PUBLIC
SAP Warehouse Operator
Document Version: 2.1 – 2023-08-09

SAP Warehouse Operator – Administration Guide

THE BEST RUN SAP

Content

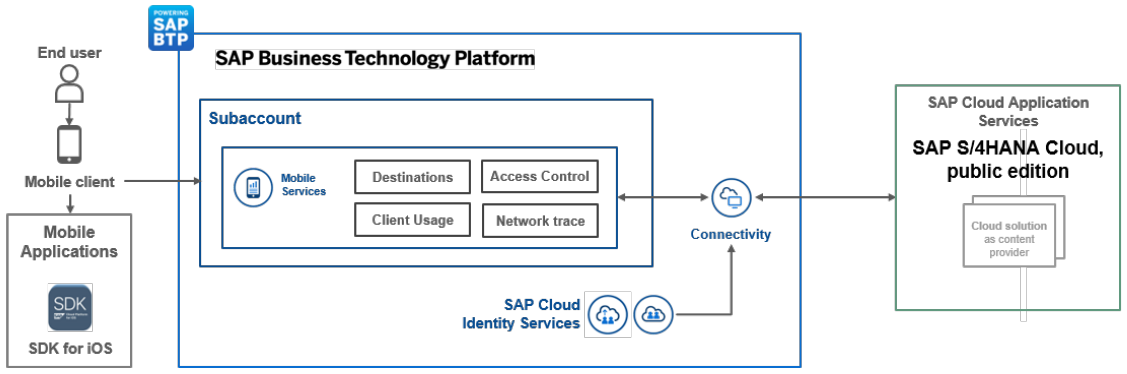
1 Overview

SAP Warehouse Operator is a native mobile app for iPhone and is integrated with Warehouse Management in SAP S/4HANA Cloud, public edition. SAP Warehouse Operator supports warehouse operators with traditional business processes such as picking and putaway tasks.

This guide is aimed at system administrators. You can find end user information about how to use SAP Warehouse Operator here: SAP Warehouse Operator – User Guide.

See an overview of the system landscape:

Building Blocks
High-level architecture for SAP Warehouse Operator



> **Note**
>
> For more information, see Important Disclaimers and Legal Information.

2 System Prerequisites

To configure the infrastructure for the SAP Warehouse Operator mobile app, you need the following system prerequisites:

General

- SAP Business Technology Platform tenant.
  See: SAP Business Technology Platform
- SAP Mobile Services
  See: SAP Mobile Services
- SAP Cloud Identity Services
  See: SAP Cloud Identity Services – Identity Authentication
- In case you configure your own IdP, it needs to be compliant with SAML 2.0 or OIDP.
  See: Configure SAML 2.0 Service Provider

SAP S/4HANA Cloud, public edition

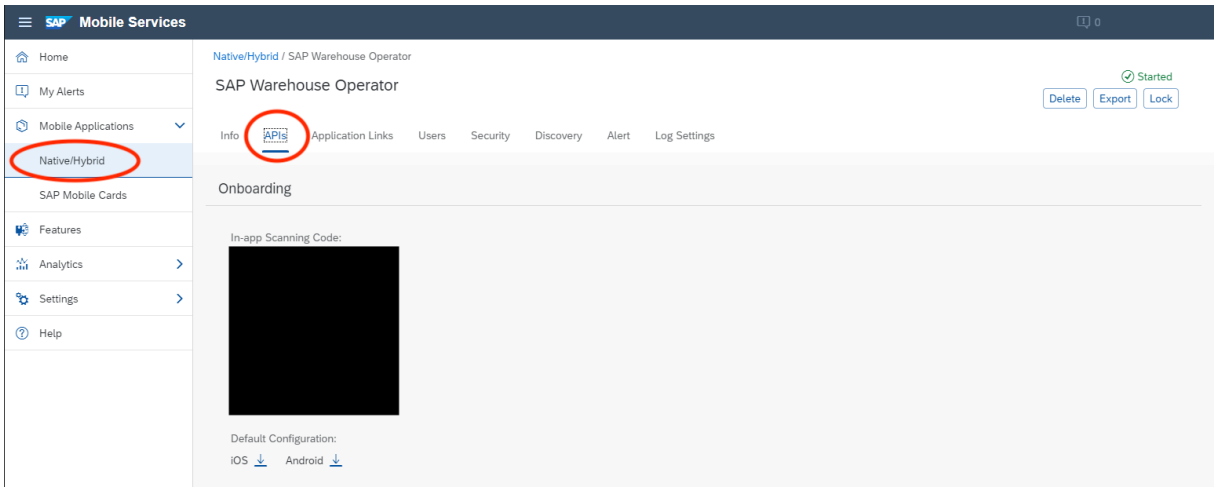
- Application content for S/4HANA Cloud, public edition
  See: SAP S/4HANA Cloud, public edition

