



MindSphere DevOps Guide


Readme


| | |
|---|----------|
| <u>Introduction</u> | 1 |
| <u>General Guidelines for Development and Operation</u> | 2 |
| <u>Security Obligations</u> | 3 |
| <u>Style Guide</u> | 4 |


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.

Table of contents

- 1 Introduction 5**
 - 1.1 Scope 5
 - 1.2 References for related materials 5
- 2 General Guidelines for Development and Operation 7**
- 3 Security Obligations 9**
 - 3.1 Introduction..... 9
 - 3.2 Access control..... 9
 - 3.3 Security of the provided Service 9
 - 3.4 Ensuring secure Service provision..... 10
 - 3.5 Reporting violations..... 10
- 4 Style Guide..... 11**

Introduction

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.

Please note that as of the date of release of this DevOps 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 Service, 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 in the following documents for the development of your application:

Guides and

Developer (<https://developer.mindsphere.io>) and your contractual agreements with Siemens.

General Guidelines for Development and Operation

2

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 Services 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 Services 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

3.1 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.

3.2 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 of 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.

3.3 Security of the provided Service

Under no circumstances may you exploit the Service 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).

3.5 Reporting violations

- 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.

3.4 Ensuring secure Service 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.

3.5 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

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> (<https://design.mindsphere.io>)).

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>).

