SIEMENS

MindSphere DevOps Guide

Readme

10/2021

Version 1.5 (Oct. 2021)

Table of contents

1 Introduction

1

1.1 Scope

This DevOps Guide is solely for use by subscribers of Operator and/or Developer Services (as included in a MindAccess Developer Plan and/or MindAccess Operator Plan or certain MindSphere Capability Packages) (incl. their Users).

It provides information for the development and testing of applications, as well as for deployment, productive operation and provisioning of applications via the respective Account and/or Environment. You must meet or exceed all requirements specified in this DevOps Guide for all applications.

The process for submitting an application to the Store in order to provide it to others, as well as the requirements for public listings on the Store and the selling of applications, are described in the Seller Guide available under (https://siemens.mindsphere.io/en/docs/guides). Please note that as of the date of release of this DevOps Guide the Seller Guide is solely applicable to subscribers (incl. their Users) of Operator and/or Developer Services as included in a MindAccess Developer Plan and/or MindAccess Operator Plan.

The requirements and recommendations described in this DevOps Guide provide only partial information and are only a supplement to the requirements described elsewhere in the agreement governing your subscription to the Developer and/or Operator Services. They shall not be understood as limiting, restricting or otherwise conflicting in any way with requirements set out elsewhere in such 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 Offerings (sometimes also referred to as 'Services') described.

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

No license to any software or Offering, know-how or other intellectually property right is granted, conveyed or implied, by this document and all rights are expressly reserved by Siemens. You may copy and use this document solely for your internal reference purposes.

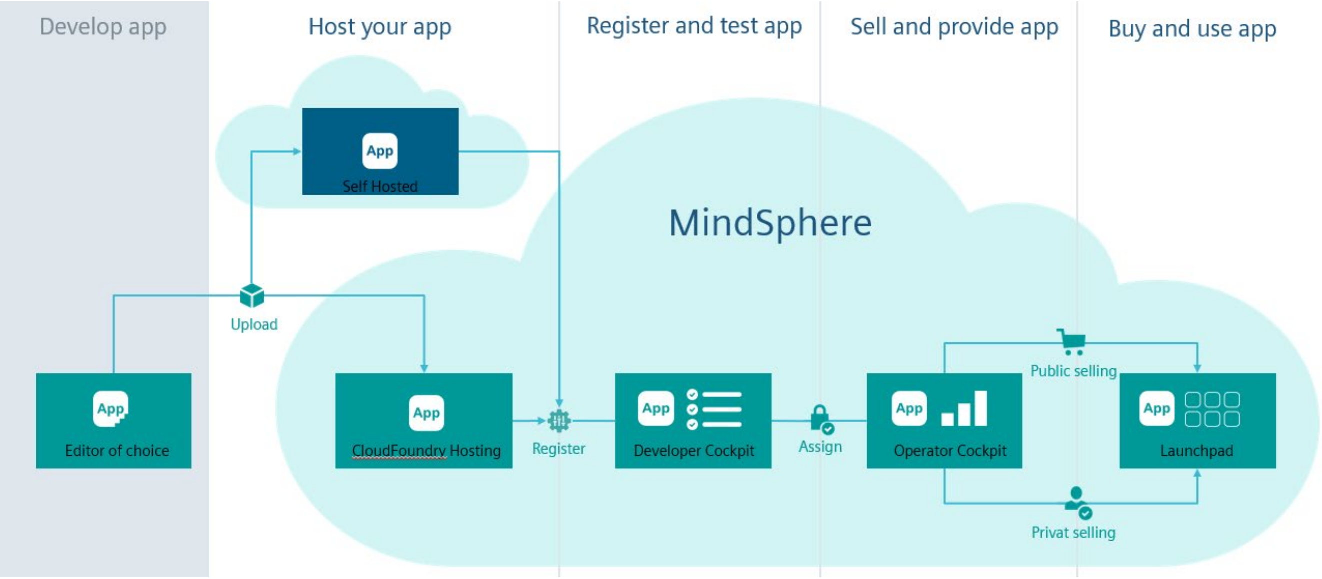
1.2 References for related materials

You must review and consider the information set out under

https://siemens.mindsphere.io/en/docs/guides and https://siemens.mindsphere.io/en/developer and your contractual agreements with Siemens.

Development, Operation and Sales Process 2

The end-to-end process that generally applies to developing your application, operations and providing it to others can be illustrated as follows:



In order to make your application commercially available, the following steps must generally be taken.

Developers' perspective

1. Subscribe to Developer Services (as included in a MindAccess Developer Plan or certain MindSphere Capability Packages)
   - For Cloud Foundry applications:

     Subscribe to the Cloud Foundry Hosting Add-on additionally to the Developer Services in order to be provided with an access to the Cloud Foundry.
   - For self-hosted applications:

     Subscribing to the Developer Services you will be able to develop and test your self-hosted applications.
2. Configure your hosting environment.
   - MindSphere-managed hosting

     Use Cloud Foundry Command Line Interface or a tool of your choice to prepare your hosting space.

