SIEMENS

Insights Hub Private Cloud Developer Guide

Readme

Introduction 1

Development and Operation Process 2

Insights Hub Private Cloud Offerings 3

General Guidelines for Development and Operation 4

Security Obligations 5

Style Guide 6

04/2023
Version 2.0 (April 2023)

Table of contents

1 Introduction 3
1.1 Scope 3
1.2 References for related materials 3
2 Development and Operation Process 4
3 Insights Hub Private Cloud Offerings 6
3.1 Introduction 6
3.2 Use of Industrial IoT APIs 7
3.3 Application call paths and Insights Hub Gateway 7
4 General Guidelines for Development and Operation 9
5 Security Obligations 11
5.1 Introduction 11
5.2 Access Control 11
5.3 Security of the provided offering 11
5.4 Ensuring secure offering provision 12
5.5 Reporting violations 12
6 Style Guide 13

Introduction 1

1.1 Scope

This Insights Hub Private Cloud Developer Guide ("Developer Guide") is solely for use by Insights Hub Private Cloud subscribers.

It provides information for the development and testing of applications. You must meet or exceed all requirements specified in this Developer Guide for all applications.

The requirements and recommendations described in this Developer Guide provide only partial information and are only a supplement to the requirements described elsewhere in the Agreement. They shall not be understood as limiting, restricting or otherwise conflicting in any way with requirements set out elsewhere in the Agreement.

This Guide is provided "as-is" and will be updated from time to time. Information in this Guide, including URL and other website references, may change without notice. This Guide has been reviewed for consistency with the Offering described.

Siemens will make efforts to keep this document accurate and up to date, however due to the rapid evolution of Insights Hub, inconsistencies cannot be entirely excluded. The information in this Developer Guide is reviewed regularly and necessary corrections are included in subsequent editions.

1.2 References for related materials

You must review and consider the information set out in the following documents for the development of your application:

Developer Documentation (https://documentation.mindsphere.io/resources/private-cloud/dev-docs/en-US/index.html)

Industrial IoT API Reference (https://documentation.mindsphere.io/resources/private-cloud/dev-docs/en-US/apis/index.html)

User Documentation (https://documentation.mindsphere.io/resources/private-cloud/dev-docs/en-US/apps/index.html)

Your contractual agreements with Siemens.

Development and Operation Process 2

The end-to-end process that generally applies to developing your application, operations and providing it to others (within your Customer Instance) can be described as follows:

Developers' perspective

1. Configure your development environment.
   - Self-managed Environment

     Configure and use your development environment according to your needs and specifications (including technical requirements for mobile device operating systems), possibly provided by the vendor of the environment.
2. Develop your application.
   - According to your needs, create a local development environment by installing appropriate software tools.
   - Use the Developer Material to see how to create an application.
   - Use Industrial IoT API Reference and API Guide for information on how to make API calls.
   - Create your application in one of the supported languages.
3. Test and evaluate your application using the tenant on your development space.
   - Register your application as described in the Developer Material.
   - Test and evaluate your application as to its technology, functionality, performance, security and user interface with regard to expected content and behavior.
   - Use tools and processes to manage application testing.

Operators' perspective

1. Subscribe to Insights Hub Private Cloud
   - For self-hosted applications:

     Subscribing to Insights Hub Private Cloud you will be able to operate and provide your self-hosted application within your Customer Instance.
2. Prepare access to your application.