3 Onboarding

A detailed onboarding guide for users of SAP Warehouse Operator can be found here: .

To enable users to onboard the SAP Warehouse Operator mobile app, the administrator needs to provide an onboarding QR code, which can be found in your SAP Mobile Services account:

1. Open the SAP Mobile Services cockpit and click on *Mobile Applications* > *Native/Hybrid*.
2. Select *SAP Warehouse Operator* from the list.
   The QR code can be found on the *APIs* tab.



4 Configure Mobile Services

Prerequisites

- You **subscribed to** SAP Mobile Services.
  For more information, see Mobile Services – Getting Started.
- You **configured** SAP Mobile Services.
  For more information about all of the configuration steps and options, see Set Up Customer Accounts.
- You configured SAP Identity Authentication Service.
  For more information, see SAP Cloud Identity Services – Identity Authentication – Create a New User.
- Optional: You configured Single Sign-On (SSO) using principal propagation.
  For more information, see SAP Build Work Zone, standard edition – Configure SSO.

Overview

In the SAP Mobile Services cockpit, you need to perform the following steps:

1. Create a Mobile Application [page 6].
2. Set up and configure Passcode Policy and Security [page 7].
3. Create Destinations [page 7].
4. Configure Mobile Client Log Upload [page 10].

4.1 Create a Mobile Application

Prerequisites

- You subscribed to SAP Mobile Services.
- You created a service instance.

Procedure

1. Log on to the SAP Business Technology Platform Mobile Service cockpit.
2. On the left side panel, click *Mobile Applications* > *Native/Hybrid*.
3. Click *New*.
4. In the dialog box that opens, put the following values into the two mandatory fields (marked with *):

- ID: `com.sap.mobile.apps.warehouseoperator`
- Name: `SAP Warehouse Operator`

5. Click *Next*.
6. In the next dialog box, activate the following features for Native Applications:
   - Mobile Client Log Upload
   - Mobile Client Resources
   - Mobile Client Usage and User Feedback
   - Mobile Connectivity
   - Mobile Network Trace
   - Mobile Offline Access
   - Mobile Settings Exchange
7. Click *Finish*.

4.2 Passcode Policy and Security

Passcode Policy

To set up and configure authentication for SAP Warehouse Operator, follow the steps described here: Mobile Services – Defining Client Password Policy.

Security

We recommend that you enable CSRF protection in Mobile Services:

1. In Mobile Services, navigate to the SAP Warehouse Operator mobile app.
2. In the *Security* tab, enable *CSRF Protection*.

4.3 Create Destinations

Prerequisites

- You configured SAP Business Technology Platform Mobile Services.
- You created the mobile application for SAP Warehouse Operator.
- You collected the URLs of the OData APIs from SAP S/4HANA Cloud.

For more information, see Defining Connectivity.

