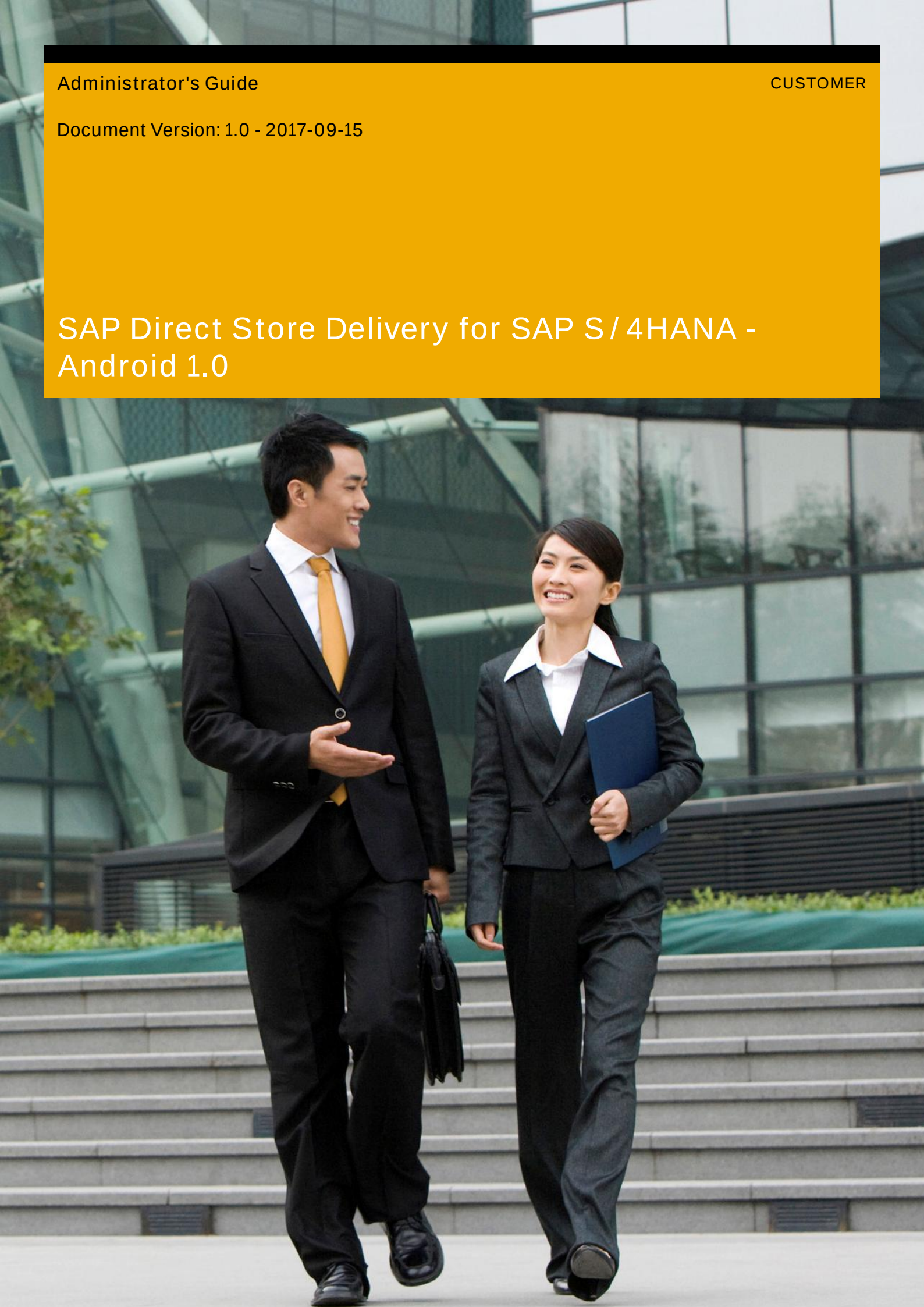
Administrator's Guide

CUSTOMER

Document Version: 1.0 - 2017-09-15

SAP Direct Store Delivery for SAP S/4HANA - Android 1.0



Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
EXAMPLE	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
EXAMPLE	Keys on the keyboard, for example, F2 or ENTER.

Document History

Version	Date	Change
1.0	2017-09-15	First Document Release

Table of Contents

1 Getting Started

1.1 About this Document

Purpose

This Administrator's Guide is the central starting point for the technical implementation of *SAP Direct Store Delivery for Android*, *option for SAP S4/HANA*. You can find cross-scenario implementation information as well as scenario-specific information in this guide.

