PUBLIC

Document Version: 1.0 – 2022-06-27

# SAP Direct Distribution Mobile App – Administration Guide

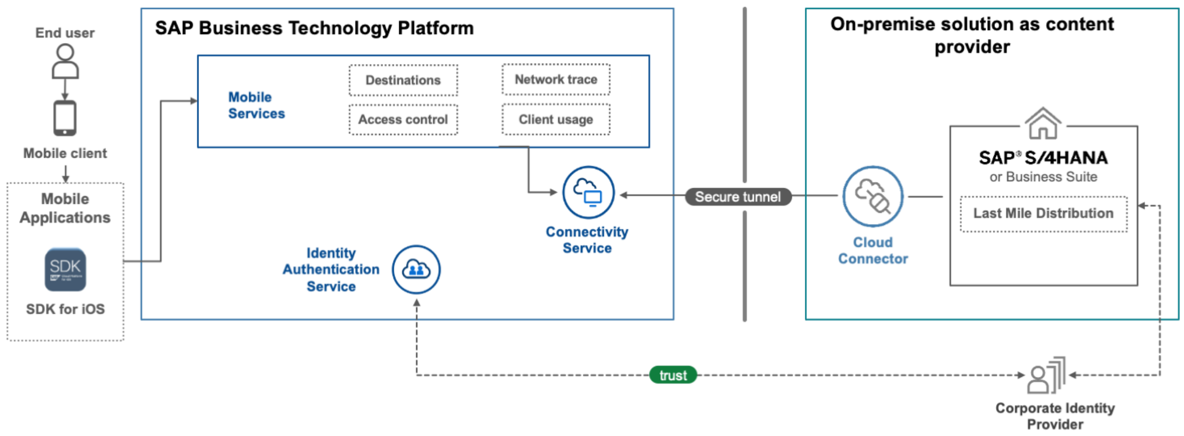
THE BEST RUN

# Content

# 1 Overview

The SAP Direct Distribution mobile app supports delivery drivers with delivering ordered goods to the final points of sale. It is a native mobile app integrated with Last Mile Distribution for Direct Distribution. For more information, see Last Mile Distribution for Direct Distribution.

This guide is aimed at system administrators. You can find end user information about how to use the SAP Direct Distribution mobile app here: SAP Direct Distribution Mobile App – Application Help.



> **i Note**
>
> The SAP Direct Distribution mobile app is available for all customers who have licensed SAP S/4HANA 2021 FPS01. The app only requires an initial activation by SAP.

# 2 System Prerequisites

To configure the infrastructure for the SAP Direct Distribution mobile app, you need the following system prerequisites:

> i Note
>
> For some of the following prerequisites, separate licenses are required.

- Application content for S/4HANA 2021 FPS01 or higher.
  See: SAP S/4HANA.
- SAP S/4HANA 2021 FPS01 Last Mile Distribution for Direct Distribution.
  See: Last Mile Distribution for Direct Distribution.

  > i Note
  >
  > The SAP Direct Distribution mobile app has to be connected to an SAP S/4HANA system in which Last Mile Distribution is implemented. To connect the app to Last Mile Distribution for Direct Distribution, a separate license is needed for SAP S/4HANA 2021 FPS01.
- SAP Business Technology Platform tenant.
  See: SAP Business Technology Platform.
- SAP Cloud connector with principal propagation.
  See: Set Up Cloud Connector.
- Configure geocoding for the SAP Direct Distribution mobile app if you want the end user to see their stops on the map.
  See: Configuring Geocoding.
- In case you configure your own IdP, it needs to be compliant with SAML 2.0 or OIDP and connected to your SAP Business Technology Platform tenant.
  See: Configure SAML 2.0 Service Provider.

# 3 Onboarding

To enable users to onboard the SAP Direct Distribution mobile app, the administrator needs to provide an onboarding QR code, which can be found in the SAP Mobile Services account.

## Context

A detailed onboarding guide for users of the SAP Direct Distribution mobile app can be found here: .

## Procedure

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

# 4 Setting Up the Mobile Adapter

In a mobile scenario, drivers use mobile devices during route execution. The mobile adapter for the Last Mile Distribution (LE-LMD) application supports the download of configuration data and master data to mobile devices and the download and upload of route data to and from mobile devices through a dedicated OData service.

The mobile adapter consists of the following components:

- Mobile Application Integration Framework (MAIF).
- OData service (LMD_MA_SMA).

## Prerequisites

> → Recommendation
>
> For performance reasons, we recommend that you run the OData service on SAP Gateway in an **embedded deployment** scenario. However, the OData service is available for both SAP Gateway in an **embedded deployment** scenario and in a **hub deployment** scenario.

To access the mobile adapter on SAP Gateway, you must perform the following steps:

- Activate SAP Gateway.
  For information, see Configuring SAP NetWeaver System for User Self Service.
- Configure the idempotent services for the SAP system.
  For information, see Defining Settings for Idempotent Services.
- Activate the business configuration set LMD_MA_SMA_OP2021FPS1.