Procedure

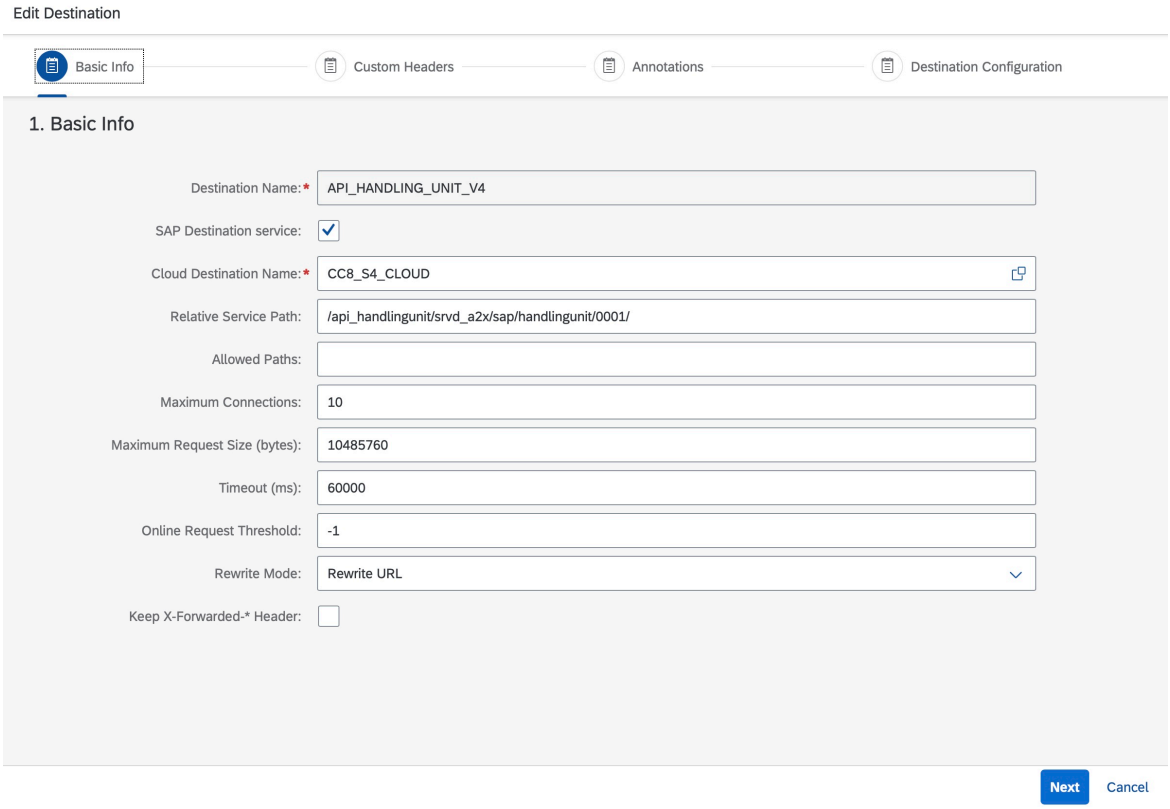
1. Configure the user propagation for SAP Business Technology Platform: User Propagation from the Cloud Foundry Environment to SAP S/4HANA Cloud. In the *Destination Configuration*, set the following parameters under *Additional Properties*:

Parameter	Value
`HTML5.DynamicDestination`	`true`
`MobileEnabled`	`true`
`WebIDEEnabled`	`true`
`WebIDEUsage`	`odata_gen`

2. Now configure the Mobile Services connectivity: Log in to the administration cockpit of SAP Business Technology Platform Mobile Service.
3. On the left-hand panel, choose *Native/Hybrid*.
4. Select *SAP Warehouse Operator* with the application ID `com.sap.mobile.apps.warehouseoperator`.
5. Choose `Mobile Connectivity` from the *Assigned Features* list.
6. In the *Mobile Destination* list, click *Create*.
7. In the dialog box, enter the data as listed in the following table:

Field	Entry
Destination Name	Enter one of the destination names from the table below.
SAP Destination Service	Checkmark this option.
Cloud Destination Name	Choose the name that you configured in your subaccount (see step 1).
Relative Service Path	Find the matching relative service paths in the table below.

This is an example of what you need to enter:



8. Click *Next*. You don't need to add information for *Custom Headers*, *Annotations*, and *Destination Configuration*. Click *Finish*.
9. Repeat these steps for all destinations using the data listed in the following table:

Destination Name	Relative Service Path
API_HANDLING_UNIT_V4	/api_handlingunit/srvd_a2x/sap/handlingunit/0001/
API_PRODUCT_V4	/api_product/srvd_a2x/sap/product/0001/
API_WAREHOUSE_V4	/api_warehouse_2/srvd_a2x/sap/warehouse/0001/
API_WAREHOUSE_RESOURCE_V4	/api_warehouse_resource_2/srvd_a2x/sap/warehouseresource/0001/
API_WAREHOUSE_ORDER_TASK_V4	/api_warehouse_order_task_2/srvd_a2x/sap/warehouseorder/0001/
API_WAREHOUSE_PHYS_STOCK_V4	/api_whse_physstockprod/srvd_a2x/sap/whsephysicalstockproducts/0001/
com.sap.mobile.apps.warehouseoperator	/api_warehouse_resource_2/srvd_a2x/sap/warehouseresource/0001/

4.4 Configure Mobile Client Log Upload

This feature allows users to upload their application logs to SAP Mobile Services so administrators can analyze them for inconsistencies or identify the root cause of an error. After the user taps *Upload Logs* inside the SAP Warehouse Operator mobile app, the logs are uploaded to SAP Mobile Services.

To view the uploaded logs, follow these steps:

1. In the SAP Mobile Services cockpit go to *Mobile Applications* > *Native/MDK* and choose your application.
2. Under *Assigned Features* choose *Mobile Client Log Upload*.
   You can now either check single log entries on the *Error Logs* tab, or check out the *Log Files* tab to get the complete log bundle that the user uploaded in the app.

Debug Log Level

In case the end users experience any issues with the app, set the *Log Level* property to `Debug` and ask the end user to upload their logs. The `Debug` log level is used for debugging purposes and includes extensive and low-level information to help you find the root cause of an error. You can find the *Log Level* property under *Mobile Client Log Upload* > *Configuration*.

> → Remember
>
> - Change the property back to `Information` after the end user has uploaded the logs. The large debug log files can cause problems.
> - Make sure to also keep the default setting of the *Delete Uploaded Log After* property at **7 days**.

For more information, see SAP Mobile Services – Configuring Mobile Client Log Upload.

4.5 Skip Orders

You can disable your users' option to temporarily skip orders to push an order to the end of the queue.

Disable the Skipping of Orders

1. Open the SAP Mobile Services Admin Cockpit of SAP Warehouse Operator.
2. Go to the *Assigned Features* list, select *Mobile Settings Exchange*.
3. Under *Feature Flags*, disable *feature.skiporder*.
4. Click *Save*.

5 Mobile Device Management (MDM)

The information in this chapter is provided to help you deploy App Config for SAP Warehouse Operator using your MDM solution of choice. With the App Config, your users don't need to use a QR code for their onboarding process and are always connected to their configured service instance. Using MDM isn't required to configure and use SAP Warehouse Operator.

Setting Up MDM

1. Create a text file that contains the following code:

```
<dict>
    <key>com.sap.mobile.apps.warehouseoperator.mobileServicesHost</key>
    <string>YOUR-HOST.com</string>
    <key>com.sap.mobile.apps.warehouseoperator.redirectURL</key>
    <string>https://YOUR-REDIRECT-URL.com</string>
    <key>com.sap.mobile.apps.warehouseoperator.clientID</key>
    <string>YOUR_CLIENT_ID</string>
</dict>
```

   Please replace the example values highlighted in **bold characters** with your own values.

Property	Description
`com.sap.mobile.apps.warehouseoperator.mobileServicesHost`	Tenant-specific SAP Mobile Services host, for example `mytenant.m.launchpad.cfapps.eu10.hana.ondemand.com` QR code property: `host`
`com.sap.mobile.apps.warehouseoperator.redirectURL`	The configured OAuth client redirect URL. It can be changed in SAP Mobile Services under the *Security* tab. QR code property: `auth→config→oauth2.clients→redirectURL`
`com.sap.mobile.apps.warehouseoperator.clientID`	The corresponding client ID of the OAuth client. It can be changed in SAP Mobile Services in the *Security* tab. QR code property: `auth→config→oauth2.clients→clientID`

2. Save the text file.
3. Upload this text file to your MDM tool and deploy the configuration to your devices.

> **Note**
>
> After enabling MDM on the administrator's side, all onboarded users receive an alert in the SAP Warehouse Operator app and are asked to onboard the app again.

6 Security

6.1 Data Protection and Privacy

This section describes the specific features and functions that SAP provides to support compliance with legal data protection requirements and data privacy.

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data privacy acts, it's necessary to consider compliance with industry-specific legislation in different countries/regions.

Application data is persisted locally in SAP Warehouse Operator and is encrypted with 256-bit AES encryption using the passcode set up by the user, or a default key if the passcode policy is deactivated.

> **i** Note
>
> In most cases, compliance with data privacy laws isn't a product feature. SAP software supports data privacy by providing security features and specific data protection-relevant functions, such as functions for the simplified blocking and deletion of personal data. SAP doesn't provide legal advice in any form. The definitions and other terms used in this guide aren't taken from any given legal source.

> **⚠** Caution
>
> The extent to which data protection is ensured depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Sensitive personal data	Special categories of personal data including social secrecy, tax secrecy, bank secrecy, social security number (U.S.), and credit card data (U.S.).

Term	Definition
Business purpose	A legal, contractual, or other justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Deletion	Deletion of personal data so that the data can no longer be used.
Retention period	The time period during which data must be available.
End of purpose (EoP)	A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization.

Passcode Protection in the Mobile Application

Administrators of SAP Warehouse Operator can configure one of the following protection scenarios:

Protection Scenario	Level of Protection	Description
App Passcode	Very High	• The user sets an application passcode during the onboarding process that fulfills the configured passcode complexity requirements. • Each time the app enters the foreground and the lock timeout has exceeded, the user has to enter the application passcode to access the app content. • All security-relevant data that is stored within the app is encrypted with a key that is derived from the application passcode.

Protection Scenario	Level of Protection	Description
Touch ID / Face ID	High	• • If Touch ID/Face ID fails, the user can also unlock the app with the device passcode. • All security-relevant data that is stored within the app is encrypted with a randomly generated key. This key is stored in the iOS key-chain and can only be read via user authentication using Touch ID/Face ID.
Default	Low	• There's no extra protection for launching the mobile app. However, device protection can still be enforced, for example by using Mobile Device Management (MDM). • All security-relevant data that is stored in the app is encrypted with a randomly generated key. This key is stored in the iOS keychain without any additional protection.

Change Log for Person-Related Data

There's no person-related data persisted on the mobile client.

Change logs must be activated in the respective back-end systems if required.

Deletion of Person-Related Data

SAP Warehouse Operator may process person-related data that is subject to data protection laws applicable in specific countries/regions as described in SAP Note 1825544: Simplified Deletion and Blocking of Personal Data in SAP Business Suite.

As there's no person-related data persisted on SAP Business Technology Platform or the Mobile Client, the respective back-end systems must provide an erasure functionality. As soon as the data is deleted or blocked in the back-end systems, it's not available anymore on the front-end, as it's a pure online application (with temporary caching). If the user deletes the SAP Warehouse Operator application from the mobile device or logs out of the application, performing those actions deletes all person-related protected data in their local data store.