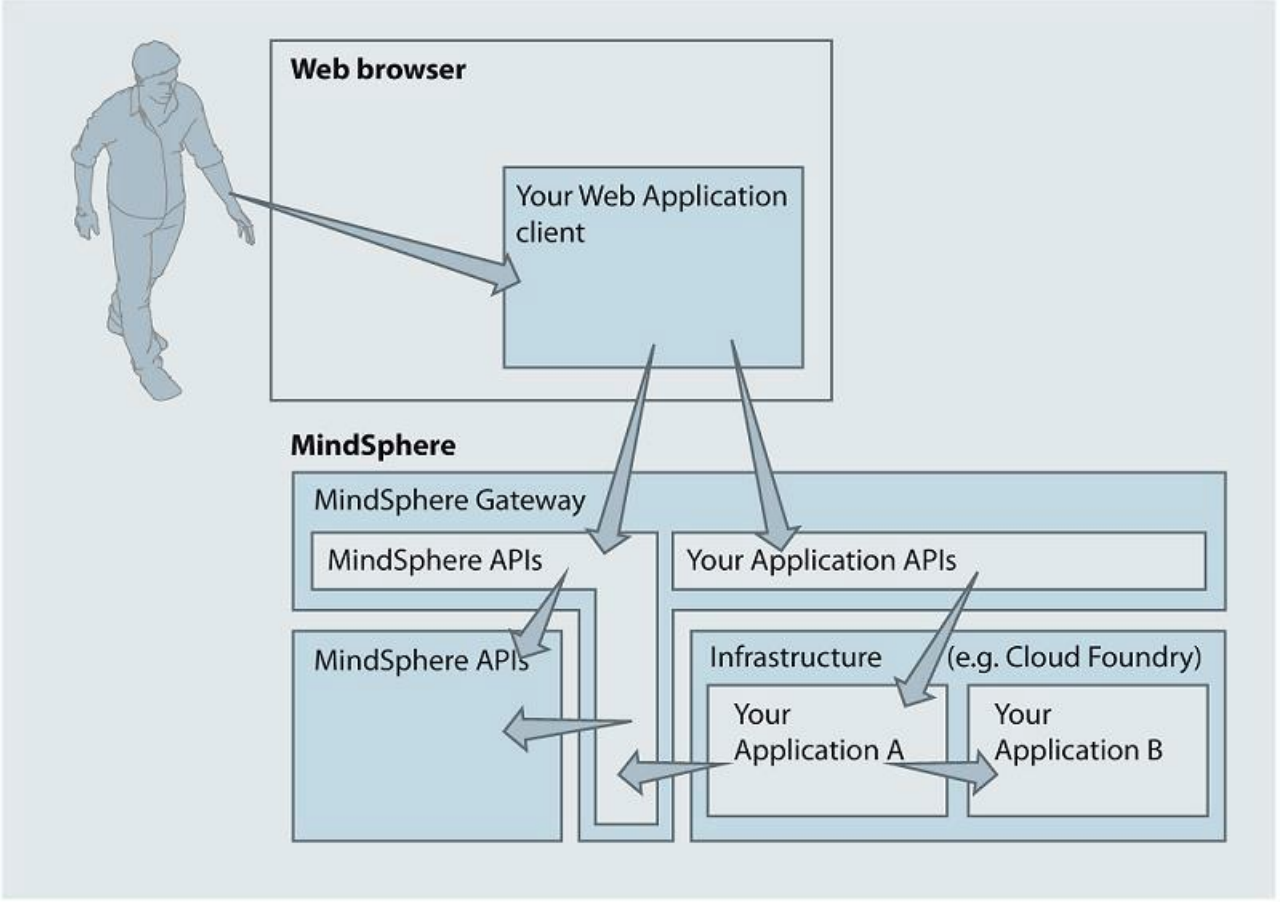
   For productive purposes you shall use the productive system in connection with your application. Therefore, you shall follow the respective process for self-hosted applications.
   - An operator can deploy and enable the application in the production environment using the Operator Cockpit and allow access to the application.
3. Operate and use your application
   - When the operated application is interactive, you may access this application on the Launchpad of your Account on the productive tenant (except for mobile native applications). Applications of the type plugin (or sometimes also referred to as extension) may be accessed within the application in which they are integrated.
   - Conduct continuous monitoring to maintain health of your application.
   - Keep your application up-to-date.

Insights Hub Private Cloud Offerings 3

3.1 Introduction

Insight Hub private provides a variety of supporting Offerings to speed application development. Services via Industrial IoT APIs are accessible via a gateway service called Insights Hub Gateway that manages the call paths and the availability of applications for customers. The graphic below illustrates exemplified call paths for a web application.

The following section describes the access to services that we expose via Industrial IoT APIs, the application registration, call paths and general guidelines for development.



