Technical Documentation | PUBLIC

Document Version: 2.73.0 – 2020-11-18

Security

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Security. 3

2 Technical System Landscape. 4

3 Security Recommendations. 6

4 Roles and Authorizations. 7

5 Data Protection and Privacy. 8

5.1 Which Personal Data is Collected?. 8

5.2 View Personal Data. 8

5.3 Deletion of Personal Data. 9

5.4 Deletion of Service Data. 9

5.5 Export of Service Data. 9

6 Security Measures. 10

7 Network and Communication Security. 11

8 Security-Relevant Logging and Tracing. 12

1 Security

The Security section of this documentation provides an overview of the security-relevant information that applies to the Internet of Things service.

The Internet of Things service is a service on the SAP BTP. Therefore, we highly recommend that you read the SAP BTP Security section for your corresponding software version. You should also refer, as needed, to Security Guides and other relevant documents such as Development Guides and Installation Guides for the respective software systems.

Additional Information

For more information about specific topics, consult the following resources.

Content	Link
SAP Security, Data Protection, and Privacy	https://www.sap.com/corporate/en/company/security.html
SAP BTP Security	Security
SAP BTP Log Viewers	Log Viewers

2 Technical System Landscape

The following simplified diagram of the solution components and their communication channels is used below to provide security-relevant information.

Customer Zone

This zone comprises the software running on the device, which has direct access to the device data and controls operations including communication on the device. This zone also includes the OAuth token for the specific device, which should be stored securely on the device. Since bidirectional communication between the cloud and the device may take place, this zone also includes the secure processing of messages received from the cloud on the device.

Cloud Zone

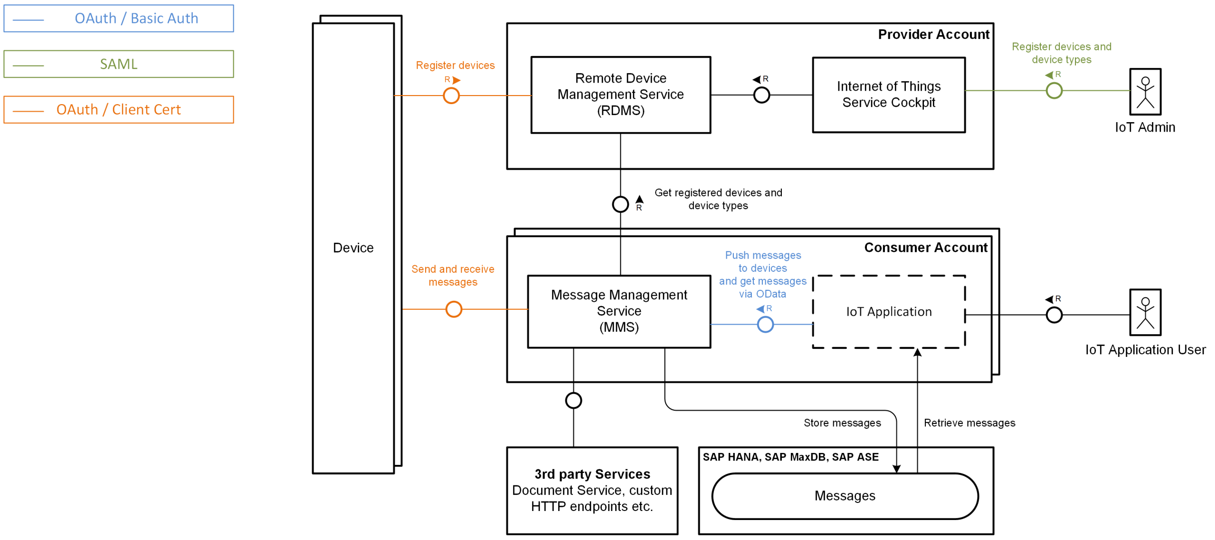
The core functions provided by the Internet of Things service are offered by the components hosted in an SAP-controlled cloud environment, the SAP BTP. These components and their security-relevant information flows are shown in the figure below. The SAP-controlled provider account hosts the Remote Device Management Service (RDMS) which is used for device management, and the Internet of Things service cockpit which acts as a user interface to the RDMS. These two components are provided in the consumer account by means of subscription. Users can access the Internet of Things service cockpit by using single sign-on with their SAP BTP account and having the appropriate role.

> i Note
>
> You must have a specific role to access the Internet of Things service cockpit. For more information, please refer to section .

The user-controlled consumer account hosts the Message Management Service (MMS) which handles the messages received by the device. Devices need to obtain an OAuth token to send or receive messages through the external APIs. External APIs include all paths that conform to the following schema: https://<host>/com.sap.iotservices.mms/v1/api/* The token needs to be added as a request header to all requests. The header has the following schema:

```
Authorization: Bearer <oauth token>
```

The dashed box represents functions a user might build to make use of the device data collected. For such a new business application, additional roles must be defined.


OAuth / Basic Auth
SAML
OAuth / Client Cert
Device
Register devices
R
Send and receive messages
Provider Account
Remote Device Management Service (RDMS)
R
Internet of Things Service Cockpit
Register devices and device types
R
IoT Admin
Get registered devices and device types
R
Consumer Account
Message Management Service (MMS)
Push messages to devices and get messages via OData
R
IoT Application
R
IoT Application User
Store messages
Retrieve messages
3rd party Services
Document Service, custom HTTP endpoints etc.
SAP HANA, SAP MaxDB, SAP ASE
Messages

3 Security Recommendations

The Internet of Things service currently comes with an initial set of security features. Also consider the following points:

Recommendation

- Do not delete or change applications, destinations, OAuth clients, and other security settings that are installed by the Internet of Things service.
- Protect the device and its stored OAuth token against unauthorized access at all times. If possible, use an encryption method to store the OAuth token on the device. Remove the old OAuth token when installing a new OAuth token on the device.
- If the device receives messages from the cloud, allow for secure processing of these messages to avoid unintended actions being triggered on the device.
- The current version logging capabilities are limited. Nevertheless, monitor the system and regularly check for any exceptional behavior.
- Consult a security expert or carefully read the information provided below to be aware of your current protection level.