To access the mobile adapter on SAP Gateway in a **hub deployment** scenario, you must additionally configure the SAP Gateway system aliases.

## Tasks

To set up the mobile adapter, you must perform the following tasks:

1. Configuration Settings for the Mobile Adapter [page 7]
2. Activate OData Service LMD_MA_SMA (Mobile Scenario) [page 8]
3. Check the Mobile Adapter Setup [page 10]
4. Authorizations for the Mobile Adapter [page 12]

> i Note
>
> For troubleshooting information, see our Troubleshooting page [page 32].

### Additional Configuration Settings

You can enable server-side paging and specify an adequate paging package size. For more information, see Download of Route Data.

By default, MAIF framework logging is enabled. The default log level is set to *Error*.

> → Recommendation
>
> We recommend that you set a higher log level for productive systems.

To switch off MAIF logging or to change the log level, perform the following steps:

1. Call transaction `/SYCLO/CONFIGPANEL`.
2. Go to the *System Configuration* panel and navigate to *System Settings* and then the *Technical Settings* subpanel.
3. Set the *Application Logging Level* according to your requirements.

## 4.1 Configuration Settings for the Mobile Adapter

If you have set up SAP Gateway in an **embedded deployment** scenario, see Activate OData Service LMD_MA_SMA (Mobile Scenario) [page 8] and start the procedure with step **1**. Furthermore, the following steps are required if you have set up SAP Gateway in an embedded deployment scenario.

### Activate the Services for Web Dynpro ABAP Applications

1. Call up transaction `SICF`.
2. Under the `default_host/sap/bc/webdynpro/syclo` node, activate all listed services.

### Define Intervals for Number Range Objects

For installations (not upgrades), you can define intervals for number range objects `/MFND/CS1`, `/MFND/DQ1`, and, if necessary, `/SMFND/SY1` by doing the following:

1. Call up transaction `SNRO`.
2. Enter the number range for object `/MFND/CS1`:
   ```
   Interval 01, Value 0000000001 ~ 0199999999: Client State record number
   ```
3. Enter the number range for object `/MFND/DQ1`:
   ```
   Interval 01, Value 0000000001 ~ 0199999999: Dependent Object Queue record number
   ```

### 4.1.1 Technical Settings for the Mobile Application Integration Framework

Technical settings affect all components of the framework.

#### Defining Technical Settings

To run the service by using MAIF, you must make define various technical settings by doing the following:

1. Call the transaction `/SYCLO/CONFIGPANEL`.
   A browser window opens.
2. Under *System Settings*, choose *Define System Technical Settings*.
3. Define a logging level.

   > i Note
   >
   > The *Application Logging Level* defines the logging level for all framework components. Logging entries are recorded in the SAP application log database under the object `/syclo/`.
4. Save your changes.

   > i Note
   >
   > You might be required to create a request.

## 4.2 Activate OData Service LMD_MA_SMA (Mobile Scenario)

Activate the dedicated OData service that supports a mobile scenario.

To enable the download of configuration data to mobile devices and the download and upload of route data to and from mobile devices, you need to activate the dedicated OData service.

#### Procedure

> i Note
>
> If you have set up SAP Gateway in an **embedded deployment** scenario, start the following procedure with step **1**. If SAP Gateway is activated as a **hub deployment**, start the procedure with step **2**.

1. Activate the OData service:
    1. Log on to the target client for the SAP system application as a user with administrative privileges.
    2. Call up transaction `/IWFND/MAINT_SERVICE`.
    3. If applicable, add the service from the local system alias and choose the following properties:

    | Technical Service Name | External Service Name |
    |---|---|
    | LMD_MA_SMA | LMD_MA_SMA |

    4. Set the relevant system aliases and proceed with the steps described in Configuration Settings for the Mobile Adapter [page 7].
2. Ensure that the system alias pointing to the SAP backend system from the SAP Gateway hub system has a correct RFC configuration in the backend.
    Additionally, ensure that trust relationships are correctly established between the SAP Gateway hub system and the backend system.
    For information, see the Configuring SAP NetWeaver System for User Self Service.
3. Activate the relevant OData service:
    1. Log on to the target client for the SAP Gateway hub system as a user with administrative privileges.
    2. Call up transaction `/IWFND/MAINT_SERVICE`.
    3. If applicable, add a service from the local system alias and choose the following properties:

    | Technical Service Name | External Service Name |
    |---|---|
    | LMD_MA_SMA | LMD_MA_SMA |

4. Activate the business configuration set `LMD_MA_SMA_OP2021FPS1`:
    1. Log on to the target client for the application as a user with administrative privileges.
    2. Call up transaction `SCPR20`.
    3. Activate the BC set `LMD_MA_SMA_OP2021FPS1`.