> **Note**
>
> The central starting point for the technical upgrade of your SAP mobile app/application/solution is the Administrator's Guide, which you can find on the SAP Help Portal at https://help.sap.com/dsd.

Use the Administrator's Guide to get an overview of *SAP Direct Store Delivery for Android*, its software units, and its scenarios from a technical perspective. The Administrator's Guide is a planning tool that helps you to design your system landscape. It refers you to the required detailed documentation, mainly:

- Installation guides for single software units
- SAP Notes
- Configuration documentation
- SAP Library documentation

The Administrator's Guide consists of the following main sections:

- Section 1. Getting Started
  explains how to use this document and provides related information (documentation and SAP notes) that is crucial for installation and upgrade.
- Section 2. SAP Direct Store Delivery Overview
  introduces SAP Direct Store Delivery and its installable components. It also presents the solution component matrix and system landscape, and provides the overall implementation sequence.
- Section 3. Business Scenarios of SAP Direct Store Delivery
  describes *SAP Direct Store Delivery for Android* in the context of each supported tour scenario.
- Section 4. Solution-Wide Topics
  covers the prerequisites for using the mobile app along with the support components.
- Section 5. Security Considerations
  provides security related information for *SAP Direct Store Delivery for Android*.
- Section 6. Related Operations Information
  provides operations related information for *SAP Direct Store Delivery for Android*.
- Section 7. References
  provides the list of documents and notes relevant for the smooth running of the mobile app.
- Section 8. Media List
  provides information about how the software and documentation for SAP Direct Store Delivery is shipped.

- Section 9. Release Availability Information
  provides information about the available software release and required software for SAP Direct Store Delivery.

  > **Note**
  >
  > You can find the most current information about the technical implementation of SAP Direct Store Delivery and the latest installation and configuration guides on the SAP Help Portal at
  >
  > https://help.sap.com/dsd.
  >
  > We strongly recommend that you use the documents available here. The guides are regularly updated.

Constraints

- The business scenarios that are presented here serve as examples of how you can use SAP software in your company. The business scenarios are only intended as models and do not necessarily run the way they are described here in your customer-specific system landscape. Ensure to check your requirements and systems to determine whether these scenarios can be used productively at your site. Furthermore, we recommend that you test these scenarios thoroughly in your test systems to ensure they are complete and free of errors before going live.
- This Administrator's Guide primarily discusses the overall technical implementation of *SAP Direct Store Delivery for Android*, rather than its subordinate components. This means that additional software dependencies might exist without being mentioned explicitly in this document. You can find more information on component-specific software dependencies in the corresponding installation guides.

1.2 Related Information

1.2.1 Planning Information

For more information about planning topics not covered in this guide, see the following content on SAP Service Marketplace:

Content	Location
Latest versions of installation and upgrade guides	SAP Help Portal at the following location: http://help.sap.com/dsd
General information about SAP Direct Store Delivery	http://service.sap.com/consumerproducts → *SAP for Consumer Products Scenario: Direct Store Delivery*
Overview application information and the collection of function- and process-oriented information about SAP Direct Store Delivery	SAP Help Portal at the following location: http://help.sap.com/dsd
SAP Business Maps - information about applications and business scenarios	http://service.sap.com/businessmaps
Sizing, calculation of hardware requirements - such as CPU, disk and memory resource - with the Quick Sizer tool	http://service.sap.com/quicksizer
Released platforms and technology-related topics such as maintenance strategies and language support	http://service.sap.com/platforms
Availability and maintenance timeframe of the product	To access the Product Availability Matrix directly, enter https://support.sap.com/pam or https://service.sap.com/fbs/availability
Network security	http://service.sap.com/securityguide
High Availability	http://scn.sap.com/docs/DOC-7848
Performance	http://service.sap.com/performance
Information about Support Package Stacks, latest software versions, and patch level requirements	https://support.sap.com/patches
Information about Unicode technology	http://scn.sap.com/community/internationalization-and-unicode

1.2.2 Further Useful Links

The following table lists further useful links on SAP Service Marketplace:

Content	Location
Information about creating error messages	https://support.sap.com/incident
SAP Notes search	http://support.sap.com/notes
SAP Software Distribution Center (software download and ordering of software)	http://support.sap.com/swdc
SAP Online Knowledge Products (OKPs) – role-specific Learning Maps	http://service.sap.com/rkt