Related Information

Roles and Authorizations [page 7]

4 Roles and Authorizations

Currently, the Internet of Things service uses two roles to restrict service access to authorized users only. The *IoT-User* role is automatically assigned to the SAP ID User of the consumer account during subscription. The other role, *IoT-MMS-User*, must be assigned manually to users after the Message Management Service (MMS) has been installed successfully on the consumer account. For more information, please refer to section .

Roles

Role Name	Intended Use
IoT-User	Assign this role to users representing a person. This role allows users to create, view, modify, and delete devices, device types, message types, and so on, using the Internet of Things service cockpit.
IoT-MMS-User	Assign this role to users representing a person. This role grants access to the Message Management Service (MMS) start page and allows users to use the sample clients available for the Data Services and the Push Service.
IoT-MMS-DevOps	Assign this role to users representing a person. This role allows users only to update or deploy the Message Management Service (MMS).

5 Data Protection and Privacy

This Data Protection and Privacy Statement applies to the SAP IoT services for SAP BTP for the Neo environment.

We have created this Privacy Statement to demonstrate our firm commitment to the individual's right to privacy. This Privacy Statement outlines our handling practices regarding such information that can be used to directly or indirectly identify an individual ("personal data").

Some SAP group entities, offerings, programs, or websites may have their own, possibly different privacy statements. We therefore encourage you to read the privacy statements of each of the SAP websites, offerings, or programs you visit or review.

> i Note
>
> SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and data protection-relevant functions, such as blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws is not covered by a product feature. Furthermore, this information should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, considering the given system landscape, and the applicable legal requirements. Definitions and other terms used in this documentation are not taken from a specific legal source.

Except for the data described below, the Internet of Things service does not collect any personal data by itself. If you use our service to process or store other personal data, you are responsible for all legal and data privacy regulations.

5.1 Which Personal Data is Collected?

The following personal data will be collected:

- User ID
- IP address
- Activity on the Internet of Things service tied to your IP address

5.2 View Personal Data

If you want to see your personal data associated with the SAP Cloud Identity Authentication service that is stored by SAP, please contact us. For more information, please refer to section .

5.3 Deletion of Personal Data

SAP will not retain your personal data longer than is necessary to fulfill the purposes for which it was collected or than is required by applicable laws or regulations. In particular, and if no such contradicting statutory obligation exists, SAP will delete your personal data once you inform SAP that you do not want SAP to further process your personal data. Please contact us as described in the section .

Please note that in this case the use of certain services or offerings may either be limited or not possible any longer. In case there is a contradicting statutory obligation for SAP to retain your personal data, SAP will block it against further processing, and then delete the relevant personal data as soon as the requirement to retain it ends.

5.4 Deletion of Service Data

In addition to personal data, SAP will also delete data specific to the Internet of Things service. This includes application and account settings as well as device meta data such as:

- Devices
- Device types
- Message fields
- Message types
- Hierarchies

Please note that the Internet of Things service ingests messages into user-controlled systems. Thus, SAP may not have access to these systems and therefore be unable to delete messages sent by devices.

5.5 Export of Service Data

During your term of subscription, you may export your data. To retrieve metadata, you may use the Remote Device Management Service (RDMS) API. For more information, please refer to section API v2 Introduction. This API offers a complete collection of your device metadata in JSON format. Note that messages sent by the device cannot be obtained using the RDMS API. The data export process for device messages depends on the respective processing service. For instance, if the SQL processing service is configured, data can be obtained and exported by connecting to the database. To learn how to access your database remotely, please refer to section Accessing Databases Remotely in the SAP BTP, SAP HANA Service documentation.

6 Security Measures

The Remote Device Management Service (RDMS), the Message Management Service (MMS), and the Internet of Things service cockpit are based on the SAP BTP. Therefore, they come with the security measures provided by this platform.

The Internet of Things service cockpit additionally uses SAP UI5 libraries. Besides the security mechanisms adopted from these underlying SAP technologies, the following security features are in place:

- Clickjacking: The Internet of Things service cockpit is built on SAP UI5 and inherits the protection mechanisms from this platform.
- Cross-Site Scripting: Data displayed to the user within the Internet of Things service cockpit is normally processed and rendered by SAP UI5 controls, whereas input validation and output encoding are performed by the renderer.
- Path Traversal: In the Internet of Things service cockpit, no URL is directly based on user input. File access functions in the Internet of Things service cockpit are not based directly on user input.
- Data Validation: The Remote Device Management Service (RDMS) comes with a special built-in validation framework. Database input is checked for syntactical correctness, including non-emptiness, allowed characters, allowed ranges, and allowed lengths. The Internet of Things service cockpit also includes validation checks during user input.

7 Network and Communication Security

Communication for all channels is encrypted and based on TLS only.

8 Security-Relevant Logging and Tracing

The standard logging features of the SAP BTP are available for the Message Management Service (MMS) component. Therefore, you can view the log files in the SAP BTP cockpit.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
    - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
    - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP