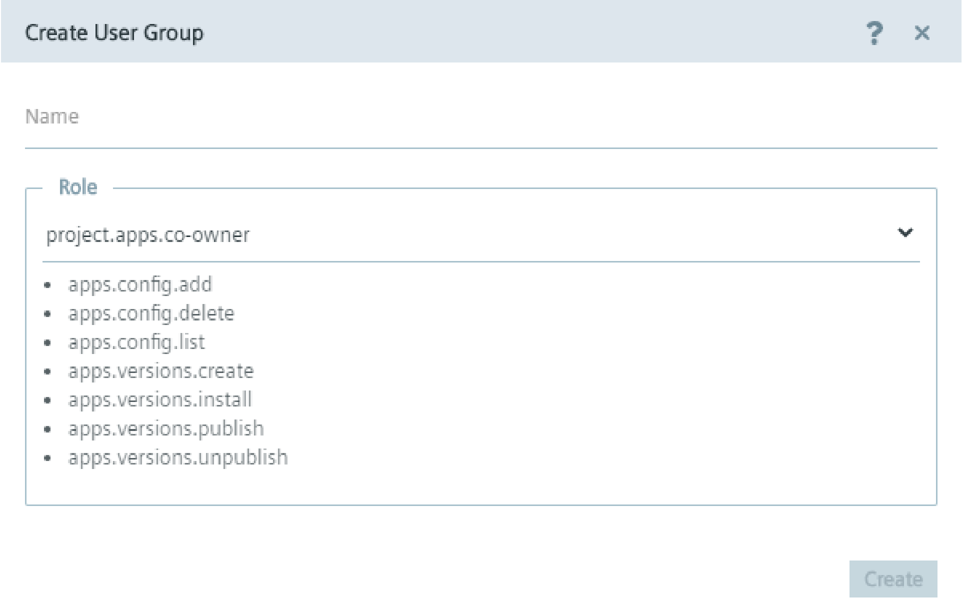
⑧ Display joined and pending users of the user group

11.1.2 Creating and editing a user group

Creating a user group

1. Click "Create User Group".

   The "Create User Group" screen is displayed.



Create User Group

Name

Role: project.apps.co-owner

- apps.config.add
- apps.config.delete
- apps.config.list
- apps.versions.create
- apps.versions.install
- apps.versions.publish
- apps.versions.unpublish

2. In the "Name" input field, enter the name of the user group.
3. From the "Role" drop-down list, select the role respectively permissions for all members of the user group.

   You get an overview about all available user roles and their permissions in the "Roles (Page 212)" subsection.
4. Click "Create".

   The user group is added to the user group drop-down list.

Editing a user group

1. From the user group drop-down list, select the user group you want to edit.
2. Click the ✎ icon next to the drop-down list.

   The "Edit User Group" screen is displayed.
3. Edit name of the user group and user roles for the members.
4. To save the changes, click "Update".
5. If you want to delete a user group, click "Delete".

11.1.3 Roles

The following are the available roles for user groups:

Role	Permissions
Co-owner	• App configurations: – Add – List – Delete • App versions: – Create new versions – Install – Publish – Unpublish • Create new app versions • Edit apps • Display app keys
Developer	• App configurations: – Add – List – Delete • App versions: – Create new versions – Install
Publisher	Publish and unpublish app versions
User	• App configurations: – Add – List – Delete • Install apps
Operator	• List app configurations • Install apps

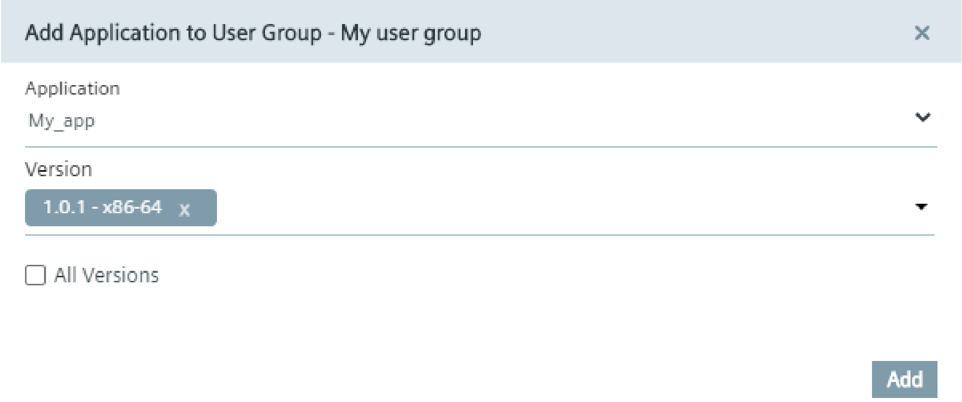
11.1.4 Adding apps

After creating an user group, you specify which apps you want to add to the user group.

Procedure

1. From the drop-down list, select the user group for which you want to add an app.
2. Click "Add Application".

   The "Add Application to User Group" screen is displayed.

   Add Application to User Group - My user group

   Application
   My_app

   Version
   1.0.1 - x86-64

   □ All Versions

3. From the "Application" drop-down list, select the app you want to add to the user group.
4. If several app versions are available, select the required app versions from the "Version" drop-down list.

   You add all available versions of the app to the user group by clicking the "All Versions" check box.
5. Click "Add".

   The app is added to the user group.

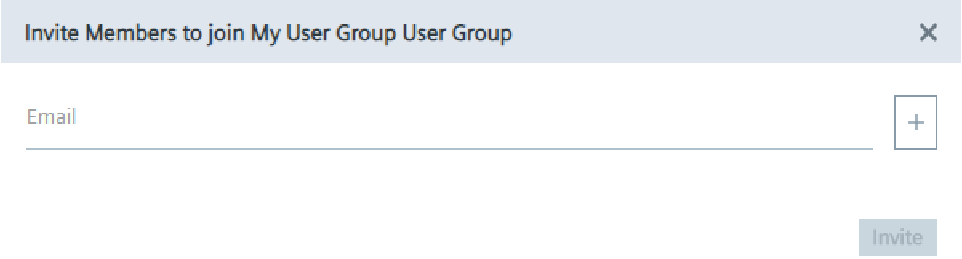
11.1.5 Inviting members

After assigning an app to an user group, you invite new users to the user group and manage the list of invited users.

Procedure

1. From the drop-down list, select the user group for which you want to invite a new user.
2. Click "Invite".

   The "Invite Members to join My User Group" screen is displayed.

   Invite Members to join My User Group User Group

   Email

3. In the "Email" input field, enter the email address of the user you want to add to the user group.
4. If you want to add more users to the user group, click the + icon.

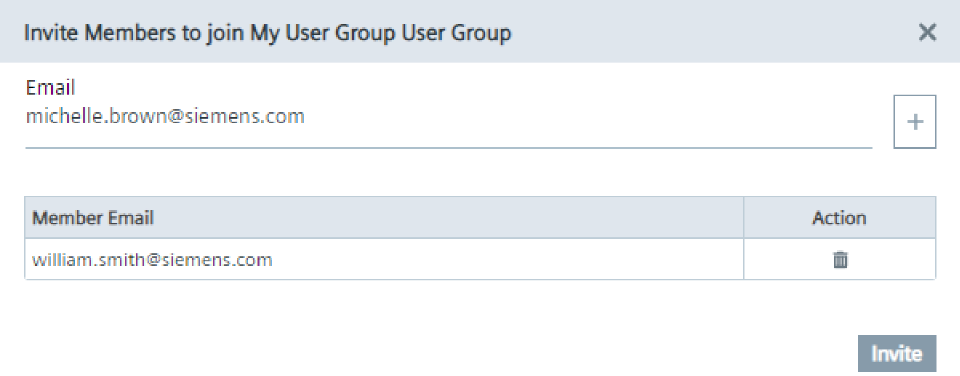
   The previously entered user is listed in the "Member Email" table.

   Note

   Deleting users

   If you want to delete a user from the user group, click the 🗑 icon for the required user.

5. In the "Email" input field, enter the email address of the next user you want to add to the user group.



Invite Members to join My User Group User Group ✕

Email
michelle.brown@siemens.com +

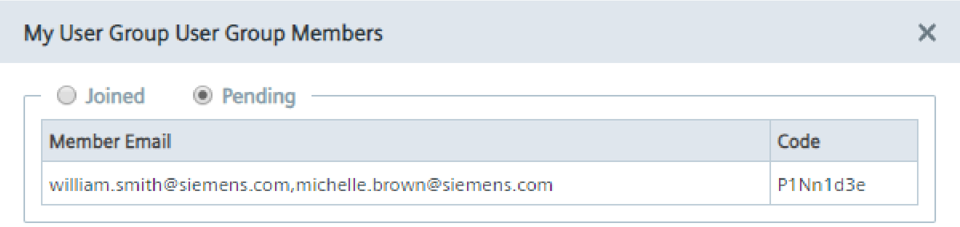
Member Email	Action
william.smith@siemens.com	🗑

6. To add the listed users to the user group, click "Invite".

   An invitation code is generated which you must send manually to the added users. The invited users then enter the invitation code in the "Authorized Applications" screen after clicking "Accept Invitation".

Invited members

When you click "Members", all joined and still pending members are displayed. To remove an user from the user group, click the 🗑 icon for the required user in the "Joined" user list. When you click the "Pending" option button, all pending users and the specific invitation code are displayed in case of resending the code to the specific users.



My User Group User Group Members ✕

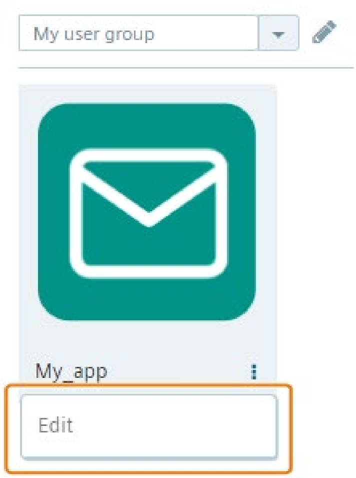
○ Joined ● Pending

Member Email	Code
william.smith@siemens.com,michelle.brown@siemens.com	P1Nn1d3e

11.1.6 Editing apps

Removing apps

1. In the "My User Groups" screen, click the ⋮ icon of the required app .
2. Click "Edit".



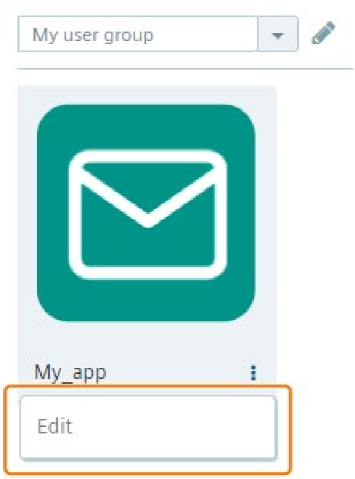
   The "Edit Application in User Group" screen is displayed.
3. From the "Version" drop-down list, select the versions of the app you want to remove.
4. Click "Remove".

   The versions are removed from the user group.

   When you select the "All Versions" check box and click "Remove", the whole app is removed.

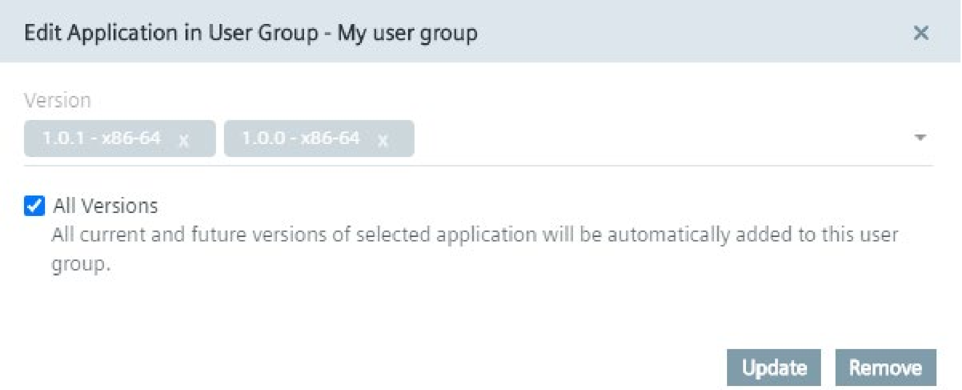
Adding automatically new app versions

1. In the "My User Groups" screen, click the ⋮ icon of the app for which you want to add new app versions automatically to the user group.
2. Click "Edit".



The "Edit Application in User Group" screen is displayed.

3. Check the "All Versions" check box.


Edit Application in User Group - My user group

Version

1.0.1 - x86-64 x
1.0.0 - x86-64 x

☑ All Versions
All current and future versions of selected application will be automatically added to this user group.