## 4.2.1 Release-Specific BC Sets

When you activate the OData service `LMD_MA_SMA` as described in Activate OData Service LMD_MA_SMA (Mobile Scenario) [page 8], you need to ensure that you activate the BC set that is relevant for your release.

### BC Sets

The following BC set is relevant for release SAP S/4HANA 2021 FPS01:

| BC Set | Description | Use |
|---|---|---|
| `LMD_MA_SMA_OP2021FPS1` | LMD Mobile Adapter for SAP Mobile Application: OP 2021 FPS1 | Contains the LMD mobile adapter OData service configuration of release SAP S/4HANA 2021 FPS01. |

## 4.3 Check the Mobile Adapter Setup

Check the setup and configuration settings of the mobile adapter.

### Procedure

1. Ensure that the required Web Dynpro that controls the behavior of the mobile application for Last Mile Distribution (`SAP_LMD_SMA`) is properly activated.
   Transactions `/SYCLO/CONFIGPANEL` and `/SYCLO/ADMIN` open the Mobile Application Integration Framework configuration panel and administration panel for the backend system.
2. Ensure that the BC set for the required version of the mobile adapter OData service is installed and activated.
   If this BC set has been properly activated, the mobile application `SAP_LMD_SMA` is displayed in transaction `/SYCLO/CONFIGPANEL` under *Mobile Application Configuration*.
3. Ensure that the OData service for the required version of the mobile adapter is activated and assigned to the *OData Service Assignment List*.
   The required OData service is displayed in transaction `/SYCLO/CONFIGPANEL` under *Mobile Application OData Service Assignment* and is assigned to the mobile application.
   The required OData service is also displayed in the list of OData services provided by the SAP Gateway system in transaction `/IWFND/MAINT_SERVICE`.
   1. In transaction `/IWFND/MAINT_SERVICE`, configure the alias assignment.
      By selecting the required OData service, the panel informs administrators which backend connection alias is used for the connection to the backend SAP Mobile Add-On services.
   2. Perform a quick test of the OData service to ensure the correct OData service document is returned by the service.
      After you select the OData service, a link to an internal test using the gateway client is included in the panel. By using the internal gateway client tool with the HTTPS connection option, system administrators can ensure that their connections reach the correct backend system from SAP Gateway and retrieve data for the proper data service providers for the mobile adapter.
   3. Ensure that the idempotency jobs are configured in the SAP Gateway system because the OData service relies on idempotency in HTTP OData services to ensure data integrity.
      You can configure idempotent services in Customizing for *SAP NetWeaver* under ▶ *SAP Gateway Service Enablement* ▶ *Backend OData Channel* ▶ *Connection Settings to SAP Gateway* ▶ *Define*

*Settings for Idempotent Services* ❯ or in transaction `WSIDPADMIN` (you need authorization to execute this transaction).

4. Ensure that the SAP backend system is set up to allow authentication of HTTPS calls.

After the OData service has been set up correctly, the OData service starts returning data in the SAP Gateway client, which can be accessed in transaction `/IWFND/GW_CLIENT`.

## 4.4 Set Up Background Jobs

Set up background jobs that support a mobile scenario.

### Procedure

1. Define the background job *Exchange Table Purge*:
    1. Define a variant for the program `/SYCLO/CORE_EXCH_PURGE_PROG` with the mobile application attribute set to `LMD_MA_SMA`.
    2. In transaction `SM36`, define a periodic background job for the `/SYCLO/CORE_EXCH_PURGE_PROG` program by using the variant defined in the previous step. Set the frequency, so that purges are performed daily.

        > **i Note**
        >
        > When the setup is completed, in transaction `/SYCLO/CONFIGPANEL`, you can specify the *Days to Keep History* for exchange table entries. To do so, go to *Exchange Object Configuration*, select the exchange object `LMD_EXCHANGE_OBJ_ROUTE_SMA`, and change the *Days to Keep History* value.

2. Define the background job *Server Side Paging Purge*:
    1. Define a variant for the program `/MFND/CORE_SVR_PAGE_PURGE_PROG` with the mobile application attribute set to the application that you are installing.
    2. In transaction `SM36`, define a periodic background job for program `/MFND/CORE_SVR_PAGE_PURGE_PROG` by using the variant defined in the previous sub-step.
3. Define the background job *Client State Purge*:
    1. Ensure that you follow the instructions in the SAP Note 2660262: *Client State Purge Utility does not support purging inactive records only*.
    2. Define a variant for program `/MFND/CORE_CLNT_ST_PURGE_PROG` and deselect the options *Active Client State Only*, *All Client States*, and *Test Run*.
    3. In transaction `SM36`, define a job for `/MFND/CORE_CLNT_ST_PURGE_PROG` as either a periodic job or a triggered-by event job by using the variant from the previous sub-step.
    For a periodic job, set the frequency according to the requirements of the client state purge. The interval defines the frequency with which previously processed client states are removed from the database.
4. Define the background job *Dependent Object Queue Purge*:
    1. Define a variant for program `/MFND/CORE_DEPOBJ_Q_PURGE_PROG` and deselect the option *Test Run*.

2. In transaction `SM36`, define a job for `/MFND/CORE_DEPOBJ_Q_PURGE_PROG` as either a periodic job or a triggered-by event job by using the variant from the previous sub-step.
   For a periodic job, set the frequency according to the requirements of the client state purge. The interval defines the frequency with which previously processed dependent object queues are removed from the database.

### Optional Settings

If necessary, you can define the background job *Inbound Transaction Queue Purge*:

1. Define a variant for the program `/SMFND/IBQ_TRANS_PURGE_PROG` and deselect the option *Test Run*.
2. In transaction `SM36`, define a job for `/SMFND/IBQ_TRANS_PURGE_PROG` as either a periodic job or a triggered-by event job by using the variant from the previous sub-step.
   For a periodic job, set the frequency according to the requirements of the client state purge. The interval defines the frequency with which previously processed dependent object queues are removed from the database.

## 4.5 Authorizations for the Mobile Adapter

To perform administrative tasks related to the mobile adapter, you need certain authorizations.

To run the OData service `LMD_MA_SMA`, specific authorizations are needed for the mobile adapter and OData service authentications must be enabled.

### Authorizations for the Mobile Adapter

You must assign authorizations to a user that is used for mobile access. For more information, see Set Up Authorizations for OData Service LMD_MA_SMA [page 13] and Mobile Access Setup [page 15].

### Authorizations for the Mobile Application Integration Framework (MAIF)

To enable MAIF background jobs and to run the corresponding reports, administrators need authorizations to run system purge utility programs. Therefore, you must define roles with the authorization required for MAIF administrative tasks. The roles must contain the following authorization:

| Authorization Object | Activity |
|---|---|
| *Mobile application - general authorization* (`/SMFND/A01`) | *Delete* |

### Authentications

To enable OData service authentications, authorizations for the relevant mobile access type (middleware access or device access) need to be set up for users. For more information, see Mobile Access Setup [page 15].

## 4.5.1 Set Up Authorizations for OData Service LMD_MA_SMA

Set up the authorizations required to download and upload route data and configuration data to and from mobile devices.

In a mobile scenario, delivery drivers and van sellers use mobile devices to record activities during route execution. The mobile adapter for Last Mile Distribution supports the download of configuration data to mobile devices and the download and upload of route data to and from mobile devices by using an OData version 2 (V2) service.

The following sections describe how to set up authorizations for the OData service `LMD_MA_SMA`.

> i Note
>
> Access to route and configuration data is additionally controlled by the authorization object `LMD_MA_AT`. Furthermore, especially for device access, users need to be granted authorizations to access this data. For more information, see Mobile Access Setup [page 15].

### Prerequisites

- You have activated the OData service and have called it at least once before you assign start authorizations. For more information see Activate OData Service LMD_MA_SMA (Mobile Scenario) [page 8].
- The way you set up roles and users for this OData service depends on the setup of SAP Gateway.
  - If SAP Gateway runs in a **hub deployment** scenario, in the SAP Gateway hub system, a role using the OData service with object type `IWSG` and the type of application *SAP Gateway: Service Groups Metadata* must be created and on the back-end server, a role using the OData service with the object type `IWSV` and the type of application *SAP Gateway Business Suite Enablement – Service* must be created and assigned to users. The roles must have the same user ID.
  - If SAP Gateway runs in an **embedded deployment** scenario, one role can be used that is assigned to both the OData service with object type `IWSV` and the OData service with object type `IWSG`.

## Procedure

> i Note
>
> If SAP Gateway runs in an **embedded deployment** scenario, you can add both services (object types `IWSV` and `IWSG`) to one `PFCG` role.

### Set Up Authorizations in the Backend System

1. Call transaction `PFCG` and create a single role.
2. Assign the authorization defaults of *SAP Gateway Business Suite Enablement – Service*:
    1. On the *Menu* tab, choose ▶ *Transaction* ▶ *Authorization Default* ▶.
       A new window opens.
    2. Select *SAP Gateway Business Suite Enablement – Service* (`IWSV`).
    3. Enter `LMD_MA_SMA 0001` and then choose *Copy*.
3. Maintain the authorizations:
    1. On the *Authorizations* tab under *Maintain Authorization Data and Generate Profiles*, choose *Change Authorization Data*.
    2. Maintain the necessary authorizations for the role.

        > i Note
        >
        > In particular, you must set up specific authorizations for authorization object `LMD_MA_AT` that control whether users who are assigned to this role can access configuration and route data by using a middleware or directly on a mobile device.

        > i Note
        >
        > You need to set up different `PFCG` roles to differentiate between users that are used for middleware access and users that are used for device access.

    3. Save your settings and then generate an authorization profile.

> i Note
>
> If full authorization is granted for authorization object `LMD_MA_AT`, all routes, irrespective of the assigned mobile access type, can be accessed by users who are assigned to this role.

### Set Up Authorizations in the SAP Gateway Hub System

1. Call transaction `PFCG` and create a single role.
2. Assign the authorization defaults of *SAP Gateway: Service Groups Metadata*:
    1. On the *Menu* tab, choose ▶ *Transaction* ▶ *Authorization Default* ▶.
       A new window opens.
    2. Select *SAP Gateway: Service Groups Metadata*.
    3. Select the OData service that is maintained and activated for the OData service with the technical service name `LMD_MA_SMA` and then choose *Copy*.

3. Maintain the authorizations:
    1. On the *Authorizations* tab under *Maintain Authorization Data and Generate Profiles*, choose *Change Authorization Data*.
    2. Maintain the necessary authorizations for the role.
    3. Save your settings and then generate an authorization profile.

### Additional Authorizations

If the OData backend service is located on a remote backend, users need RFC authorizations in the backend system (authorizations for authorization objects `S_RFC` and `S_RFCACL`). You can use the predefined role `/IWFND/RT_GW_USER` provided by SAP Gateway as a template. For more information, see Roles in the SAP Gateway Landscape. Assign the created `PFCG` role to the technical service user on the backend server.

## 4.5.2 Mobile Access Setup

Route data can be accessed by using a middleware or a mobile device. Authorizations for the relevant mobile access type need to be set up for users.

Only one mobile access type can be specified for each route type. During route assembly, the system determines the mobile access type configured for a route.

### Configuration of Mobile Access

To ensure that the data of a route can be accessed directly on a mobile device, you need to specify a mobile access for each route type. Go to Customizing for *Logistics Execution* under ▶ *Last Mile Distribution* ▶ *Basic Settings* ▶ *Map Mobile Access Types to Route Types* ◀.

> i Note
>
> During route assembly, the system determines the mobile access types of route types of the category *Mobile*.
>
> Make sure to specify a mobile access type. When no mobile access type is specified, the default *Middleware Access* is used.

> i Note
>
> Only users with the required authorizations can download and upload data directly to and from a mobile device. Users must be assigned to a business partner with the role *Driver* and must be the main driver of the relevant route. For more information, see the section below and Managing Master Data for Drivers.

## Authorizations for Mobile Access

The system checks the authorization object LMD_MA_AT (*Last Mile Distribution: Mobile Adapter Access Type*) to determine the mobile access type by which a user is authorized to access configuration and route data. The authorizations defined for authorization object LMD_MA_AT must be assigned to the PFCG roles of users that download and upload data by using the OData service.

The authorization field *Activity* (ACTVT) must have the value *Execute*. The authorization field *Mobile Access Type* (ACCESS_TYP) must have the following value:

- *Device Access*: DA

If full authorization is granted for the authorization field ACCESS_TYP, the users assigned to the corresponding PFCG roles can download and update the data of routes for which middleware access is defined and the data of routes for which device access is defined.

## User Setup for Mobile Access

For each request, the mobile adapter determines the access type based on the user that is used to access route data and the assigned authorization for authorization object LMD_MA_AT. Therefore, for mobile device access and middleware access, users of different user types must be maintained. For device access, in particular, a so-called "business user" is needed which is assigned to a business partner with the partner role *Driver*. Furthermore, different PFCG roles must be created for users that require authorizations for middleware access and for users that require authorizations for device access, as described in the following sections.

### User Setup for Middleware Access

To enable middleware access, a **technical service user** must be created by using transaction SU01.

> i Note
>
> A service user needs authorizations to access the mobile adapter service and to download and upload data. For more information about setting up authorizations to download and upload route data and configuration data, see Set Up Authorizations for OData Service LMD_MA_SMA [page 13]. In particular, the authorization field ACCESS_TYP of authorization object LMD_MA_AT must be set to ' ' for middleware access.

### User Setup for Device Access

Each route has a main driver assigned which is an SAP business partner with partner role TM0001 (*Driver*). Only specific drivers must be able to access route data directly from a mobile device. Therefore, to enable device access, a user must be created that has a relationship to a driver. Last Mile Distribution uses the **SAP S/4HANA business user** to achieve this. Furthermore, a device user needs to be assigned a PFCG role that has authorization field ACCESS_TYP of authorization object LMD_MA_AT set to DA for device access.

An SAP S/4HANA business user consists of an SU01 user and a business partner of one of the following partner role categories:

- *Employee* (BUP003)
- *External Resource* (BBP005)

- *Resource* (WFM001)

The setup of an SAP S/4HANA business user depends on whether Human Capital Management (HCM) is active. For more information about the business user concept and how to maintain a business user, see SAP Note 2570961.