3.2 Use of Industrial IoT APIs

Industrial IoT APIs expose RESTful services, e.g. Time Series or Asset Management. As a subscriber to our Offerings you are eligible to use the Industrial IoT APIs according to your subscription.

When using the Industrial IoT APIs, you must comply with the following requirements:

- The APIs provided by the Platform may only be used in the manner and for the purpose described by the API Reference.
- Only use API calls as described in the API Reference.
- Be advised that changes to the Industrial IoT APIs will occur due to future enhancements and the evolution of the Platform. We will use all reasonable efforts to avoid changes and to inform you in advance in case they are expected.

3.3 Application call paths and Insights Hub Gateway

Call paths for applications

Any access to the Industrial IoT APIs must utilize the Insights Hub Gateway. Depending on whether you are developing a web application with a browser client or a pure backend application, accessing APIs will be different and are documented in the Developer Material.

Your web application browser client can

- call Industrial IoT APIs. These calls must target URLs of the following schema:

  ```
  <web-app-host>/api/<api-name>[-<api-provider>]/v<major>/<endpoint>
  ```

- call your own application APIs. These calls have to target URLs of the following schema:

  ```
  https://<tenant>-<webapp>[-
  <provider>].<region>.mindsphere.io/[<path>]
  ```

Your mobile native application can

- call Industrial IoT APIs and your own application APIs with a service credentials access token obtained from an authorization server. These calls have to target URLs of the following schema:

  ```
  https://gateway.<region>.mindsphere.io/api/<api-name>[-<api-
  provider>]/v<major>/<endpoint>
  ```

Your Insights Hub backend application can

- call Industrial IoT APIs with a service credentials access token obtained from an authorization server. These calls have to target URLs of the following schema:

  ```
  https://gateway.<region>.mindsphere.io/api/<api-name>[-<api-
  provider>]/v<major>/<endpoint>
  ```

- call other backend applications of your own using an access token obtained from a browser client call.

Availability in Insights Hub Gateway

In order to make your applications available in Insights Hub Gateway, the following naming convention must be utilized.

Calls from a web application client following the schema:

`https://<tenant>-<webapp>[-<provider>].industrysoftware.automation.siemens.com.<path>]`

will be routed to an internal URL that looks as follows

`https://<application>-<tenant-id>.apps.industrysoftware.automation.siemens.com.<path>]`

General Guidelines for Development and Operation 4

Without prejudice to all other requirements, your application must at all times comply with the following:

- It is prohibited for your application to function as a distribution mechanism for software or include feature or functionalities that create or enable software stores, distribution channels or other mechanisms for software delivery within such applications. These restrictions do not include your web application which allows for the delivery of client code to browsers.
- It is prohibited for your application to utilize outdated software components and buildpacks, including, but not restricted to, open source software.
- You must ensure that your application utilizes up-to-date software components. As soon as updates are available, these updates must be applied. Usage of any software components with publicly known vulnerabilities is prohibited.
- You must ensure that any content, in particular the application is capable of automatic restart without manual operator intervention in the event of a non-availability of the Offering or a hardware or system failure occurring with the Offering. You must also build your application in a manner that it can restore its running state upon system restart.
- If any software vulnerability is found, we may, for the safety and security of other users, prevent access to your application.
- You are solely responsible for servicing your application.
- Your application must be deployed under a URL sub-domain that is assigned to your Account.

Data Handling

When handling data (including personal data) it is your responsibility to ensure that you comply with applicable laws and the terms of the Agreement as well as the expectations of your customers. Be transparent about what types of data are accessed and how they are processed and protected by your application; as well as make sure that your customers have given their consent to such access and processing.

Design considerations

The following recommendations should be considered in the development of your application.

12-Factor App

It is highly recommended to follow the 12-Factor methodology.

Failure, errors and exceptions

Always handle errors and exceptions. Make sure that your application exits gracefully in the event of exceptions and application errors. When errors and exceptions are logged, it is recommended to use the correlation id.

Fault tolerance

The service calls and resource access should take into account that the requested Offering may not be available at all times. Therefore, it is necessary that an appropriate retry mechanism is implemented.

Scalability

It is necessary that a horizontal scaling of your application and Offering is implemented by running multiple instances depending on the concurrency and load requirements. The cloud infrastructure services should be used for horizontal scaling.