4. Click "Update".

All current and future versions of the selected app will be automatically added to this user group.

11.2 My Admin Groups

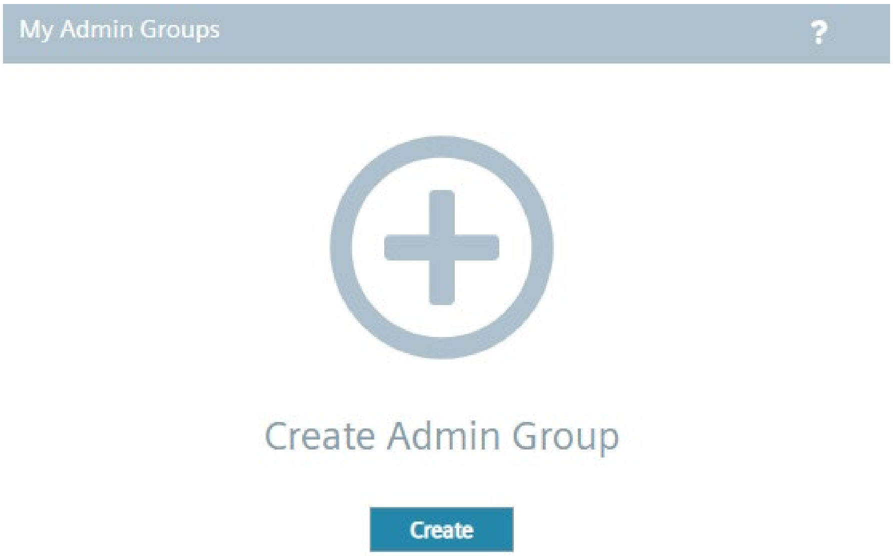
11.2.1 Overview

Admin groups enable access to Edge Devices. In the "Groups > My Admin Groups" screen you create groups and add new users to these groups. In that way, you share your Edge Devices with members of the group.

After inviting new users to a group, all members of the group have access to any Edge Devices within this group. Depending on the permissions you give other group members, the members are, for example, just allowed to reboot or shutdown Edge Devices.

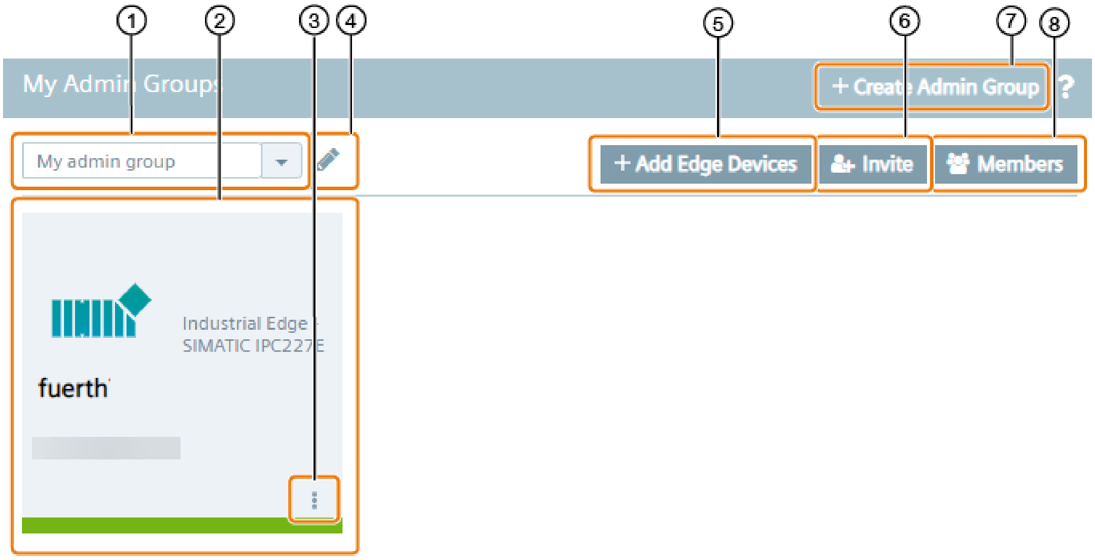
The layout of the "My Admin Groups" screen varies depending on whether or not you have already created an admin group.

If you have created no groups yet, the "My Admin Groups" screen is displayed as follows:



Once you have created an admin group, the "Create Admin Group" button is displayed on the right of the title bar of the "My Admin Groups" screen and the "Add Edge Devices" button is enabled.

The following screen shows an example with an already added Edge Device:



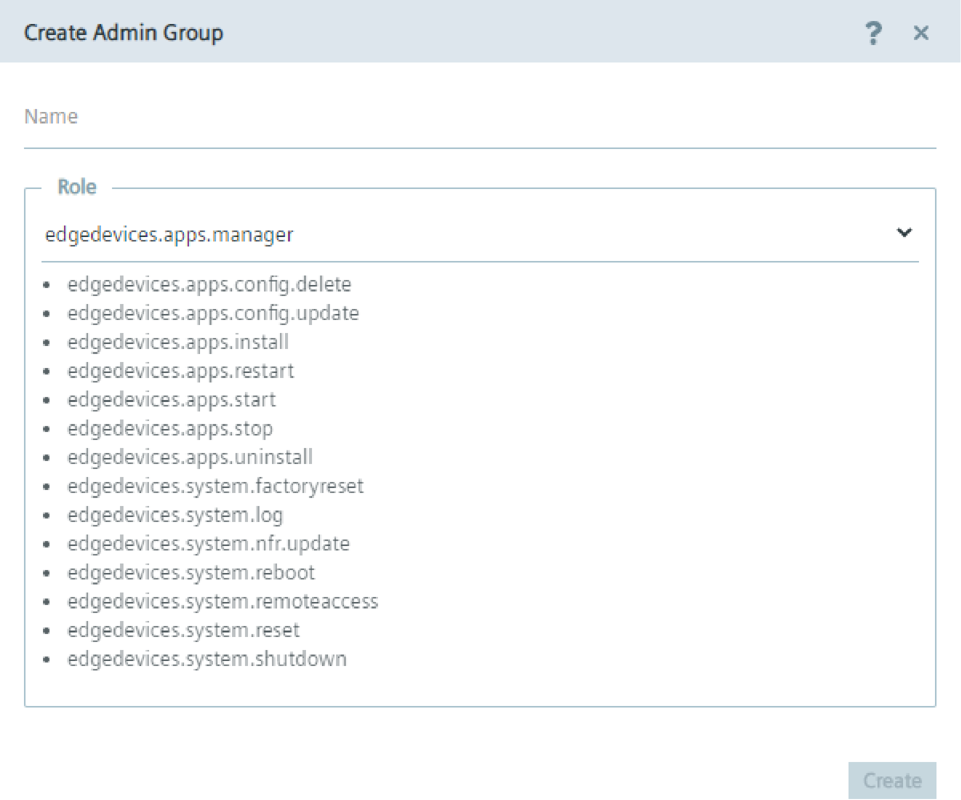
① Drop-down list of existing admin groups
② Assigned Edge Devices to the group
③ Removing Ede Devices from the group and opening Edge Device statistics
④ Editing the in ① selected group
⑤ Adding an Edge Device to the group
⑥ Invite new members to the group
⑦ Create a new admin group
⑧ Display joined and pending users of the group

11.2.2 Creating and editing an admin group

Creating an admin group

1. Click "Create Admin Group".

   The "Create Admin Group" screen is displayed.



Create Admin Group

Name

Role

edgedevices.apps.manager

- edgedevices.apps.config.delete
- edgedevices.apps.config.update
- edgedevices.apps.install
- edgedevices.apps.restart
- edgedevices.apps.start
- edgedevices.apps.stop
- edgedevices.apps.uninstall
- edgedevices.system.factoryreset
- edgedevices.system.log
- edgedevices.system.nfr.update
- edgedevices.system.reboot
- edgedevices.system.remoteaccess
- edgedevices.system.reset
- edgedevices.system.shutdown

2. In the "Name" input field, enter the name of the group.
3. From the "Role" drop-down list, select the role respectively permissions for all members of the admin group.

   You get an overview about all available roles and their permissions in the "Roles (Page 221)" subsection.
4. Click "Create".

   The group is added to the drop-down list.

Editing an admin group

1. From the drop-down list, select the group you want to edit.
2. Click the ✎ icon next to the drop-down list.

   The "Edit Admin Group" screen is displayed.
3. Edit name of the group and roles for the members.
4. To save the changes, click "Update".
5. If you want to delete a group, click "Delete".

11.2.3 Roles

The following are the available roles for admin groups:

Role	Permissions
Co-admin	• Shared Edge Devices: – Reboot – Shutdown – Reset – Hard reset – Update – Delete – Import certificates – Manage labels – Download logs – Update NFR settings – Enable/Disable remote access – Add/Delete/Display tags • Apps on shared Edge Devices: – Update configuration – Delete configuration – Install – Uninstall – Restart – Start – Stop
Apps manager	• Shared Edge Devices: – Reboot – Shutdown – Reset – Hard reset – Download logs – Update NFR settings – Enable/Disable remote access • Apps on shared Edge Devices: – Update configuration – Delete configuration – Install – Uninstall – Restart – Start – Stop

Role	Permissions
Manager	• Shared Edge Devices: – Update – Delete

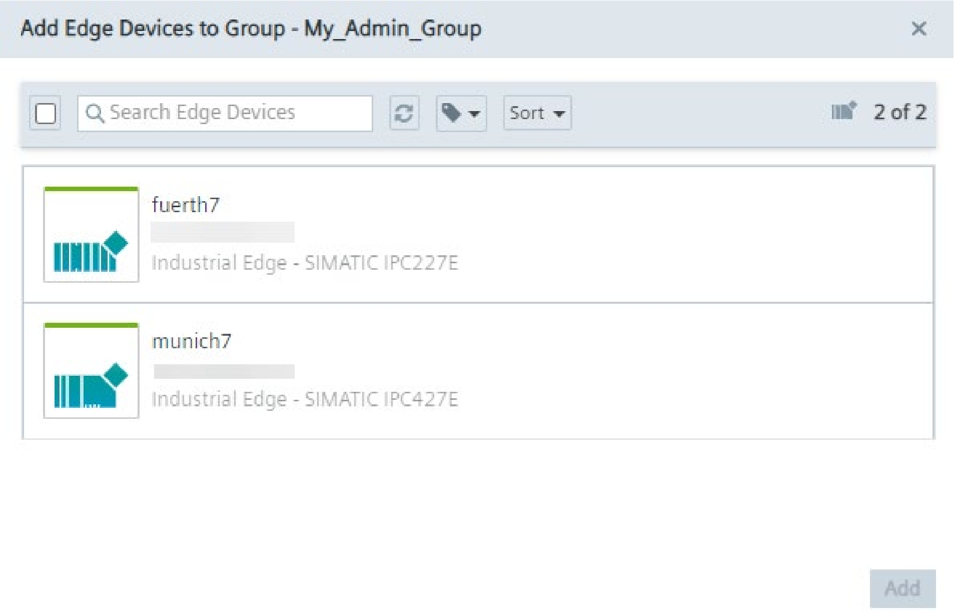
11.2.4 Adding an Edge Device

After defining permissions for a group, you specify which Edge Devices you want to share.

Procedure

1. From the drop-down list, select the group for which you want to share an Edge Device.
2. Click "Add Edge Devices".

   The "Add Edge Devices to Group" screen is displayed.



Add Edge Devices to Group - My_Admin_Group

□ Search Edge Devices | Sort | 2 of 2

fuerth7
Industrial Edge - SIMATIC IPC227E

munich7
Industrial Edge - SIMATIC IPC427E

Add

3. Select the Edge Devices you want to share to the group.
4. Click "Add".

   The Edge Devices are added to the group.

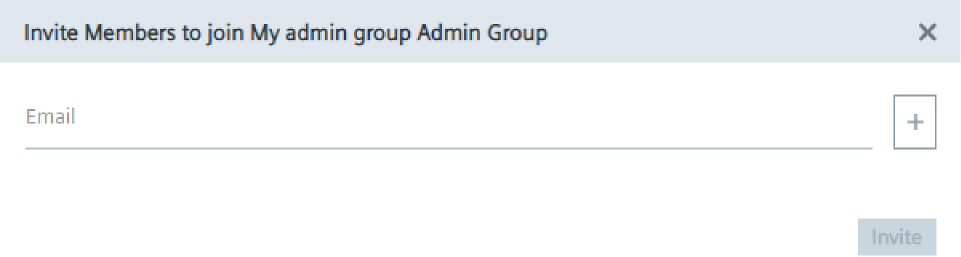
11.2.5 Inviting members

After assigning an Edge Device to an admin group, you invite new users to the admin group and manage the list of invited users.