1.2.3 Related Master Guides

This Administrator's Guide is based on Master Guides for cross-industry applications. You can find more information about the relevant applications in the following documents:

Title	Location
SAP Mobile Direct Store Delivery 3.0 Master Guide and other guides	http://service.sap.com/instguides → *SAP Mobile* → *SAP Mobile Applications* → *SAP DSD* → *SAP MDSD 3.0*
Full SAP S/4HANA 1610	https://help.sap.com/ → *Product finder* → *SAP S/4HANA* → *Product Documentation*
Master Guide SAP Enhancement Package 2 for SAP CRM 7.0	http://service.sap.com/instguides → *SAP Business Suite Applications* → *SAP CRM* → *SAP CRM 7.0 Enhancement Package 2* → *Plan*
User Interface Add-On 1.0 for SAP NetWeaver	http://service.sap.com/instguides → *SAP NetWeaver* → *User Interface Add-On 1.0 for SAP NetWeaver*
User Interface Add-On 2.0 for SAP NetWeaver	http://service.sap.com/instguides → *SAP NetWeaver* → *User Interface Add-On 2.0 for SAP NetWeaver*
SAP Gateway	http://service.sap.com/instguides → *SAP NetWeaver* → *SAP Gateway* → *SAP Gateway 2.0*

1.3 Important SAP Notes

You must read the following SAP Notes before you start the installation. These SAP Notes contain the most recent information on the installation, as well as corrections to the installation documentation.

Make sure that you have the up-to-date version of each SAP Note, which you can find on SAP Service Marketplace at http://support.sap.com/notes.

SAP Note Number	Title	Description
1928776	Release Strategy for Mobile Direct Store Delivery	See this note for information about installing SAP Direct Store Delivery add-on for SAP ERP ABAP 6.0.
2276859	Installation Information for *SAP Direct Store Delivery for Android* 1.0	See this note for information about installing *SAP Direct Store Delivery for Android* mobile app.
2291828	Release restrictions/information for *SAP Direct Store Delivery for Android* 1.0	See this note for information about release restrictions and additional information about installing *SAP Direct Store Delivery for Android*
2373655	Installation Information for *SAP Direct Store Delivery for Android* Plugin Signer	See this note for information about installing *SAP Direct Store Delivery for Android* Plugin Signer.
1977108	Restrictions/Features of SAP Direct Store Delivery related to mobile offline pricing	See this note for information about offline pricing functionality of SAP Direct Store Delivery
659222	ED: Performance Index for MSEG and VBFA	See this note for information about optimizing the read performance of the table VBFA. For more information, see the section Related Operations Information.
1955420	EA-APPL corrections necessary for SAP Direct Store Delivery (MOBDSDEI)	
1873573	Enhancements for SAP Direct Store Delivery in SAP_APPL	
1899013	Enhancements for SAP Direct Store Delivery in EA-APPL	
1917902	Enhancements for Add-on SAP Direct Store Delivery in EA_APPL	

SAP Note Number	Title	Description
1929301	Enhancements for SAP Direct Store Delivery in EA_APPL	
1848999	Central Note for CommonCryptoLib 8 (replacing SAPCRYPTOLIB)	
2135717	Enable new menu items in SD transactions for Add-On SAP Direct Store Delivery (MOBDSDEI)	

2 SAP Direct Store Delivery Overview

SAP Direct Store Delivery is an SAP mobile app that supports the process of selling and distribution of goods directly to the customer store bypassing the retailer warehouses.

The Android-based mobile app provides a closed-loop solution by fully integrating DSD mobile capability with enhanced SAP Mobile Direct Store Delivery (SAP DSD) functions included in SAP S/4HANA and by making some CRM activities available from SAP Customer Relationship Management (SAP CRM).

The mobile app enables your mobile users, that is, your field sales force and delivery drivers, to respond quickly to customer needs for new and revised orders while reducing material losses.