6.2 Identity and Access Management

This section contains an overview about how administrators can configure the security-relevant aspects of the SAP Warehouse Operator solution.

6.2.1 Mobile Client

This topic describes the security concepts of the SAP Warehouse Operator mobile app. It also shows the possible configuration options that affect security on the mobile device.

Application Onboarding

The SAP Warehouse Operator mobile app is an SAP application that is distributed via Apple's App Store. Because of this, you need to configure which SAP Business Technology Platform (BTP) account it should connect to during the onboarding process. This process starts the very first time the app is launched on the mobile device. The required data that is used to connect to the correct SAP Business Technology Platform account is referred to as "application onboarding" in this document.

The mobile app uses QR codes to retrieve this application onboarding.

It's important that this onboarding process is secured, so that no malicious configuration data can be injected into the mobile app.

Authentication Concept

The SAP Warehouse Operator mobile app authenticates the user on SAP BTP's SAML Identity Provider during the onboarding process. After successful authentication, the mobile app requests an OAuth2 token from SAP BTP that is used for all subsequent authentication communication. If the Access Token expires, the mobile app requests a new token via the Refresh Token. This doesn't require any user interaction. If the Refresh Token is also expired, the user has to authenticate again on SAP BTP's SAML Identity Provider.

Secure Communication

All communication channels of the mobile app use the HTTPS protocol to encrypt the data in transit. The mobile app fulfills Apple's App Transport Security requirements, which ensure that a defined minimum level of security configuration is met.

Security Configuration of the Mobile App

The mobile app supports several levels of security. This is because there's always a tradeoff between security and comfort for the end user. In the most secure mode, the user always has to enter a passcode when the app moves from background into foreground. This has a significant impact on the user experience. Administrators can configure this in SAP Mobile Services, to ensure that the individual security requirements are met.

The security level is expressed by defining the protection level. The following protection levels are defined:

Level	Security	Comfort
App Passcode Protection	Very High	Low
Biometric Protection	High	Medium
Default Protection	Medium	High

The selected protection level influences how the user can access the app and also how local data is encrypted. The persisted data includes critical elements such as the OAuth2 token that is used for authentication on SAP Mobile Services.

Note that even with the lowest protection level, all of the iOS protection mechanisms apply. You can, for example, use a Mobile Device Management (MDM) system to enforce protection on the device level with a device passcode. This means that all stored data is already encrypted by the operating system. If the device is protected with a passcode, then this is already a high security level.

The protection modes that are discussed here are in addition to these default iOS device security mechanisms.

Security Configuration User Interface

Administrators configure security in the SAP Mobile Services cockpit.

Application Login

The administrator can configure a lock timeout in the cockpit. This timeout value is taken into consideration when the mobile app is launched. The mobile app shows a login screen if the protection mode is either App Passcode Protection or Touch ID/Face ID Protection, and if one of these two situations apply:

- The mobile app starts.
- The mobile app moves from the background into the foreground and the configured timeout is expired.

Depending on the app protection level, the mobile app shows either a screen to enter the app passcode or the iOS framework shows a screen to authenticate using Touch ID/Face ID (with a fallback to the device passcode).

App Protection Levels

App Passcode Protection

This protection level is applied if the administrator has checked the *Enable Passcode Policy* box.

Choosing this protection level has the following consequences:

- The user has to set an application passcode during the onboarding process that fulfills the configured complexity requirements.
- Each time the app enters the foreground and the lock timeout has exceeded, the user has to enter the application passcode to enter the app.
- All security-relevant data that is stored in the app is encrypted with a key that is derived from the app passcode.
- The app passcode is never persisted locally nor is it sent to the server.

If the administrator didn't configure the passcode policy in the cockpit, this protection level is the default.