Procedure

1. From the drop-down list, select the admin group for which you want to invite a new user.
2. Click "Invite".

   The "Invite Members to join My Admin Group" screen is displayed.



3. In the "Email" input field, enter the email address of the user you want to add to the group.
4. If you want to add more users to the group, click the + icon.

   The previously entered user is listed in the "Member Email" table.

Note

Deleting users

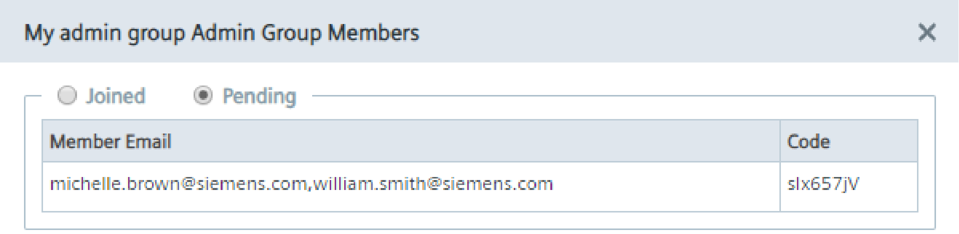
If you want to delete a user from the group, click the 🗑 icon for the required user.

5. In the "Email" input field, enter the email address of the next user you want to add to the group.
6. To add the listed users to the group, click "Invite".

   An invitation code is generated which you must send manually to the added users. The invited users then enter the invitation code in the "Authorized Edge Devices" screen after clicking "Accept Invitation".

Invited members

When you click "Members", all joined and still pending members are displayed. To remove a user from the admin group, click the 🗑 icon for the required user in the "Joined" user list. When you click the "Pending" option button, all pending users and the specific invitation code are displayed in case of resending the code to the specific users.



○ Joined ● Pending

Member Email	Code
michelle.brown@siemens.com,william.smith@siemens.com	slx657jV

11.2.6 Joining other groups

To join another group, the owner of the group must invite you to the group. After the owner invites you, the owner sends you the invitation code to join the group.

Members of a group can, depending on the permissions, for example install private apps to shared Edge Devices.

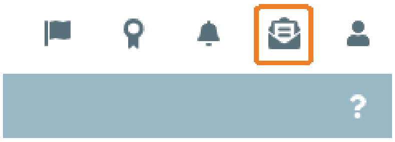
The permissions of a group are listed in the "Roles (Page 221)" subsection.

Requirement

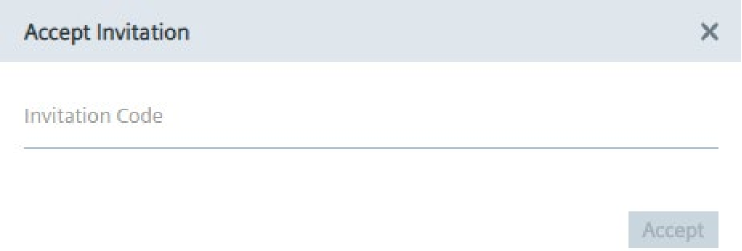
The invitation code is received.

Procedure

1. In the top-right corner, click the icon to accept an invitation.



The "Accept Invitation" screen is displayed.


Accept Invitation

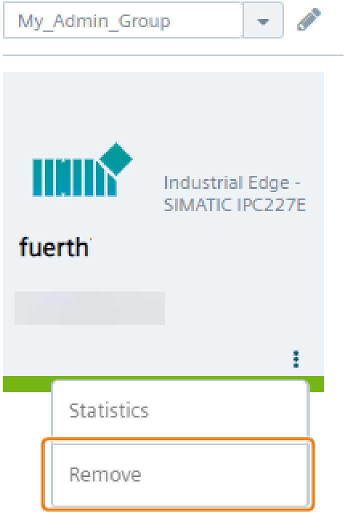
2. In the "Invitation Code" input field, enter the invitation code that you received from the owner of the group.
3. Click "Accept".

   If the invitation code is valid, all Edge Devices that were assigned to the group are now available.

11.2.7 Removing and checking Edge Devices

Removing Edge Devices

1. In the "My Admin Groups" screen, click the ⋮ icon of the Edge Device you want to remove from the group.
2. Click "Remove".



   The "Remove Edge Device" screen is displayed.
3. Click "Remove".

   The Edge Device is removed from the group.

Checking Edge Device statistics

1. Click the ⋮ icon of the Edge Device for which you want to check its statistics.
2. Click "Statistics".

   The "Statistics" screen is displayed.

Note

Connecting to the Edge Device

If the remote access is enabled for the Edge Device, you open the UI of the Edge Device by clicking "Connect".

Job Status

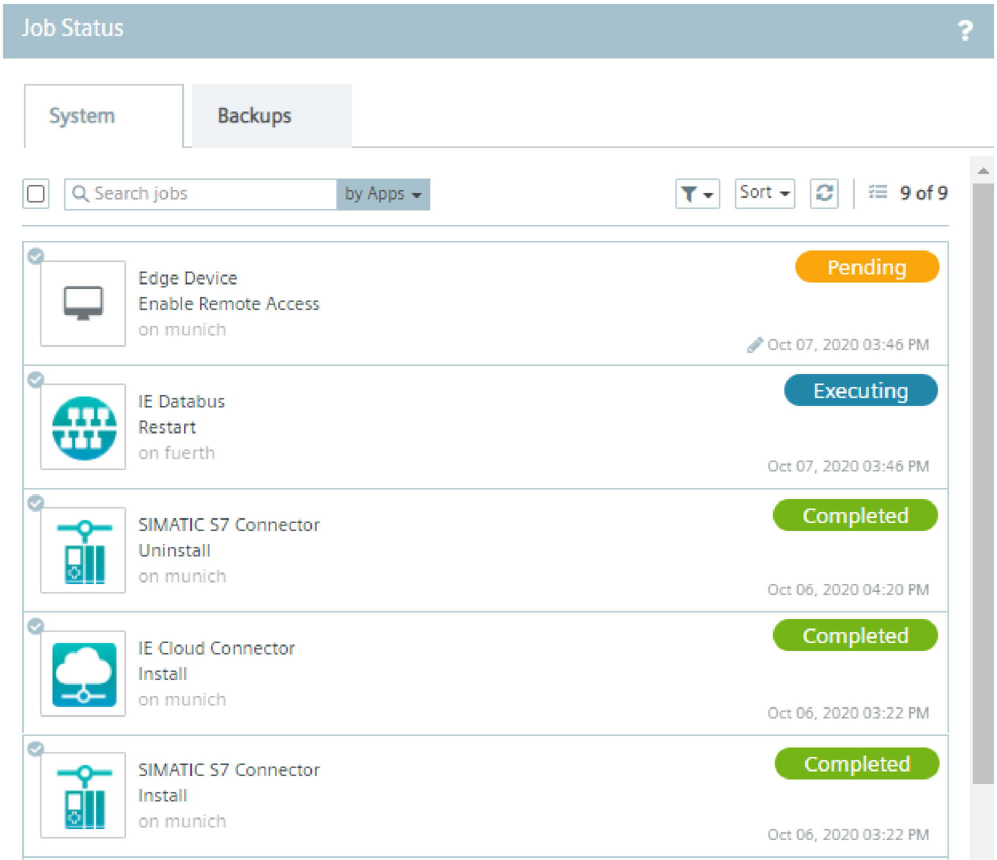
12

12.1 Overview

When you, for example, install an app or restart an Edge Device or perform a backup of an IED state, an according job is created and performed in the IEM. The "Job Status" screen provides a possibility to check all performed jobs. Jobs related to apps and Edge Devices are listed under the "System" tab, jobs regarding backup and restore operations of Edge Devices are listed under the "Backups" tab. Each job is displayed in an own row. At the end of each row, the status of the performed job is displayed, for example whether or not the job execution was successful.

Apps and Edge Devices jobs

Jobs related to apps and Edge Devices are displayed as follows for example:



Edge Device
Enable Remote Access
on munich
Pending
Oct 07, 2020 03:46 PM

IE Databus
Restart
on fuerth
Executing
Oct 07, 2020 03:46 PM

SIMATIC S7 Connector
Uninstall
on munich
Completed
Oct 06, 2020 04:20 PM

IE Cloud Connector
Install
on munich
Completed
Oct 06, 2020 03:22 PM

SIMATIC S7 Connector
Install
on munich
Completed
Oct 06, 2020 03:22 PM

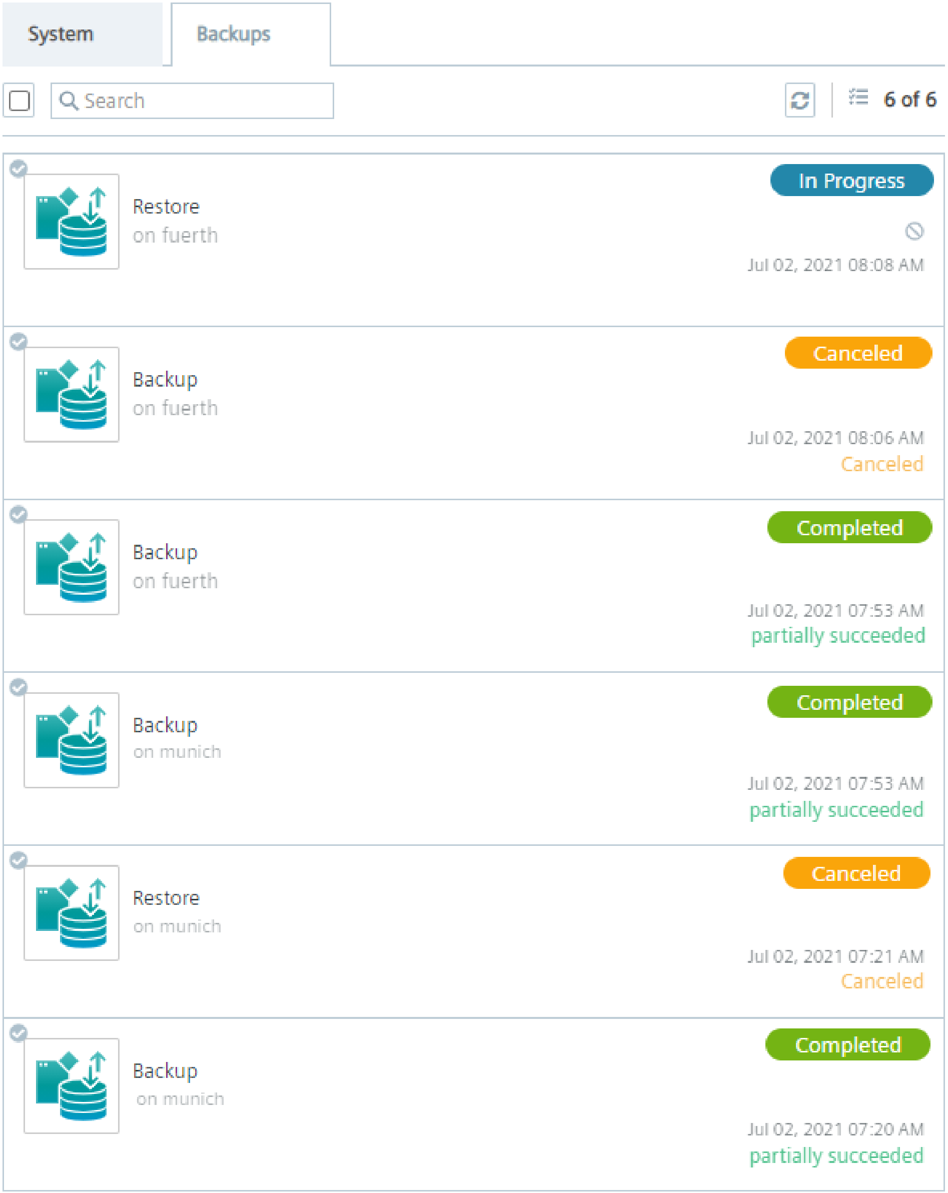
You have the possibility to perform the following:

- Delete jobs: By selecting 1 or more jobs, the selected jobs are marked and the 🗑 icon is enabled with which you delete the corresponding jobs. You can also cancel respectively delete pending jobs if the respective jobs have not reached yet the IED respectively if the respective jobs are not displayed yet in the task manager in the Edge Device UI.