     Configure Cloud Foundry as well as separately ordered or included Backing Services like additional data stores or message queues.
   - Self-managed hosting

     Configure and use your hosting environment according to your needs and specifications (including technical requirements for mobile device operating systems), possibly provided by the vendor of the environment.
3. Develop your application.
   - According to your needs, create a local development environment by installing appropriate software tools.
   - Use the Developer Documentation to see how to create an application.
   - Use MindSphere API Reference and API Guide for information on how to make API calls.
   - Create your application.
4. Test and evaluate your application using the Development Environment (or Developer Tenant) or Test Environments (only included in certain MindSphere Capability Packages).
   - Register your application as described in the Developer Documentation.

     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 Operator Services (as included in a MindAccess Operator Plan or certain MindSphere Capability Packages).

   - For Cloud Foundry applications:

     Subscribe to the Cloud Foundry Hosting Addon (only relevant for MindSphere Capability Packages) additionally to the Operator Services in order to be provided with an access to the Cloud Foundry.

   - For self-hosted applications:

     Subscribing to the Operator Services you will be able to operate and sell your self-hosted applications.

2. Prepare access to your application.

   For productive purposes you shall use the Productive Environment in connection with your application. Therefore, you shall follow the respective process for Cloud Foundry and self-hosted applications.

   - An operator is able to deploy the application in the production environment using the Operator Cockpit.
   - The Operator Cockpit provides mechanism to onboard the application into the Store. You can find comprehensive information about the selling of applications in the Seller Guide.
   - Finally, an operator can allow access to the application by using the Operator Cockpit.

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 Environment (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 (e.g. open source software, latest buildpacks for Java and Node.js in Cloud Foundry, updates on Backing Services).

Seller's perspective

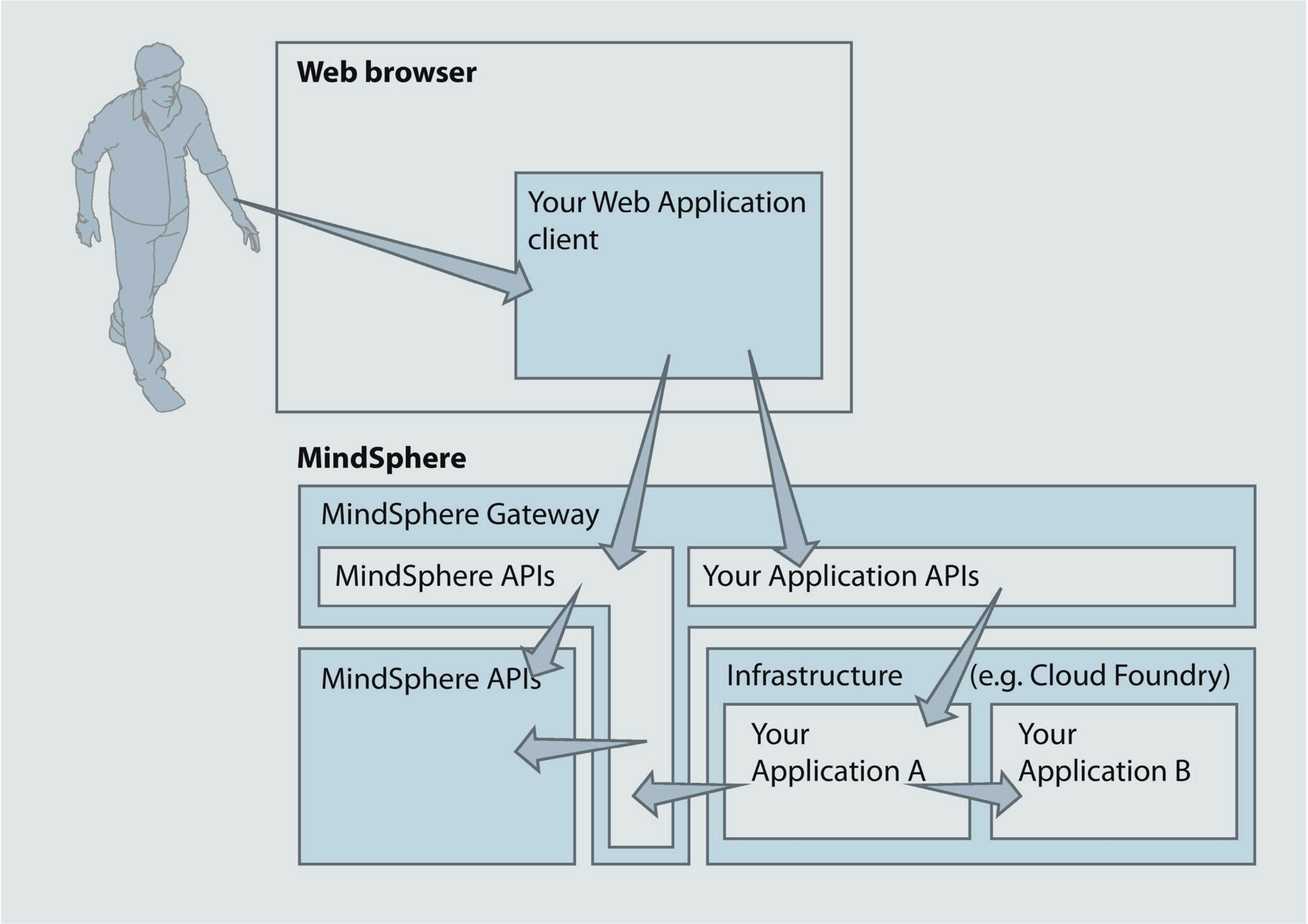
1. Subscribe to Operator and/or Developer Services (as included in a MindAccess Developer Plan and/or MindAccess Operator Plan or certain MindSphere Capability Packages): Deploy your application.
2. Register your application.
3. Enter the publishing data into the Operator Cockpit.
4. Submit content via Operator Cockpit to MindSphere Store.
5. Publish your application via the MindSphere Store.