Touch ID/Face ID Protection

This protection level is applied if the administrator has configured the passcode policy in the cockpit with these values:

Configuration Name	Configuration Value
No passcode required	false
Biometric authentication allowed	true

In addition to these settings, the following conditions must be fulfilled:

- Touch ID/Face ID is enabled on the mobile device.
- During the onboarding process, the user agreed to use Touch ID/Face ID for device unlocking.

If any of these conditions isn't met, then the mobile app uses the default protection mechanism.

Choosing this protection level has the following consequences:

- Each time the app moves to the foreground and the lock timeout has exceeded, the user has to unlock the app using Touch ID/Face ID.
- If Touch ID/Face ID fails, the user can also unlock the app with the device passcode.
- All security-relevant data that is stored in the app is encrypted with a randomly generated master key. This key is stored in the iOS keychain and can only be read if the user authenticates using Touch ID/Face ID. This key never leaves the device.

Default Protection

This protection level is applied if the administrator has configured the passcode policy in the cockpit with these values:

Configuration Name	Configuration Value
No passcode required	true

Configuration Name	Configuration Value
Biometric authentication allowed	false

Choosing this protection level has the following consequences:

- There's no extra protection for launching the mobile app. However, there can still be device protection (device passcode) that is enforced, for example using MDM.
- All security-relevant data that is stored in the app is encrypted with a randomly generated master key. This key is stored in the iOS Keychain without any additional protection. This key never leaves the device.

6.2.2 Role Concept – Mobile Services

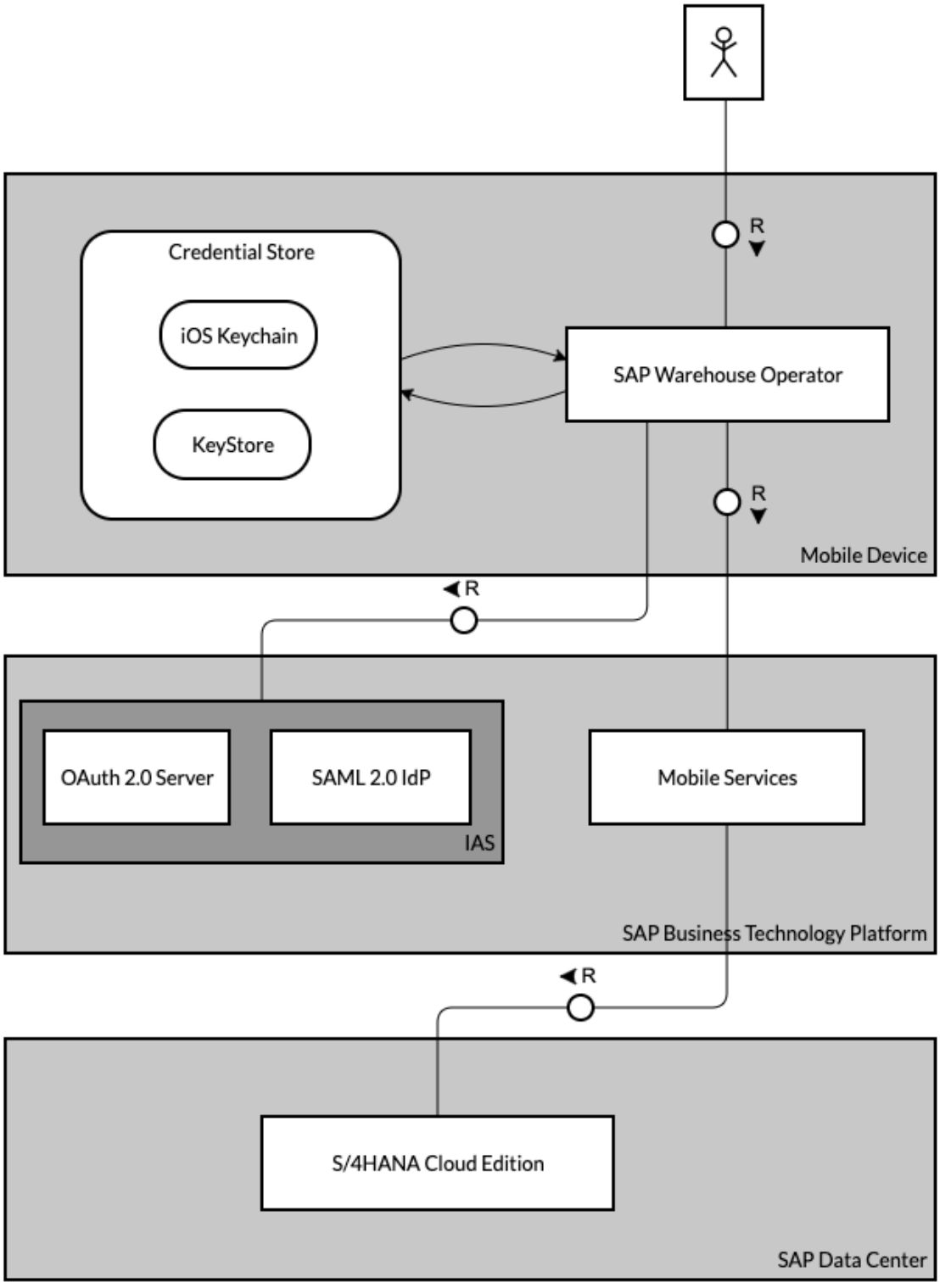
Performing administrative tasks on SAP Mobile Services should be restricted to authorized users only. SAP Mobile Services provides a set of roles that the relevant users need to be assigned to.