2.1 Software Units of SAP Direct Store Delivery

SAP Direct Store Delivery comprises the following software units:

Software Unit	Description
SAP Direct Store Delivery for Android 1.0 (MOB DIR. STORE DELIV AND 1.0)	The front end part of SAP Direct Store Delivery that is installed on mobile devices with Android 5.0 Lollipop or higher. The devices are used, for example, for preselling, delivery, and van selling.
SAP Direct Store Delivery for Android Plugin Signer (MOB DIR STORE DELIV X86)	A component to sign plug-ins comprising enhancements to the *SAP Direct Store Delivery for Android* front end part. It is installed on devices with Microsoft .NET Framework 4.5.
SAP Direct Store Delivery for Mobile, integration to SAP S/4HANA (MOB DIR STORE DELIV INT S4 1.0)	One of two back end components of SAP Direct Store Delivery that is an add-on to SAP S/4HANA. In the SAP back end systems, data can be exchanged between SAP CRM 7.02, 7.12, or 7.13 and SAP S/4HANA 1610 FPS02.
SAP Direct Store Delivery for Mobile, integration to SAP CRM (MOB DIR. STORE DELIV. CRM 7.02, 7.12, 7.13 or 7.14)	The second of two back end components of SAP Direct Store Delivery that is an add-on to SAP CRM. In the SAP back end systems, data can be exchanged between SAP CRM 7.02, 7.12, 7.13 or 7.14 and SAP S/4HANA 1610 FPS02.
SAP Direct Store Delivery for Android Tour Monitor (MOB DIR STORE DELIV UI5)	A browser-based component based on the SAP UI Development Toolkit for HTML5 installed in SAP S/4HANA. It is used to monitor the routes of the mobile users.
User Interface Add-On 2.0 for SAP NetWeaver 2.0 SPS05 and SAP Gateway 2.0 SPS12	The underlying products for the *SAP Direct Store Delivery for Android* Tour Monitor component

Software Unit	Description
SAP S/4HANA 1610 FPS02	The underlying product for the SAP Direct Store Delivery for Mobile, integration to SAP S/4HANA (MOB DIR STORE DELIV INT S4 1.0) component
SAP Enhancement Package 2 for SAP CRM 7.0	The underlying product for the SAP Direct Store Delivery for Mobile, integration to CRM (MOB DIR. STORE DELIV. CRM 7.02, 7.12, 7.13 or 7.14) component

2.2 Software Component Matrix

This section provides an overview of which SAP Direct Store Delivery business scenario uses which software unit. For the latest component version and patch level requirements, see SAP Note 1928776.

Business Scenario	Software Units Key: X = mandatory (X) = optional							
	MOB DIR. STORE DELIV AND 1.0	MOB DIR STORE DELIV X86	MOB DIR STORE DELIV INT S4 1.0	MOB DIR. STORE DELIV. CRM 7.02, 7.12, 7.13 or 7.14	MOB DIR STORE DELIV UI5	UI Add-On 2.0 and Gateway 2.0	S/4HANA Integration	CRM Integration
Mobile Direct Store Delivery	X	(X)	X	(X)	(X)	(X)	X	(X)

Note

If SAP CRM is not integrated, MOB DIR. STORE DELIV. CRM 7.02, 7.12, 7.13 or 7.14 is also not required.

2.3 System Landscape

The system landscape varies slightly depending on whether SAP CRM is integrated. The following figure illustrates the landscape required for *SAP Direct Store Delivery for Android* and includes an overview of the architecture:

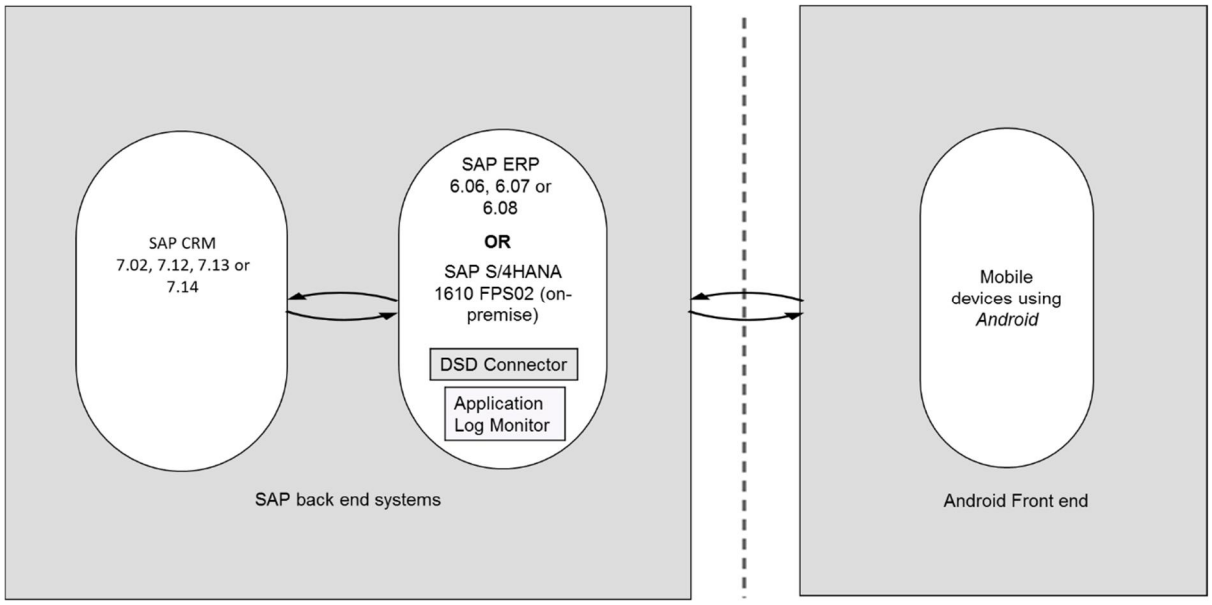


Figure 1: *SAP Direct Store Delivery for Android* System Landscape

In the SAP back end systems, data can be exchanged between SAP S/4HANA 1610 FPS02 and SAP CRM 7.02, 7.12, 7.13 or 7.14.

The DSD Connector, located in SAP S/4HANA , is a staging area for downloading, uploading, and status handling of data that is relevant to the activities of mobile users. It comprises a set of database tables in the schema of the mobile app, which act as an interface between SAP systems and the mobile devices, which use Android 5.X.

At the end of tours, data uploaded from mobile devices to the back end systems via DSD Connector triggers the following:

In SAP S/4HANA , invoices and collected payments are settled in the Settlement Cockpit and Route Accounting. Sales documents, financial postings, and materials movements are updated and created.

When these processes are complete, final billing can be processed.

If SAP CRM is integrated, CRM activity data is uploaded from the DSD Connector in SAP S/4HANA to SAP CRM.

In the Application Log Monitor in SAP S/4HANA , tour statuses and application log messages from mobile devices are made available for monitoring.

Caution

We strongly recommend that you use a minimal system landscape for test and demo purposes only. For performance, scalability, high availability, and security reasons, do not use a minimal system landscape as your production landscape.

2.4 Overall Implementation Sequence

Purpose

The following table describes the overall installation sequence for *SAP Direct Store Delivery for Android*. This table contains all available software units. However, to implement a specific scenario, you only need a subset of available software units. Some are only required for special processes. For information about which software is required to implement a specific scenario, see Software Component Matrix or the scenario-specific sections under Business Scenarios of SAP Direct Store Delivery.

For the latest component version and patch level requirements, see http://service.sap.com/sp-stacks.

For documentation listed in the following table, see References.

Process

Implementation Sequence

Step	Action [Required Documentation]	Remarks/Subsequent Steps
1	Setting up a map tile server as well as route calculation server	Using map functionality is optional but recommended; See Map integration for more information
2	Install the SAP Direct Store Delivery add-on in SAP S/4HANA (back end) [Installation Note: 1928776]	
3	Install the SAP Direct Store Delivery add-on in SAP CRM (back end) [Installation Note: 1928776]	Integration with SAP CRM is optional but recommended.
4	In SAP S/4HANA, complete the Customizing of SAP Direct Store Delivery	Implementing the /EMSE/* BC-Sets is optional
5	In SAP CRM, complete the Customizing of SAP Direct Store Delivery	Customizing settings for SAP CRM are optional
6	Complete the implementation of your mobile devices in accordance with your IT and business requirements	
7	Install the *SAP Direct Store Delivery for Android* mobile app on mobile devices (front end) [Installation Note: 2276859]	
8	Install the *SAP Direct Store Delivery for Android* Plugin Signer [Installation Note: 2373655]	Plugin Signer is only required if enhancement libraries have been built

3 Business Scenarios of SAP Direct Store Delivery for Android

3.1 Mobile Direct Store Delivery

Overview

You can use this business scenario to support the selling and distribution of goods directly to the customer store bypassing the retailer warehouses.

The Android-based mobile app, *SAP Direct Store Delivery for Android*, provides a closed-loop solution by fully integrating DSD mobile capability with enhanced SAP Mobile Direct Store Delivery (SAP DSD) functions included in SAP S/4HANA and by making some CRM activities available from SAP Customer Relationship Management (SAP CRM).