- Search jobs: By entering keywords in the "Search jobs" input field, you search the jobs for the entered keywords with regard to apps or Edge Devices jobs. To start the job search, press <Enter> after entering the keywords.
- Filter jobs: With the ⏷ ▾ icon you filter the job table regarding job status and several operations.
- Sort jobs: Sort the job table with the Sort ▾ icon.
- Refresh the jobs table: You refresh the job table by clicking the ⟳ icon.

Backup and restore jobs

Jobs related to backup and restore operations are displayed as follows for example:



Restore
on fuerth
In Progress
Jul 02, 2021 08:08 AM

Backup
on fuerth
Canceled
Jul 02, 2021 08:06 AM
Canceled

Backup
on fuerth
Completed
Jul 02, 2021 07:53 AM
partially succeeded

Backup
on munich
Completed
Jul 02, 2021 07:53 AM
partially succeeded

Restore
on munich
Canceled
Jul 02, 2021 07:21 AM
Canceled

Backup
on munich
Completed
Jul 02, 2021 07:20 AM
partially succeeded

You can also delete backup and restore jobs, search for Edge Devices and refresh the table as described for apps and Edge Devices jobs.

When you perform a backup or restore of an IED state, an according job is created and displayed with the "In Progress" status. You can cancel the operation while the job is in "In Progress" status by clicking the ⊘ icon. Confirm the cancelation by clicking "Stop" in the displayed screen. When you cancel a backup or restore job, the status switches to "Canceling". Until all corresponding jobs are finished, the backup or restore job will be in "Canceling" status. Once the job has been canceled, the status displays "Canceled". When the restore job has been canceled, a reset will be triggered to keep the Edge Device in a consistent state. A partly stored IED state will be deleted completely, a partly restored Edge Device will get reset again.

Not enough disk space for backup data

When storing an IED state of an Edge Device (Edge Device backup), the "Something went wrong - please retry" error message might occur when the process has failed. If this error message is displayed, check whether there is still enough free disk space available in the hard disk for storing backup data since this might be the failure reason. You can check the free and used disk space in the "Statistics (Page 27)" subsection of the Maintenance UI.

Job status

The following are the possible job status:

Scope	Job status	Description
Apps and Edge Devices	Pending	The job is submitted
	Skipped	The execution was skipped
	Executing	The job is processing
	Failed	The execution has failed
	Completed	The execution was successful
Backup and restore	In Progress	Backup or restore job is in progress
	Canceling	Backup or restore job is being canceled
	Canceled	Backup or restore job has been canceled
	Error	Backup or restore could not be executed
	Completed	The execution was successful

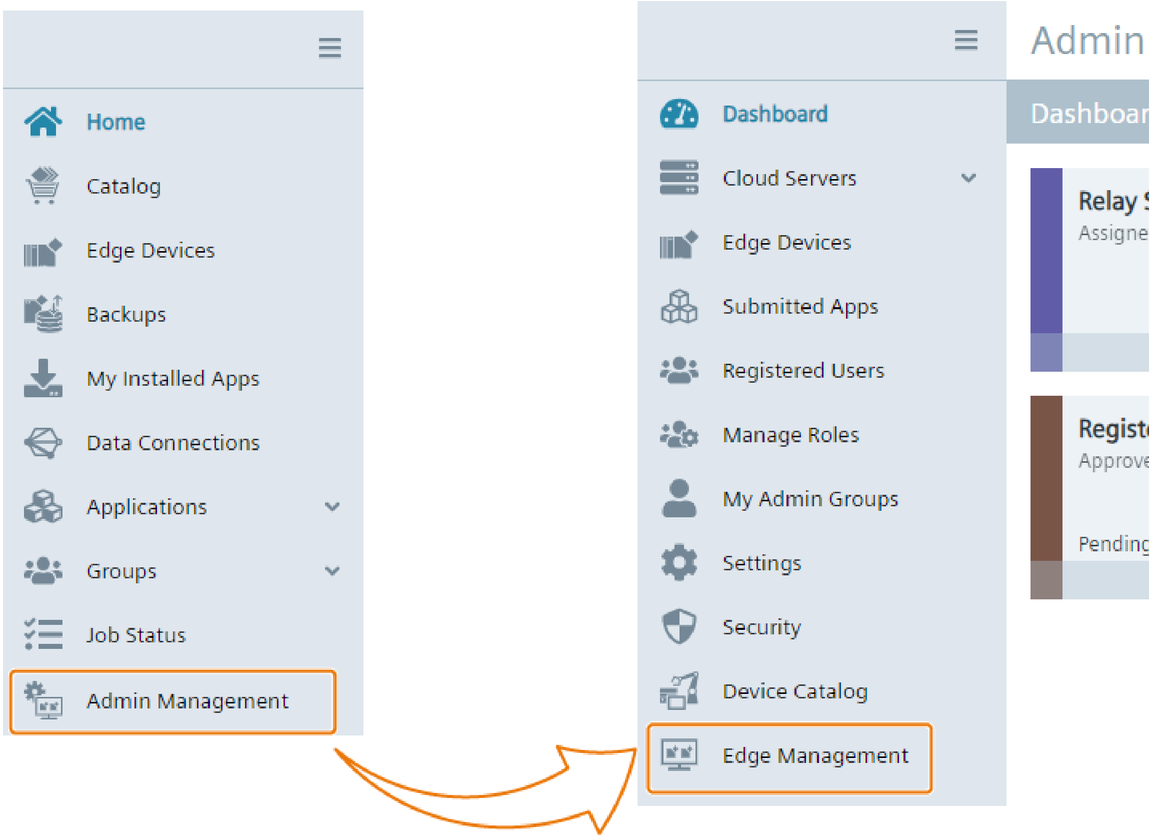
Admin UI 13

13.1 Overview

The Admin UI provides additional functionality to configure the IEM. Also, the Admin UI gives an overview about the whole system, for example how many Edge Devices are connected to the IEM or which users have access to the IEM.

Opening and closing the Admin UI

Only the admin of the IEM and users with the according permissions can open the Admin UI. For the admin and these specific users, the "Admin Management" menu item is enabled in the navigation menu. By clicking this menu item, the "Dashboard" screen of the Admin UI will be opened. To close the Admin UI and to return to the Management UI, click the "Edge Management" menu item.



Alerts

By clicking the 🔔 icon in the header of the Admin UI, the "Alerts" screen is displayed. This icon is only available for the admin of the IEM.

The "Alerts" screen displays, for example, the following alerts and notifications:

- Certificate expiry alerts, for the IEM and for the Registry server
- Certificate updated alerts
- Invalid certificate alerts, for example if certificate start date is after current date
- Certificate expired alert, for example if certificate is expired and the Edge Device owner has not responded for 15 days

Accept invitations

When you are not the admin of the IEM but have admin permissions, the 🔔 icon is displayed instead of the ✉ icon in the header of the Admin UI. This icon is used to accept invitations and join other groups in which you are invited. By clicking this icon, enter the invitation code you received to join a group.

Navigation

To navigate within the Admin UI, use the navigation menu on the left.

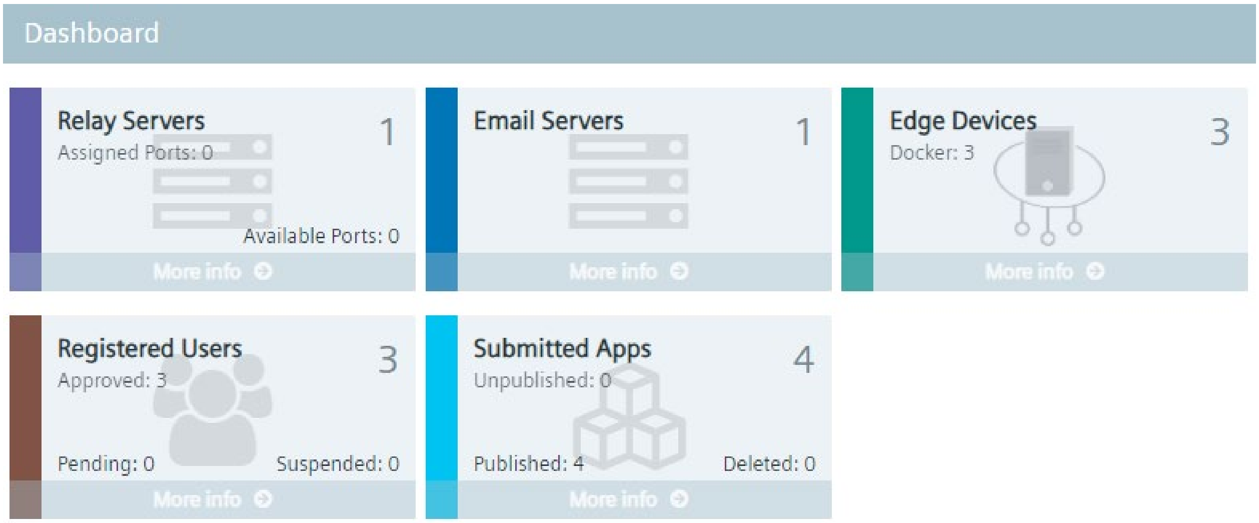
The navigation menu consists of the following menu items:

- Dashboard
- Cloud Servers
- Edge Devices
- Submitted Apps
- Registered Users
- Manage Roles
- My Admin Groups
- Settings
- Security
- Device Catalog
- Edge Management

13.2 Dashboard

The "Dashboard" screen shows you multiple different information, for example number of connected Edge Devices and number of registered users, in a quick overview. The different information are presented as tiles which correlate to menu items of the Admin UI. By clicking "More Info" of a tile, you will be redirected to the according screen.

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



13.3 Cloud Servers

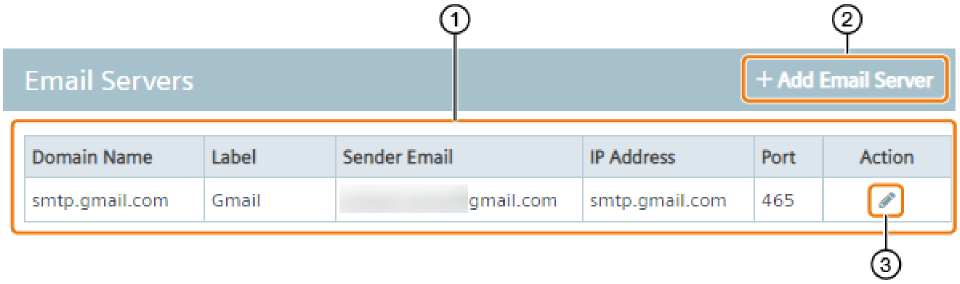
The "Cloud Servers" menu item consists of the following sub items:

- Relay Servers
- Email Servers

Each sub item lists the corresponding servers and provides you the possibility of adding new servers of that type.

Structure of each sub item

The sub items have the same structure. The following figure shows the structure of an added email server as an example:



Domain Name	Label	Sender Email	IP Address	Port	Action
smtp.gmail.com	Gmail	[redacted]gmail.com	smtp.gmail.com	465	✎

① Server list

A table with all servers of the specified type.

② Add Server

To add an email server, click this button.

③ Edit server

To edit the server, click this button.
You can edit the server configuration or delete the server.

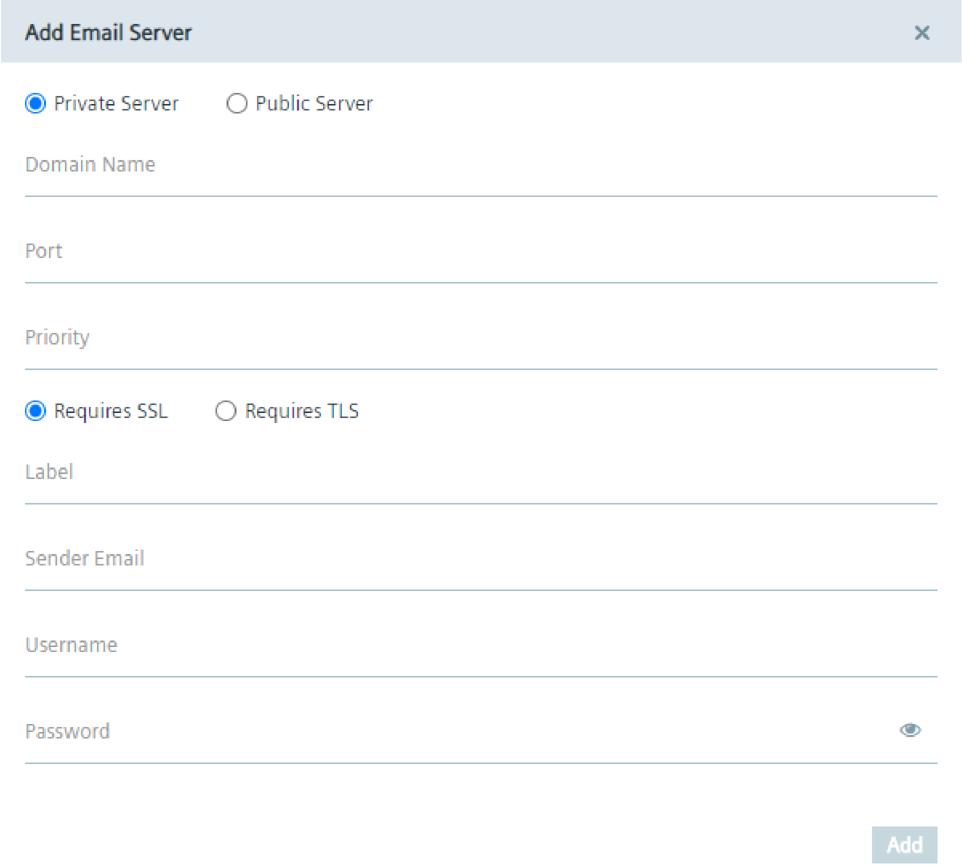
For relay servers, only 1 relay server is valid per IEM which you add when you set up the IEM. You find more information on the relay server in the "Adding a relay server" subsection in the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)" manual.

13.3.1 Adding an email server

Procedure

1. In the "Email Servers" screen, click "Add".

   The "Add Email Server" screen is displayed.

   Add Email Server

   ● Private Server ○ Public Server

   Domain Name

   Port

   Priority

   ● Requires SSL ○ Requires TLS

   Label

   Sender Email

   Username

   Password

   You have the possibility to add a private or a public email server.

2. To add a private email server, select the "Private Server" option. When you want to add a public server, select the "Public Server" option and select "Gmail" from the drop-down list below.

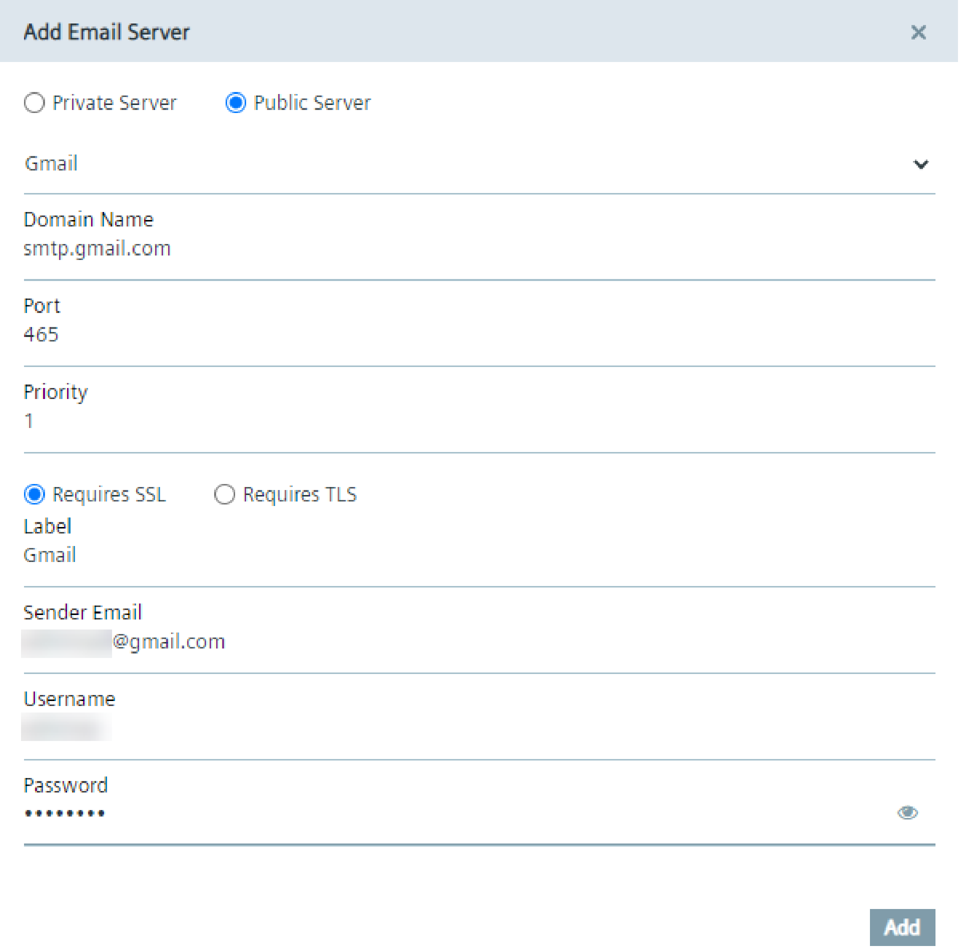
   Only "Gmail" email servers are available for public email servers.

3. In the "Domain Name" input field, enter the domain name of the email server.

4. If the email server requires SSL, enter the "465" port in the "Port" input field and select the "Requires SSL" option.
   If the email server requires TLS, enter the "587" port in the "Port" input field and select the "Requires TLS" option.

5. In the "Priority" input field, enter the priority for the email server. For the first added email server, enter "1".

   When you have added multiple email servers, the email server with the highest priority will be used as the default email server. For example, only when the email server with the priority 1 is offline and disconnected, the email server with priority 2 will be used.
6. In the "Label" input field, enter a name for the email server.
7. In the "Sender Email" input field, enter your email address on the email server.
8. In the "Username" input field, enter your username on the email server.
9. In the "Password" input field, enter the according password of the username.



Add Email Server ×

○ Private Server ● Public Server

Gmail

Domain Name
smtp.gmail.com

Port
465

Priority
1

● Requires SSL ○ Requires TLS

Label
Gmail

Sender Email
[redacted]@gmail.com

Username
[redacted]

Password
••••••••

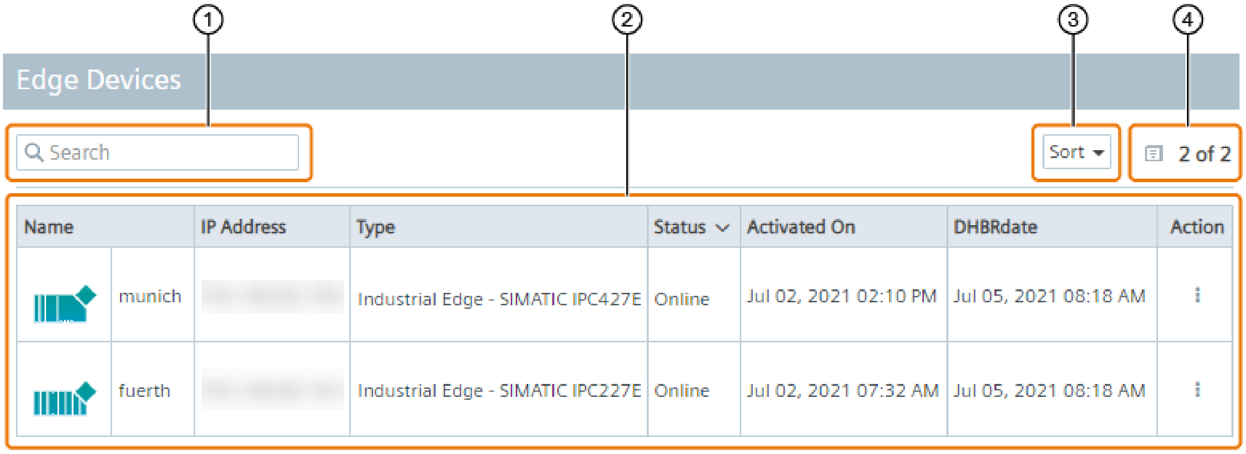
10. Click "Add".

    The email server will be added to the email server list.

13.4 Edge Devices

The "Edge Devices" screen lists all Edge Devices that are connected to the IEM and all Edge Devices that has been shared with you.

The following figure shows the layout of the Edge Devices list as an example:



Name		IP Address	Type	Status	Activated On	DHBRdate	Action
	munich	[redacted]	Industrial Edge - SIMATIC IPC427E	Online	Jul 02, 2021 02:10 PM	Jul 05, 2021 08:18 AM	⋮
	fuerth	[redacted]	Industrial Edge - SIMATIC IPC227E	Online	Jul 02, 2021 07:32 AM	Jul 05, 2021 08:18 AM	⋮

① Search

To search the list for a specific term, enter the term in this input field and press <Enter>.

② Edge Device list

The connected Edge Devices are listed including the most important information.

To display the statistics of an Edge Device, click the icon under "Action" and click "Statistics".

To open available log files of an Edge Device, click the icon under "Action" and click "Logs".

③ Sort

To sort list, activate an option from this drop-down list.

④ Number of Edge Devices

13.4.1 Downloading logs

To open available log files of an Edge Device, click the icon under "Action" and click "Logs".

The "Logs" screen of the Edge Device is displayed.

In the "Logs" screen, you check the following:

- Logs of the Edge Device
- Logs of Edge Apps that are installed on the Edge Device

The "Edge Device" tab lists all log files which are related to that specific Edge Device. The "Installed Applications" tab lists all log files which are related to Edge Apps that are installed on that Edge Device.

The date of a log file represents the date when the logs has been uploaded from the Edge Device to the IEM.

Note

Uploading logs

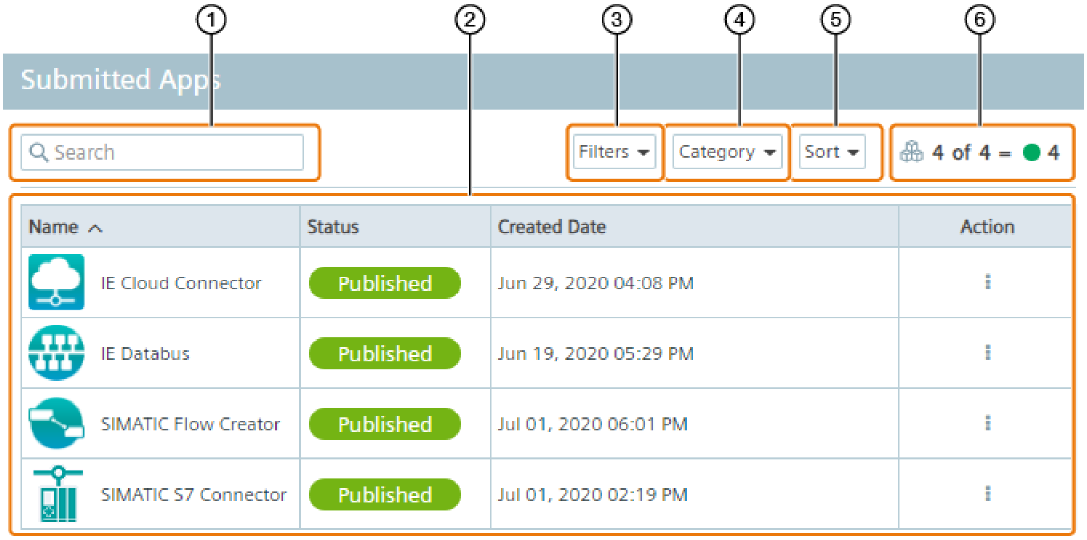
Logs are being uploaded from Edge Devices to the IEM every 24 hours by default. You change the time period in the "Settings > Configuration > Portal" menu in the Edge Device UI.

By clicking the ⤓ icon, the corresponding log file with the specific logs are downloaded to the standard download folder of your Internet browser.

13.5 Submitted Apps

The "Submitted Apps" screen lists all Edge Apps that have been published, unpublished or deleted from the IEM.

The following figure shows the layout of the list as an example:



Submitted Apps

Search | Filters | Category | Sort | 4 of 4 = ● 4

Name	Status	Created Date	Action
IE Cloud Connector	Published	Jun 29, 2020 04:08 PM	⋮
IE Databus	Published	Jun 19, 2020 05:29 PM	⋮
SIMATIC Flow Creator	Published	Jul 01, 2020 06:01 PM	⋮
SIMATIC S7 Connector	Published	Jul 01, 2020 02:19 PM	⋮

① Search

To search the list for a specific keyword, enter the keyword in this input field and press <Enter>.

② Edge App list

The Edge Apps are listed including the most important information.

To show all Edge Devices on which the app is installed, click the icon under "Action" and click "Edge Devices".

To unpublish an Edge App from the catalog in the Management UI, click the icon under "Action" and click "Unpublish". Confirm by clicking "Unpublish".