MindSphere Platform Services 3

2.1 Introduction

MindSphere provides a variety of supporting Offerings to speed application development. Services via MindSphere APIs are accessible via a gateway service called MindSphere 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 MindSphere APIs, the application registration, call paths and general guidelines for development.



2.2 Use of MindSphere APIs

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

When using the MindSphere 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 MindSphere 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.

2.3 Application call paths and MindSphere Gateway

Call paths for applications

Any access to the MindSphere APIs must utilize the MindSphere 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 Documentation.

Your web application browser client can

- call MindSphere 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 MindSphere 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 MindSphere backend application can

- call MindSphere 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 MindSphere Gateway

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

Calls from a web application client following the schema:

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

will be routed to an internal URL that looks as follows

```
https://<application>-<tenant-id>.apps.eu1.mindsphere.io
```

Cloud Foundry

In order to make your application callable from a web application client, you need to create a Cloud Foundry based application with a name `<application>-<tenant-name>,` where `<tenant-name>` is your tenant name and `<application>` is the name to be used as path parameter in the web application client call.

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 (e.g. latest buildpacks for Java and Node.js in Cloud Foundry, updates on Backing Services). 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.
- When you deploy your Cloud Foundry application, you must create one space per application.

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 governing your subscription to the Developer and/or Operator Services 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

4.1 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.

4.2 Access control

- You are provided with an access token for your applications to use services via MindSphere APIs. This access token may only be used for the intended purpose. All other uses are this access token are prohibited.
- Applications running on the MindSphere Platform 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 services via MindSphere APIs regularly over time. If not otherwise specified and permitted in writing, the interval between password changes shall not exceed the period of 12 months.

4.3 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 Service/ Offering that is restricted.
- falsify or forge security mechanisms of the provided Service/ Offering. This includes forging protocol headers (e.g., IP, TCP or UDP) and the illegitimate use of the provided Service/ Offering to hide certain activities (e.g., using a proxy or providing a pseudonymous or anonymous network node through the provided Service/ Offering).

- usage of the provided Service/ 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 Service/ Offering.

4.4 Ensuring secure Offering provision

Any violation of the requirements listed in this DevOps 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 DevOps 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.

4.5 Reporting violations

If you become aware of or experience any violation of this DevOps Guide, you must immediately notify and provide assistance, as requested, to stop or remedy the violation.

To report any violation of this DevOps 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 MindSphere Design System (available under https://design.mindsphere.io).

The Operator Cockpit sets the specifications and requirements for the following areas:

Application Icon and display name

Application Icon

Your application icon is the first way to communicate the benefits of your application. Within MindSphere your application requires input from you in order to create a unique icon for your application. Your registered company name must be attached to the application icon to clearly indicate that you are the provider of the application. The design of your application icon must be distinctively different from the design of icons used by Siemens as part of the services (e.g. Asset Manager, Fleet Manager).

Display name

Every application must have a unique display name. The name of the application is important so that potential customers have a clear understanding of what your application offers.

Application user interface

When you make your application available via a MindSphere URL to subscribers of the MindAccess IoT Value Plan or MindSphere Capability Packages, your application web frontend must provide the following elements:

- MindSphere OS Bar must be integrated by code snipped into your application. MindSphere OS Bar provides a User with essential core functions like Home-Button. For information how to integrate MindSphere OS Bar please refer to Developer Documentation.
- 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.

When you make available your self-hosted application via a non-MindSphere URL to 3rd parties, your application web frontend must not

- integrate the MindSphere OS Bar or any part of it.
- refer to Siemens by any means. This comprises but is not limited to design and content but excludes references to MindSphere which are necessary to illustrate login (or other technical) requirements.

Branding

Details regarding branding you must comply with when marketing your solution can be found in the Marketing Guide (available under https://siemens.mindsphere.io/en/docs/guides).