### Business User for Driver

To set up a business user for a driver, the partner role *Driver* (TM0001) must be maintained for the business partner of the business user. Furthermore, the SU01 user must be assigned authorizations to access the OData service. For more information about setting up authorizations for a mobile adapter user, see Set Up Authorizations for OData Service LMD_MA_SMA [page 13].

The following steps are required to set up a business user for a driver:

1. Creation of an SU01 user
2. Creation of a business user using the SU01 user
3. Maintenance of a driver role for the business partner of the business user

## Full Access

> **Note**
>
> If a user is assigned to a role that has full authorization for authorization field ACCESS_TYP of authorization object LMD_MA_AT, then the user is authorized to access all configuration and route data, irrespective of the mobile access type that is assigned to the route or a given route type. In this case, only an SU01 user is required.

# 5 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 Launchpad Service – Configure SSO.
- You set up a connection to your SAP S/4HANA On-Premise system using the SAP Cloud Connector.
  For more information, see SAP Launchpad Service – Set Up Cloud Connector.

## Overview

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

1. Create a Mobile Application [page 18]
2. Passcode Policy [page 19]
3. Create Destinations [page 19]
4. Configure Offline Feature [page 21]

## 5.1 Create a Mobile Application

### Prerequisites

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

### Procedure

1. Log on to your SAP Mobile Services account.
2. On the left side panel, click ▶ *Mobile Applications* › *Native/Hybrid* ◀.

3. Click *New*.
4. In the dialog box that opens, fill out the mandatory fields (marked with a *) with your desired name and ID, and click *Next*.
5. 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
6. Click *Finish*.

## 5.2 Passcode Policy

### Passcode Policy

To set up and configure passcode protection for the SAP Direct Distribution mobile app, follow the steps described here: Mobile Services – Defining Client Password Policy.

## 5.3 Create Destinations

### Prerequisites

- You activated the Mobile OData Service for Last Mile Distribution.
- You set up a connection to your SAP S/4HANA On-Premise system using SAP Cloud Connector. For more information, see SAP Launchpad Service – Set Up Cloud Connector.
- You created a mobile application for SAP Direct Distribution [page 18].

### Context

The app uses a dedicated OData service, which is part of S/4HANA On-Premise. To be able to call this service, make sure that your S/4HANA On-Premise system is connected to your SAP BTP tenant using an SAP Cloud Connector, and maintain the resource-mapping path to the S/4HANA On-Premise OData service described in the next paragraphs.

i Note

Replace `<host>` and `<port>` with your respective host and port names. An example URL could be: `http://a123:456/sap/opu/odata/sap/LMD_MA_SMA`.

## Procedure

1. Log in to the administration cockpit of SAP Mobile Services.
2. On the left-hand panel, choose *Native/Hybrid*.
3. Select *SAP Direct Distribution*.
4. Choose `Mobile Connectivity` from the *Assigned Features* list.
5. In the *Mobile Destination* list, click on the *Create* icon.
6. In the dialog box, enter the data according to the following tables:

Basic Information

| Field | Entry |
|---|---|
| Destination Name | `com.sap.mobile.apps.directdistribution` |
| URL | `http://<host>:<port>/sap/opu/odata/sap/LMD_MA_SMA` |
| Use Cloud Connector | Yes |
| Maximum Connections | 10 |
| Maximum Request Size (Bytes) | 10485760 |
| Timeout | 600000 |
| Online Request Threshold | -1 |
| Rewrite Mode | Rewrite URL |

Custom Headers

| Field | Entry |
|---|---|
| sap-client | `<client>`<br>Override Client: yes |

Destination Configuration

| Field | Entry |
|---|---|
| Propagate User Name | Yes |
| SSO Mechanism | Cloud Connector SSO |

For more information on parameter values for these fields, see Defining Connectivity.

7. Click *Finish*.

## 5.4 Configure Offline Feature

The offline feature configuration allows to configure the data sync between SAP Mobile Services and the client.

### Prerequisites

- You subscribed to SAP Mobile Services.
- You created destinations.
- You created a mobile application for SAP Direct Distribution [page 18].

### App Setup

1. Log in to the administration cockpit of SAP Mobile Services.
2. On the left-hand panel, choose *Native/Hybrid*.
3. Select the SAP Direct Distribution mobile app.
4. Choose `Mobile Offline Access` from the *Assigned Features* list.
   On the *Configuration* tab, the destination created earlier should be listed.
5. Tap the import icon and upload the `.ini` file.

> → Tip
>
> You can find the `.ini` file here: 3168134.

### Activate *Upload Offline Store* Feature

This feature allows users to upload their device database to SAP Mobile Services so administrators can analyze the device data for inconsistencies or identify the root cause of an error.