Application health

Your application should implement some kind of "health" interface or mechanism for checking that the application is not only running but fully functional. Using the same conventions for all applications, a global health tracking and monitoring can be established.

Security Obligations 5

5.1 Introduction

Without prejudice to all other requirements, you are required to follow security best-practices and implement and maintain security mechanisms in order to achieve the intended security level of your application and support the integrity of the Platform and connected networks and equipment. This includes your obligation to comply with the security obligations set in this chapter.

5.2 Access Control

- You are provided with an access token for your applications to use services via Industrial IoT APIs. This access token may only be used for the intended purpose. All other uses are this access token are prohibited.
- Applications running on your Insights Hub instance are provided with JSON Web Tokens (abbreviated "JWT"). JWTs have to be validated according to rfc7519. All requests with invalid or missing JWTs must be rejected by you.
- You must take all necessary measures to protect access tokens against unauthorized third parties. If you become aware of a risk that an unauthorized party had access to such access tokens you must immediately send an e-mail to security@mindsphere.io.
- You are obliged to change your password on a regular basis.
- You are obliged to change passwords used by you to access our Offerings regularly over time. If not otherwise specified and permitted in writing, the interval between password changes shall not exceed the period of 12 months.

5.3 Security of the provided offering

Under no circumstances may you exploit the Offering in order to:

- gain unauthorized access to parts of the provided Offering that are restricted.
- intercept (passively or actively) a data flow of the provided Offering that is restricted.
- falsify or forge security mechanisms of the provided Offering. This includes forging protocol headers (e.g., IP, TCP or UDP) and the illegitimate use of the provided Offering to hide certain activities (e.g., using a proxy or providing a pseudonymous or anonymous network node through the provided Offering).

- usage of the provided Offering to publish, send or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations ("spam"), including commercial advertising and informational announcements.
- access or diminish resources (computational, storage or otherwise) of other users of the provided Offering.

5.4 Ensuring secure offering provision

Any violation of the requirements listed in this Developer Guide or misuse of the provided Offering may be investigated by us. Following measures may be applied:

- Removal, disablement of access to, or modification of any content or resource that violates this Developer Guide or any other agreement regarding the provided Offering.
- Reporting of any activity that is known or under suspicion of the violation of laws or regulations to appropriate authorities.
- Cooperation with law enforcement including reports of relevant security violations to law enforcement authorities.

5.5 Reporting violations

If you become aware of or experience any violation of this Developer Guide, you must immediately notify and provide assistance, as requested, to stop or remedy the violation. To report any violation of this Developer Guide, please contact us by e-mail at security@mindsphere.io.

Style Guide 6

To make a consistent appearance, your application must comply with the requirements stated in the Operator Cockpit. Further information and details of the style guide and specifications can be found in the Operator Cockpit documentation and in the Insights Hub Design System (available under https://design.mindsphere.io). The Operator Cockpit sets the specifications and requirements for the following areas:

Application user interface

When you integrate your application as a part of your Insights Hub Private Cloud, your application web frontend must provide the following elements:

- Insights Hub OS Bar must be integrated by code snipped into your application. Insights Hub OS Bar provides a User with essential core functions like Home-Button. For information how to integrate Insights Hub OS Bar please refer to Developer Material.
- a control with your company name, telephone number or e-mail address that describes how to receive service and support for your application. For your application, this control is not allowed to refer to Siemens.

Branding

- You must not use designations relating to Siemens, such as “Siemens”, “Si”, any similar reference to the designation “Siemens”, including but not limited to SIMATIC, SINUMERIK, SINALYTICS, and any abbreviations thereof, logos relating to Siemens or any word or logo confusingly similar thereto except as expressly provided for herein.
- You must not use the name of your solution or any of your trademarks or trade names in direct or indirect combination with or adjacent to any Siemens product or otherwise refer thereto except as expressly provided for herein.
- separate written consent, as provided below in this Developer Guide, or as otherwise provided upon your individual request. Trademarks and trade names of Siemens include without limitation Insights Hub, MindConnect, MindApps, MindAccess, MindServices and other designations beginning with “Mind”.