To delete an Edge App from the IEM, click the icon under "Action" and click "Delete". Confirm by clicking "Delete".

To republish an unpublished Edge App from the catalog or to publish a newer version of an Edge App to the catalog in the Management UI, click the icon under "Action" and click "Publish". Select the desired version and confirm by clicking "Publish".

③ Filter

To filter the list, activate one or more parameters in this drop-down list.

④ Category

Filter the list by 1 of the selected categories.

⑤ Sort

To sort the list, activate an option from this drop-down list.

⑥ Number of Edge Apps

Shows how many Apps are displayed on this page including their status.

13.5.1 Unpublishing apps

If you want to remove an app from the catalog in the Management UI, you can unpublish the app. In this case, the app is no longer available for installation. Only the admin can unpublish apps from the catalog.

Once the app is unpublished, the admin and user with the according permission can publish the app again to the catalog.

Requirement

The app has been imported to the catalog.

Procedure

1. Click the ⋮ icon under "Action" of the Edge App that you want to unpublish from the catalog.
2. Click "Unpublish".
3. To confirm the process, click again "Unpublish".

   The Edge App is being unpublished from the catalog.

13.5.2 Deleting apps

The admin and users with the "apps.delete" permission can delete submitted apps in the Admin UI from the IEM. Deleting an app removes all app versions and its data irrecoverable.

Procedure

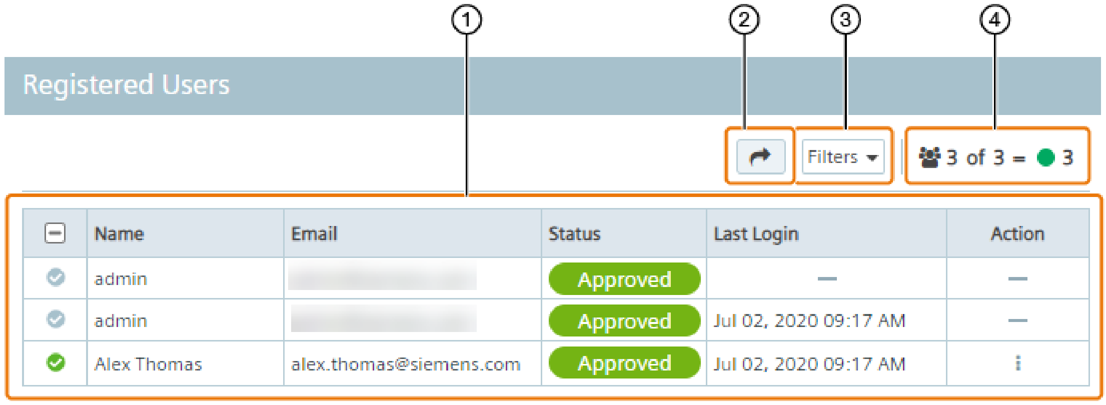
1. Click the ⋮ icon under "Action" of the app that you want to delete from the IEM.
2. Click "Delete".
3. To confirm the process, click again "Delete".

   The app is being deleted from the IEM. Once the app is deleted from the IEM, the app status switches from "Being Deleted" to "Deleted".

13.6 Registered Users

In the "Registered Users" screen you manage all registered users on the IEM and pending users who have signed up to the IEM.

The following figure shows the layout of the list as an example:



Registered Users

Filters ▾ | 3 of 3 = ● 3

□	Name	Email	Status	Last Login	Action
✓	admin	[redacted]	Approved	—	—
✓	admin	[redacted]	Approved	Jul 02, 2020 09:17 AM	—
✓	Alex Thomas	alex.thomas@siemens.com	Approved	Jul 02, 2020 09:17 AM	⋮

① User list

To select and deselect a user, click the check mark.

To select all users, activate the check box in the header of the table.

To approve the access to the IEM for a pending user, click the icon under "Action" and click "Approve". Confirm by clicking again "Approve".

To remove a registered user from the IEM, click the icon under "Action" and click "Suspend". Confirm by clicking again "Suspend".

To transfer the IEM access of a registered user to a new user, click the icon under "Action" and click "Transfer Ownership".

② Usage

This button is only visible, if 1 or more users are selected.

When you click this button, you get an overview of all Apps that have been submitted and all Edge Devices that have been added to the IEM by the user.

③ Filter

Filter users according to their status.

④ Number of users

Shows how many users are displayed on this page including their status.

13.6.1 Transfer IEM access

You have the possibility to transfer the IEM access of an existing registered user to a new user without performing the sign up process for the new user. When you transfer the IEM access to a new user, the previously registered user is deleted from the IEM. Deleting the admin by this operation and transferring your own access to a new user by yourself is not possible.

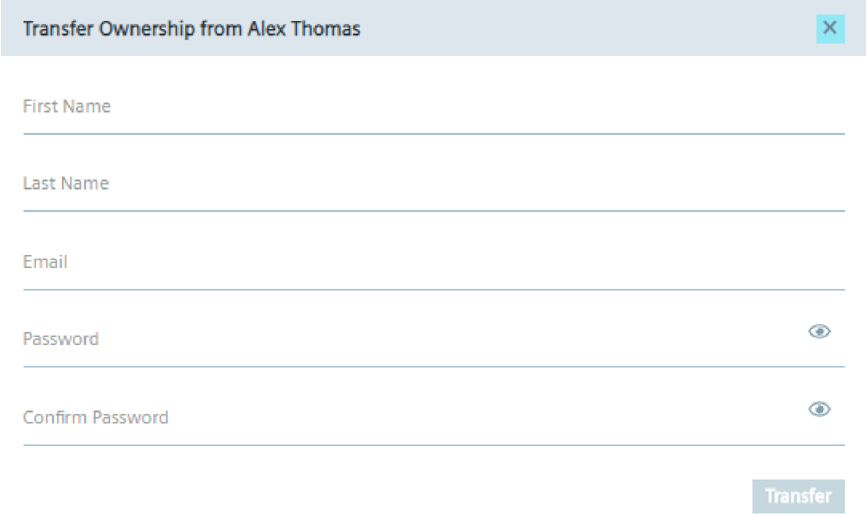
Requirement

- The email address of the new user must not already exist.
- Only the admin and users with the "users.delete" permission can perform this operation.

Procedure

1. Click the ⋮ icon under "Action" of the user whose IEM access you want to transfer to a new user.
2. Click "Transfer Ownership".

   The "Transfer Ownership" screen is displayed.

   Transfer Ownership from Alex Thomas

3. Complete the "Transfer Ownership" screen by entering the required information for the new user.

   The password must meet the following criteria:

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

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

   The previously registered user is replaced by the new user. The new user has now access to the IEM and the previously registered user is deleted from the IEM.

13.7 Manage Roles

The "Manage Roles" screen allows you to display and create roles. Roles include a set of permissions that you can assign to the role.

To give users specific permissions in the IEM, create roles inclusive the required permissions, assign the roles to existing admin groups in the the "My Admin Groups" screen and add users to the specific admin group. Also, depending on the role, some functionalities in the Admin UI are available or not.

By default, the following roles are available which cannot be deleted:

- Co-admin
- Update manager

13.7.1 Creating a role

Procedure

1. Click "Create Role".

   The "Create Role" screen is displayed.
2. In the "Name" input field, enter the name of the new role.
3. In the "Description" input field, enter a description for the role.
4. Select the permissions for the new role.
5. Click "Create".

   After you created the role, you can assign the new role to an admin group.

13.8 My Admin Groups

The "My Admin Groups" screen provides you the possibility to create admin groups and list all available admin groups. The list allows you to manage all admin groups.

To give an user admin roles, you create an admin group and add the user to the admin group. Members of an admin group receive permissions depending on the role that is assigned to the admin group. Depending on the admin role, functionalities of the Admin UI are available or not.

When you have created minimum 1 admin group, you can perform the following actions from the list by clicking the according icon:

- Edit: Delete the admin group or change the name and admin role assigned to the admin group
- Invite Members: Add members to the admin group
- Show Members: Show a list of all admin group members

13.8.1 Creating an admin group

Procedure

1. Click "Create".

   The "Create Admin Group" screen is displayed.
2. In the "Name" input field, enter the name of the admin group.
3. From the "Role" drop-down list, select an admin role.

   The permissions associated with the admin role are displayed. All members of this admin group have all permissions of the admin role.
4. Click "Create".

   The admin group is being created and added to the admin group list.

13.8.2 Inviting members to an admin group

Procedure

1. Click the + icon of the admin group you want to add members.

   The "Invite Members" screen is displayed.
2. In the "Email" input field, enter the email address of the user you want to add to the admin group.
3. If you want to add more users to the group, click the ⊞ icon.

   The previously entered user is listed in the "Member Email" table.

   Note

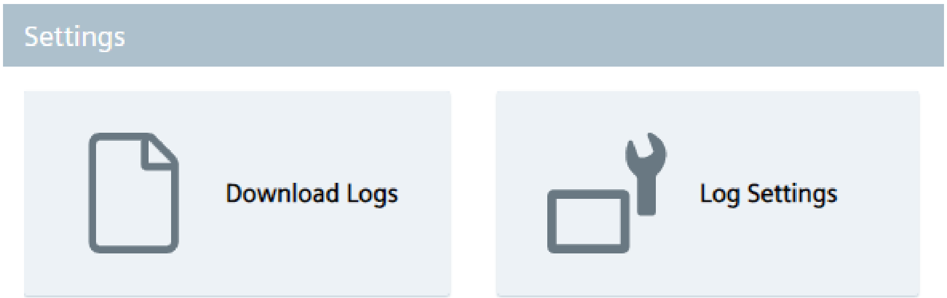
   Deleting users

   If you want to delete a user from the group, click the 🗑 icon for the required user.
4. In the "Email" input field, enter the email address of the next user you want to add to the group.
5. To add the listed users to the group, click "Invite".

   An invitation code is generated which you must send manually to the added users. The invited users enter the invitation code by clicking the icon to accept an invitation in the header of the Management UI.

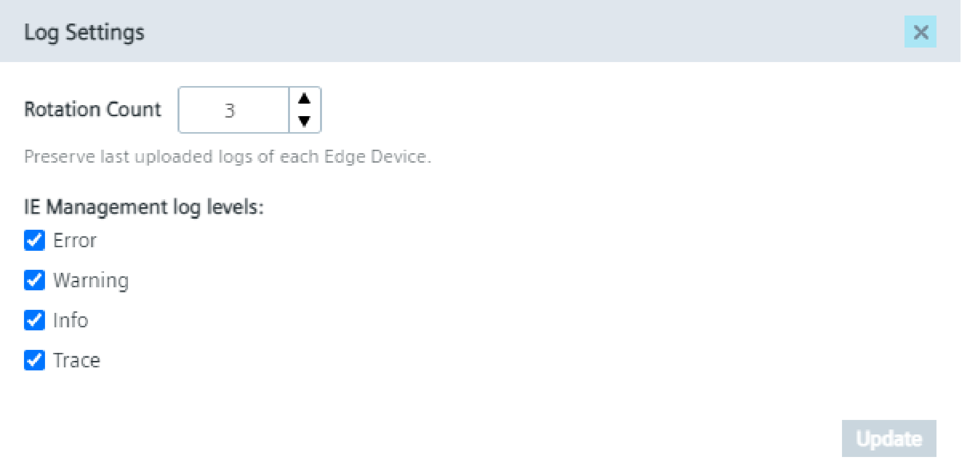
13.9 Settings

In the "Settings" screen you can download log files and decide which log types are written into the log files.



To download log files, click the "Download Logs" tile.

To decide which log types are written into the log files, click the "Log Settings" tile.



Log Settings

Rotation Count 3

Preserve last uploaded logs of each Edge Device.

IE Management log levels:

☑ Error

☑ Warning

☑ Info

☑ Trace

The "Rotation Count" setting manages the amount of log files of each Edge Device that are stored on the IEM. The IEM only stores the amount of the latest log files that you have set in this setting, by default 3 log files are getting stored. The rest will be removed automatically from the IEM.

You can decide which log types are written into the log files by selecting or deselecting the respective check box. To apply your changes, click "Update".