> i Note
>
> If this feature isn't enabled, users will get an error message if they tap on *Upload Offline Store* in the *Settings* screen of the SAP Direct Distribution mobile app.

1. Log in to the administration cockpit of SAP Mobile Services.
2. On the left-hand panel, choose *Native/Hybrid*.
3. Select the SAP Direct Distribution mobile app.
4. Choose `Mobile Offline Access` from the *Assigned Features* list.
5. 2. On the *Offline Policies* tab, activate the *Enable Offline Store Upload* checkbox.

# 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 is necessary to consider compliance with industry-specific legislation in different countries.

> ℹ Note
>
> In most cases, compliance with data privacy laws is not 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 does not provide legal advice in any form. The definitions and other terms used in this guide are not 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 the SAP Direct Distribution mobile app 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.<br>• 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.<br>• 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 | • Each time the app enters the foreground and the lock timeout has exceeded, the user has to unlock the app using Touch ID/Face ID.<br>• If Touch ID/Face ID fails, the user can also unlock the app with the device passcode.<br>• All security-relevant data that is stored within the app is encrypted with a random generated key. This key is stored in the iOS keychain and can only be read via user authentication using Touch ID/Face ID. |
| Default | Low | • There is no extra protection for launching the mobile app. However, device protection can still be enforced, for example by using Mobile Device Management (MDM).<br>• All security-relevant data that is stored in the app is encrypted with a random generated key. This key is stored in the iOS keychain without any additional protection. |

## Change Log for Person-Related Data

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

Change logs must be activated in the respective backend systems if required.

## Deletion of Person-Related Data

The SAP Direct Distribution mobile app may process person-related data that is subject to data protection laws applicable in specific countries as described in SAP Note 1825544: Simplified Deletion and Blocking of Personal Data in SAP Business Suite.

As there is no person-related data persisted on SAP Business Technology Platform or the Mobile Client, the respective backend systems must provide an erasure functionality. As soon as the data is deleted or blocked in the backend systems, it will be not available anymore on the frontend, as it is a pure online application (with temporary caching). If the user deletes the SAP Direct Distribution mobile app 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 Direct Distribution mobile app.

- Mobile Client [page 25]
- Role Concept – Mobile Services [page 28]

### 6.2.1 Mobile Client

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

#### Application Onboarding

The SAP Direct Distribution 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 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 Direct Distribution 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 does not 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 is 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 the 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 end 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 did not 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 is not 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 random 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 |
| Biometric authentication allowed | false |

Choosing this protection level has the following consequences:

- There is 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 random generated primary 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

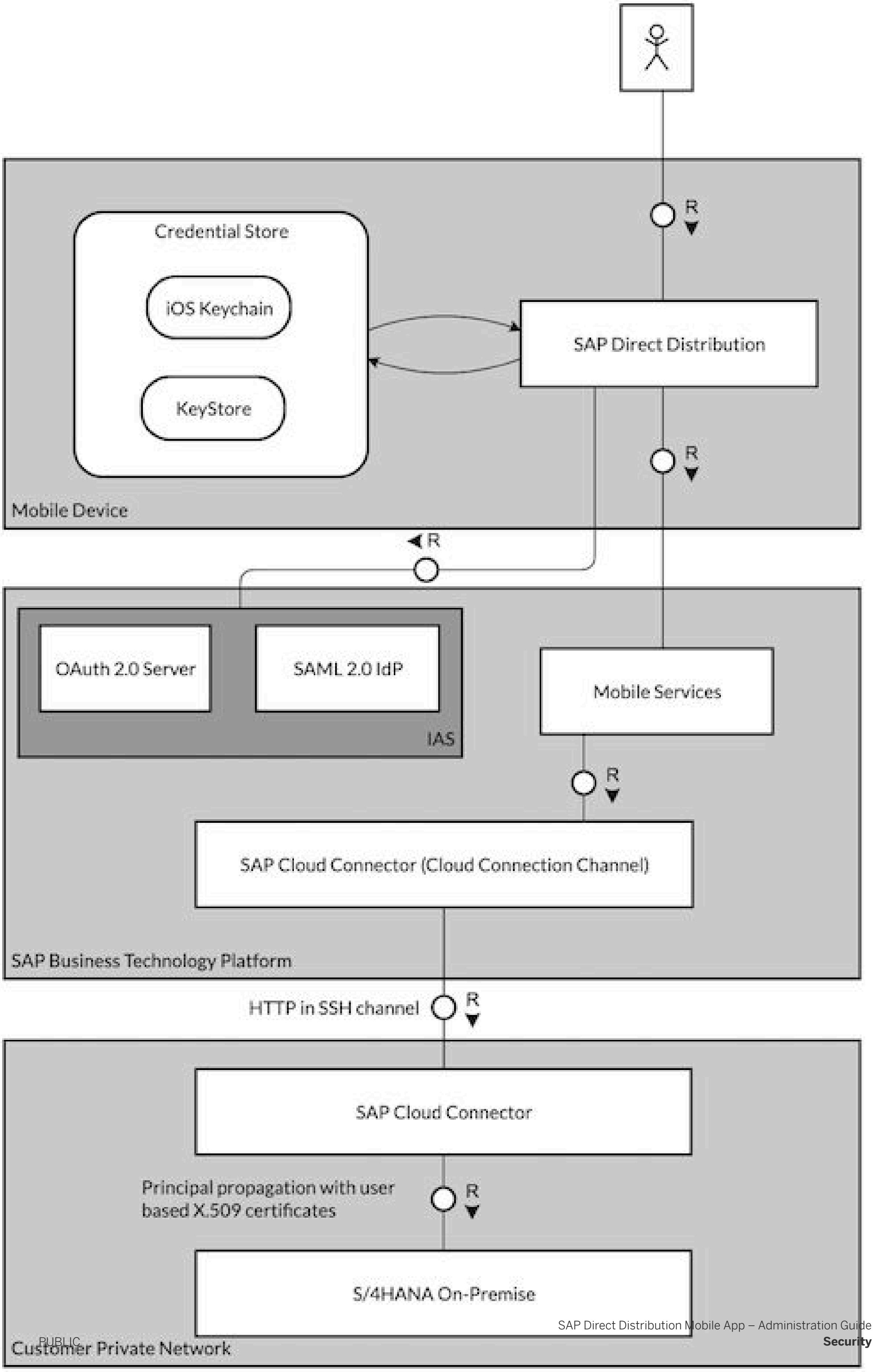
Performing administrative tasks on SAP Mobile Services should be restricted to authorized users only. SAP Mobile Services provides a set of roles that the relevant users need to be assigned to.