The list of roles and their purpose can be found here: Set Up Customer Accounts.

For information about defining groups and assigning users, see Security Administration: Managing Authentication and Authorization.

6.3 Technical System Landscape

The following diagram shows the security components in the system landscape, and especially how authentication is handled in the SAP Warehouse Operator scenario:



SAP Warehouse Operator deals with personal data. The personal data is persisted in the back-end systems of the customer and processed on the customer's mobile devices that have the SAP Warehouse Operator mobile app installed.

Communication between the SAP Warehouse Operator mobile app and SAP Business Technology Platform is secured by industry best practices and state-of-the-art open cryptographic standards. Customers use a unique, customer-specific URL. The communication channels are secured by using Transport Layer Security protocol (TLS 1.2) which is used in HTTPS. Users of the iOS application authenticate on SAP Business Technology Platform using the SAML 2.0 protocol. Based on this process step, the mobile app requests an OAuth 2.0 Token from SAP Business Technology Platform and stores it on the device in a SQLCipher database. This database uses Advanced Encryption Standard (AES) with 256-bit key length to persist its content on top of the iOS file system, which is also encrypted. Administrators on SAP Mobile Services can configure how the user has to authenticate on the mobile app to access this token. This also influences the algorithm how to create and persist the key of the SQLCipher database.

The configuration of Mobile Services and the Integration content is stored on SAP Business Technology Platform. This data can only be read and modified by authenticated users with the respective authorization roles. It's important that those roles are only assigned to administrative users. For more information, see Role Concept – Mobile Services [page 19].

In the SAP Warehouse Operator solution, no business data is stored on SAP Business Technology Platform but only in the cloud back-end systems. These back-end systems are accessed from SAP Business Technology Platform directly. The authentication to those systems is done via a principal propagation mechanism. This ensures that the mobile user that has been authenticated on SAP Business Technology Platform is propagated to the respective SAP ABAP and Java-based back-end systems. There's no technical user involved in this communication. As the back-end systems have their own User Store, the users need to be mapped and synchronized against the user database on the SAML IdP. If Identity Authentication Service is used as the SAML IdP, a variety of options exist to connect these two user stores. These are described in Corporate Identity Providers.

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 an 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

THE BEST RUN SAP