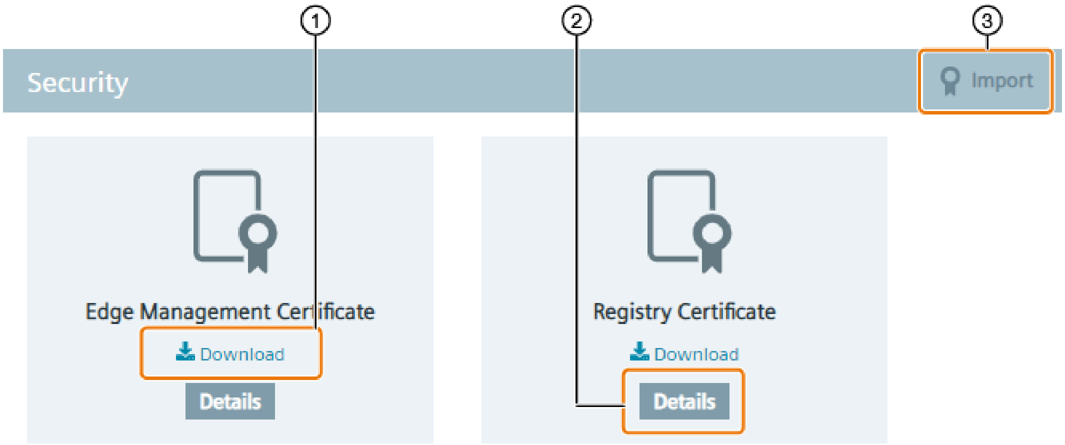
13.10 Security

IEM with own certificates

If you have set up the IEM with your own certificates, you have the possibility to perform the following actions for the "Edge Management Certificate" and the "Registry Certificate":

- Downloading certificates
- Displaying certificate details
- Importing certificates

The following figure shows the "Security" screen in that case:

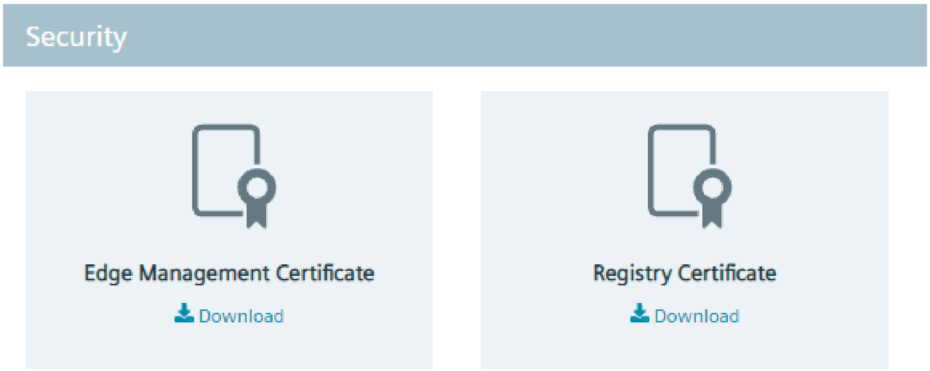


If the certificates are about to expire, you can import new certificates respectively replace existing certificates.

IEM with self-signed certificates by the IEM

If you have set up the IEM with self-signed certificates by the IEM itself, you can just download the "Edge Management Certificate" and the "Registry Certificate".

The following figure shows the "Security" screen in that case:



13.11 Device Catalog

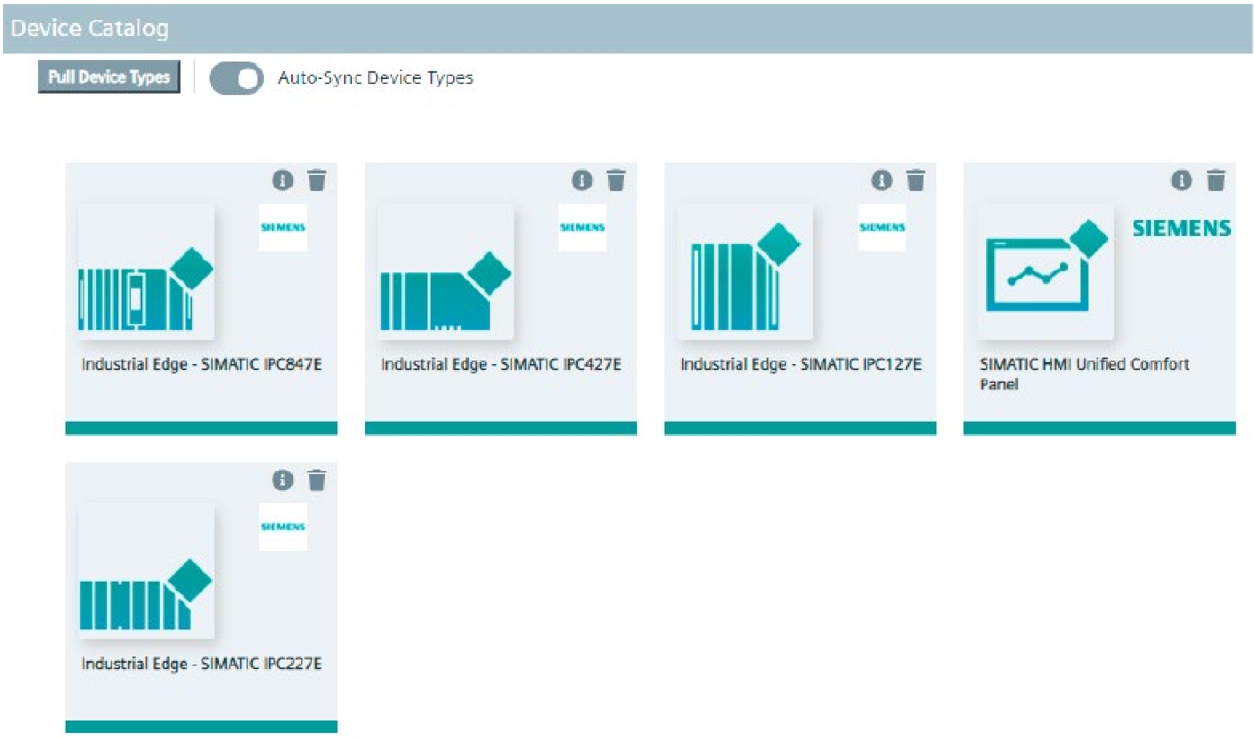
The "Device Catalog" menu item provides you the possibility to synchronize Edge Device Types and Edge Device OS versions with the IEM.

Requirement to work with the Device Catalog

To synchronize and update OS versions, the "IE Device Catalog" app must be installed in the IEM-OS. If you set up a new IEM, the "IE Device Catalog" app will be installed automatically. If you use an IEM V1.0 or V1.1 or you update your IEM from 1 of these versions to the newest version, you must manually install the "IE Device Catalog" app from the catalog in the Maintenance UI. To install the "IE Device Catalog" app, proceed in the same manner as described in the "Installing Configurators" subsection from the "Industrial Edge Management - Getting Started (https://support.industry.siemens.com/cs/us/en/view/109779989)" manual.

Edge Device Types

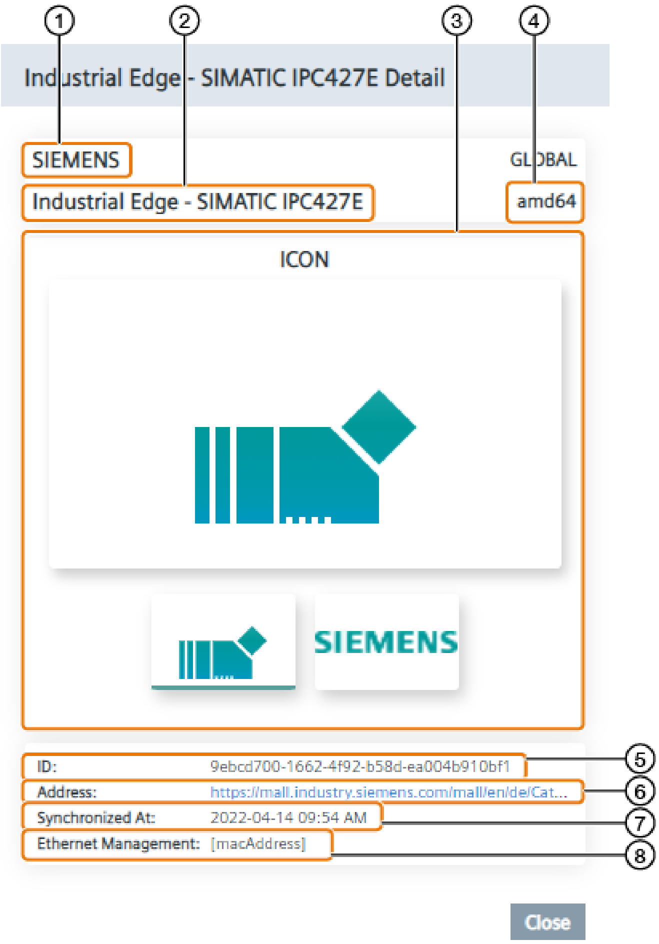
The "Device Catalog" screen displays all available Edge Device Types.


Device Catalog
Pull Device Types
Auto-Sync Device Types
SIEMENS
Industrial Edge - SIMATIC IPC847E
SIEMENS
Industrial Edge - SIMATIC IPC427E
SIEMENS
Industrial Edge - SIMATIC IPC127E
SIEMENS
SIMATIC HMI Unified Comfort Panel
SIEMENS
Industrial Edge - SIMATIC IPC227E

By clicking "Pull Device Types", you manually synchronize all published Edge Device Types from the IE Hub to the IEM. If you want to automatically synchronize the published Edge Device Types from the IE Hub to the IEM, enable the "Auto-Sync Device Types" toggle. If you do not want to automatically synchronize the published Edge Device Types from the IE Hub to the IEM, disable the toggle. In that case, you must manually synchronize the Edge Device Types to stay up to date.

Edge Device Type details

By clicking the ⓘ icon, the details of the respective Edge Device Type are displayed, as for example the SIMATIC IPC427E below:



Industrial Edge - SIMATIC IPC427E Detail

SIEMENS

GLOBAL

Industrial Edge - SIMATIC IPC427E

amd64

ICON

ID: 9ebcd700-1662-4f92-b58d-ea004b910bf1

Address: https://mall.industry.siemens.com/mall/en/de/Cat...

Synchronized At: 2022-04-14 09:54 AM

Ethernet Management: [macAddress]

① Vendor

② Name of the Edge Device Type

③ Icons

④ Architecture

⑤ ID

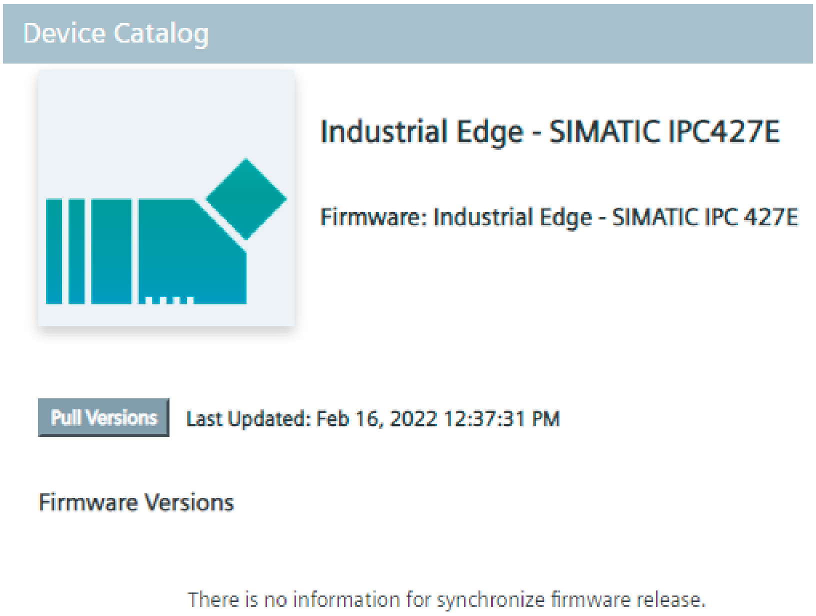
⑥ Order web address

⑦ Synchronization date and time

⑧ Ethernet management (type of network interface connection)

Synchronizing Edge Device OS versions

By clicking the tile of an Edge Device Type, firmware versions of the Edge Device Type and additional information are displayed. The following figure shows the details of the "Industrial Edge - SIMATIC IPC427E" Edge Device Type as an example:



Device Catalog

Industrial Edge - SIMATIC IPC427E

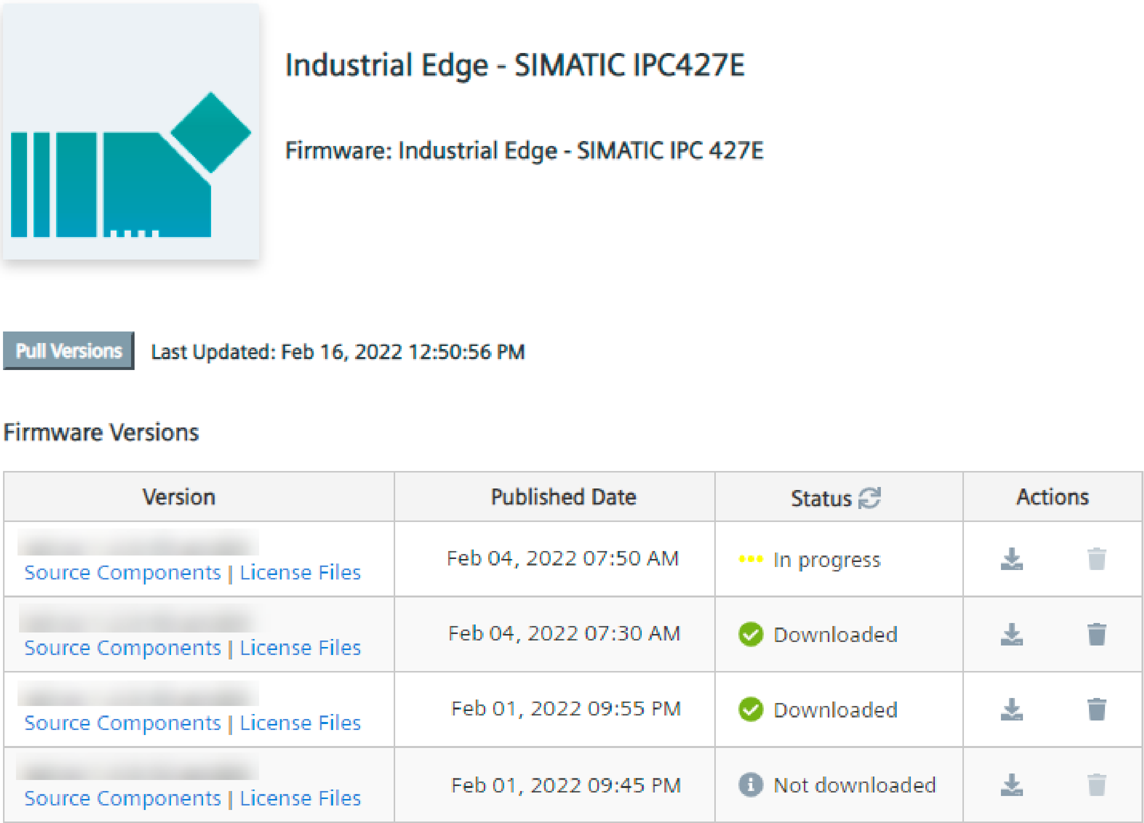
Firmware: Industrial Edge - SIMATIC IPC 427E

Last Updated: Feb 16, 2022 12:37:31 PM

Firmware Versions

There is no information for synchronize firmware release.

By clicking "Pull Versions", meta data of all Edge Device OS versions of this Edge Device Type, that have been released in the Industrial Edge Hub, are getting loaded and listed, as shown in the following figure for example.



Industrial Edge - SIMATIC IPC427E

Firmware: Industrial Edge - SIMATIC IPC 427E

Pull Versions Last Updated: Feb 16, 2022 12:50:56 PM

Firmware Versions

Version	Published Date	Status ⟳	Actions
[redacted] Source Components | License Files	Feb 04, 2022 07:50 AM	••• In progress	⤓ 🗑
[redacted] Source Components | License Files	Feb 04, 2022 07:30 AM	✓ Downloaded	⤓ 🗑
[redacted] Source Components | License Files	Feb 01, 2022 09:55 PM	✓ Downloaded	⤓ 🗑
[redacted] Source Components | License Files	Feb 01, 2022 09:45 PM	ⓘ Not downloaded	⤓ 🗑

The date next to the "Pull Versions" button displays the latest request of these meta data. This process requires an Internet connection. Once you have pulled released Edge Device OS versions, these versions will be displayed, even when you are not connected anymore afterwards to the Internet. The respective Edge Device OS versions also include its source components and license files. By clicking 1 of the links, the respective file is being downloaded. When a new Edge Device OS version is published and you click "Pull Versions", the new version is automatically listed. Following status are available for released Edge Device OS versions:

- Not downloaded: The OS version is not downloaded and not synchronized yet with the IEM.
- In progress: The OS version is being synchronized with the IEM.
- Downloaded: The OS version has been downloaded and synchronized with the IEM.

By clicking the ⟳ icon, you refresh the status of all firmware versions.

By clicking the ⤓ icon, the OS version will be downloaded and synchronized with the IEM. This download process requires an Internet connection and takes a while. When the synchronization was successful, the status switches to "Downloaded".

By clicking the 🗑 icon, you delete already downloaded and synchronized Edge Device OS versions from the IEM. The respective Edge Device OS versions are no longer available for firmware updates.

After the OS version is downloaded and synchronized with the IEM, you can update the OS of your Edge Devices to this version. You update the Edge Device OS in the Management UI in the "Edge Devices" screen by clicking the 🔧▾ icon and clicking "Firmware Update". You find information on how to update the Edge Device OS in the "Updating an Industrial Edge Device OS (Page 133)" subsection.

List of abbreviations/acronyms

14

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

Glossary

.app file

File extension for IE Edge Apps.

3rd Party Industrial Edge App

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

Admin UI

Included in the Industrial Edge Management App. UI enabled for admins and users with admin permissions to manage IED-OS versions and registered users for example.

Application Programming Interface (API)

In computing, an Application Programming Interface (API) is an interface that defines interactions between multiple software applications or mixed hardware-software intermediaries. It defines the kinds of calls or requests that can be made, how to make them, the data formats that should be used, the conventions to follow and so.

Centrally-managed Edge

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

Classless Inter-Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) is the successor to class-oriented domains for Internet routing and enables better allocations of Internet addresses. It combines a number of class C Internet Protocol (IP) addresses to reduce the burden on routing tables in the Internet.

Container

Containers are isolated environments on a shared operating system. Unlike VMs, containers do not bundle a full operating system, but only required libraries and settings for running the intended software. Containers are isolated on the kernel layer. This makes for efficient, lightweight, self-contained systems and guarantees that software will always run the same regardless of where it is deployed.

Data source

A data source is a physical element of a device, e.g. OPC-UA Server or S7, which collects data in the automation level.

Device-OS

Operating system used by Device Builders to integrate into the IED-OS.

Disaster Recovery (DR)

Disaster Recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant negative events. Having a disaster recovery strategy in place enables an organization to maintain or quickly resume mission-critical functions following a disruption.

Docker

Docker is a container platform that eases configuring, creating and sharing specific development environments and packaging software to be deployed everywhere. Docker provides a runtime and image format and a command line interface.

Industrial Edge

Industrial Edge represents an open, ready-to-use Edge computing platform consisting of Edge Devices, Edge Apps, Edge connectivity and an app and device management infrastructure. It enables collecting and analyzing data from industrial resources, enables a faster and more reliable rollout of apps on the shop floor, and provides central management for devices and apps with maximum scalability – with no need to intervene in the existing automation system (for example, to adapt controller software). Depending on your requirements, you can determine data that stays locally and data that can be used with a cloud solution on an optional basis.

Industrial Edge App Configuration Service (IEACS)

The Industrial Edge App Configuration Service enables to display templated app configuration files. App developers, that used templated app configurations in their applications, benefit from displayed forms in the Management UI and gain advantage of input validation, error messages and highly improved usability for the customer.

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 App Publisher CLI

Command Line Interface of the Industrial Edge App Publisher to use the IEAP in a build pipeline for example.

Industrial Edge Cloud Connector

App for data distribution to data services of cloud providers.

Industrial Edge Cloud Connector Configurator

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 Connectors

Connecting to external systems to exchange data (without preprocessing). The name is derived from the protocol that is being used to connect to the system, for example the SIMATIC S7 Connector is derived from SIMATIC S7 protocol.

Industrial Edge Control (IECTL)

The Industrial Edge Control (IECTL) is a Command Line Interface to interact with Industrial Edge and its components.

Industrial Edge Databus

System App for data distribution in Industrial Edge.

Industrial Edge Databus Configurator

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 Kit (IEDK)

Abstraction layer that separates hardware specifics from the operating system with the software functionality of the IERT.

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 a SIMATIC IPC Edge Device. The IED-OS enables SIMATIC IPCs to be managed as Edge Device.

Industrial Edge Ecosystem

The Industrial Edge Ecosystem builds on top of the IE Platform and serves for value creation by partners, such as App Providers, Device Builders, Solution Partners and others.

Industrial Edge Hub Access

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

Industrial Edge Management License

License (subscription) which customers need to buy in the Industry Mall or marketplace. The management license for IE Devices includes the annual fee to manage an Industrial Edge Device.

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)

The IEM-OS is the core orchestration engine of the Industrial Edge Management. Hosts IEM Services and provides service capabilities.

Industrial Edge Management Services

Applications that are provided with the IE Hub Access and that are free of charge. An IEM Service extends the IEM basic functionality. The IEM App, Device Catalog, IE State Service or the IE App Configuration Service belong to IEM Services.

Industrial Edge Marketplace

Marketplace beside the Industry Mall to purchase IE Apps.

Industrial Edge Platform

Consists of the Industrial Edge Hub, the Industrial Edge Management and Industrial Edge Devices.

Industrial Edge Runtime (IERT)

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

Industrial Edge Service Medium

Software artifact (*.iso) provided to flash onto USB flash drives. It is used to get log files of bricked Edge Devices and to reset Edge Devices.

Industrial Edge State Service (IESS)

The Industrial Edge State Service is an IEM service that provides the possibility to implement Disaster Recovery (DR) strategies based on your DR plan respectively requirements. With the IE State Service, you can store the IED state of an Edge Device on the IEM and restore a required stored IED state on the Edge Device in case of any occuring errors respectively failures in the Edge Device.

Industrial Edge System App

The IE Databus is considered as the only System App. The System App is an application that is provided free of charge with the IE Hub Access. It provides the data distribution in Industrial Edge. In comparison to Edge Apps, the System App is shipped with the IEM by default and is given special rights because it provides essential functionality for the IEM.

Industrial Edge App

Overall name for software applications which are distributed on the Industrial Edge Device. Apps always have a direct benefit for the user (backbone of value delivery) but are limited in their functionality. It can consist of one or more Docker containers. Siemens is not possible in the product name.

Industrial Edge Device (IED)

A hardware device which includes the Edge Device OS, provided by a Device Builder, with the purpose of providing Industrial Edge functionality. Industrial Edge Apps can be deployed on Edge Devices. Contains the Industrial Edge Runtime (IERT).

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.

Layer 2

The data link layer, or layer 2, is the second layer of the seven-layer OSI model of computer networking. This layer is the protocol layer that transfers data between nodes on a network segment across the physical layer.

Maintenance UI

UI to install and update IEM Services, configurators and the Industrial Edge Management App, as well as UI to configure IEM settings.

Management UI

Included in the Industrial Edge Management App and central user interface of Industrial Edge. The Management UI provides, amongst others, Edge App and Edge Device management.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

Organization

Organization is an instance of the Industrial Edge Hub in which you manage resources such as licenses, IEM instances, users and other entities such as Edge Device types and apps. You can own or be a member of more than one organization to distinguish between different user groups.

Secrets

Secrets are sensitive data that generally must be protected.

Shared Access Signature (SAS)

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources and how long the SAS is valid, among other parameters.

Side loading

Describes the process of bringing IE Apps into the IE Platform without need of the IE Hub. Side loaded apps can harm the system as Siemens has neither verified nor signed these applications. The operator owns the responsibility for any impact to the IE Platform due to side loaded apps.

Siemens Digital Exchange (DEX)

The Siemens Digital Exchange (DEX) is the (Industrial Edge) marketplace for purchasing digital products as well as services. This eCommerce marketplace seamlessly connects customers to catalogs of Siemens and third-party software products and services. The DEX is reachable under this link (Page).

SIMATIC S7 Connector

App that provides connectivity to the plant network.

SIMATIC S7 Connector Configurator

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.

Tags

Tags refer to elements (variables), which allow values to be obtained from data sources (OPC-UA or S7 etc.). They are combined into a relevant aspect. For example, "temperature" and "torque" are data points of the aspect "Energy_consumption". Tags are configured in SIMATIC S7 Connector Configurator.

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.

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is an international standard for a secure crypto processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.

Virtual Machine (VM)

A Virtual Machine (VM) imitates dedicated hardware and runs an operating system. Software running inside the VM and end users have the same experience as on a dedicated system. IaaS providers use a so called hypervisor which provides the VM with the configured hardware which is provided by the host. In the IaaS environment the type of hardware can be almost anything that is available in a data center.