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 the SAP Direct Distribution mobile app scenario.


R
Credential Store
iOS Keychain
KeyStore
SAP Direct Distribution
R
Mobile Device
R
OAuth 2.0 Server
SAML 2.0 IdP
IAS
Mobile Services
R
SAP Cloud Connector (Cloud Connection Channel)
SAP Business Technology Platform
HTTP in SSH channel
R
SAP Cloud Connector
Principal propagation with user based X.509 certificates
R
S/4HANA On-Premise
Customer Private Network

The SAP Direct Distribution mobile app deals with personal data. The personal data is persisted in the Finance backend systems of the customer and processed on the customer's mobile devices that have the SDD mobile app installed.

Communication between the SAP Direct Distribution 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 SAP 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.

In the SDD mobile app, no business data is stored on SAP Business Technology Platform but only in the on-premise backends. These backend systems are accessed from SAP Business Technology Platform via the SAP Cloud Connector. The authentication to those systems is done via a principal propagation mechanism provided by the SAP Cloud Connector. 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 backend systems. There is no technical user involved in this communication. As the backend 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.

# 7 Troubleshooting

Here are some hints on how to troubleshoot potential issues with the SAP Direct Distribution mobile app.

## Configuring the Backend

### Mobile Adapter Troubleshooting

See: Last Mile Distribution – Mobile Adapter Troubleshooting

### Inbound Transaction Queue

The Inbound Transaction Monitor allows the administrator to search and view inbound transactions created for a specific mobile application. It also allows the administrator to perform full lifecycle management tasks for any given inbound transaction using the transaction inspector tool.

Open the Inbound Transaction Monitor by calling up the transaction `/SYCLO/ADMIN`. On the *Monitoring* tab, you can see all errors of all applications. Filter by selecting the SAP Direct Distribution mobile app under *Mobile Application*, and click *Search*. A list of all errors related to this app appears. Click on an error to view the details.

### Offline Store

In case a user of the SAP Direct Distribution mobile app gets an error when trying to upload the offline store, make sure you enabled the functionality in SAP Mobile Services. For more information, see Configure Offline Feature [page 21].

## Using the App

### How do I onboard the SAP Direct Distribution mobile app when using it for the first time?

For a detailed onboarding guide, see SAP Direct Distribution Mobile App – User Guide – Onboarding.

If you are not a customer of SAP, you can also try the demo mode of the SAP Direct Distribution mobile app.

### Where do I find the onboarding QR code?

You can find the onboarding QR code in your SAP Mobile Services account. For more information, see SAP Direct Distribution Mobile App – Administration Guide – Onboarding.

### I can't scan documents or access my camera roll within the app. Why?

Make sure to allow the app to access your camera and your camera roll. Open the settings of your phone, select the SAP Direct Distribution mobile app and allow the app to access all photos. Enable the camera as well if you want to scan documents and barcodes.

### I can't see my position on the map. Why?

Make sure to share your position with the app. Open the settings of your iPhone, go to ▶ *Privacy* ▶ *Location Services* ▶ and select the SAP Direct Distribution mobile app. Allow the app to access your location while using the app.

# 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

THE BEST RUN SAP