The mobile app gives you the flexibility to define roles for mobile users, that is, your field sales force and delivery drivers, to enable them provide services for preselling, delivering, and van selling, as well as a mixed role that combines these roles. Mobile users who are presellers take orders, delivery drivers fulfill presold orders, and van seller sell goods from speculative loads on their vehicles.

This business scenario comprises the following business processes:

1. Taking Orders by Preseller

   You can use this business process to enable a preseller take orders from customers on a tour. At customer sites on tours, presellers use the mobile app to take orders for specific quantities of materials from their customers. Presellers can use the mobile app to capture electronic signatures to confirm orders, to perform pricing for confirmed orders, and to print copies of orders for customers. The mobile app supports presellers by enabling them to update or create CRM activities and they can use it for occasionally connected scenarios.

2. Delivering Presold Orders by Delivery Driver

   You can use this business process to enable a delivery driver fulfill presold orders for customers on a tour.

   At customer sites on tours, delivery drivers use the mobile app to deliver presold materials from their trucks. If necessary, they can change orders taken by presellers by adding items and changing item quantities. The mobile app supports the return of goods (for example, spoiled goods, incorrect items) and the return of empties, which are added to deliveries. Deliver drivers can use the mobile app to perform pricing for final deliveries and to print delivery notes, invoices, and receipts for collected payments. The mobile app supports delivery drivers by enabling them to update or create CRM activities and they can use it for occasionally connected scenarios.

3. Delivering Without Presold Orders by Van Seller

   You can use this business process to enable van sellers deliver materials without presold orders to customers on a tour.

At customer sites on tours, van sellers use the mobile app to deliver materials from a speculative load on their trucks. The mobile app supports the return of goods (for example, spoiled goods, incorrect items) and the return of empties, which are added to deliveries. Van sellers can use the mobile app to perform pricing for final deliveries and to print delivery notes, invoices, and receipts for collected payments. The mobile app supports van sellers by enabling them to update or create CRM activities and they can use it for occasionally connected scenarios.

Technical System Landscape

For details, see the section System Landscape.

Software Units

For details, see the section Software Component Matrix.

Implementation Sequence

For details, see the section Overall Implementation Sequence.

Further Information

The following documents provide more information about Mobile Direct Store Delivery.

Content	Location
Scenario Description	See the documentation in SAP Solution Manager.
Configuration Documentation	See the documentation in SAP Solution Manager.
Scenario Security Guide	For more information, see SAP Service Marketplace at http://service.sap.com/securityguide.

4 Solution-Wide Topics

4.1 Prerequisites for Using this Solution

For details about the prerequisites, see the installation notes, the section Related Operations Information, and the documentation in SAP Solution Manager. You can find the required links in the section References.

4.2 Support Components

To get support for SAP Direct Store Delivery, create incidents under the following components as applicable:

- MOB-APP-ERP-DSD for the SAP S/4HANA back end
- MOB-APP-CRM-DSD for the SAP CRM back end
- MOB-APP-DSD-CLT for the client

4.3 Customizing

For details in the SAP S/4HANA system, see Customizing for *SAP Direct Store Delivery* under *Logistics Execution → SAP Direct Store Delivery*.

For details in the SAP CRM system, see Customizing for *SAP Direct Store Delivery* under *Customer Relationship Management → SAP Direct Store Delivery.*

5 Security Considerations

This section provides an overview of the security considerations that are specific to *SAP Direct Store Delivery for Android* 1.0.

5.1 Fundamental Security Guides

For a complete list of the available SAP security guides, see SAP Security Guides on SAP Service Marketplace at http://service.sap.com/securityguide. The current version of the SAP NetWeaver security guide, which deals with general security issues, is also available via this quick link.

Additional Information

For more information about specific security topics, see the locations on SAP Service Marketplace as shown in the following table:

Content	Location
Security	http://service.sap.com/security
Security Guides	http://service.sap.com/securityguide
Released Platforms	http://service.sap.com/platforms
Network Security	http://service.sap.com/securityguide
Infrastructure Security	http://service.sap.com/securityguide
SAP Solution Manager	http://support.sap.com/solutionmanager

Additional security guides:

Content	Location
SAP S/4HANA 1610	https://help.sap.com/ → *Product finder* → *SAP S/4HANA* → *Product Documentation* → *Security Guide*
Web Dynpro ABAP	Security Guide
SAP NetWeaver User Interface Services	Security Guide
Securing SAPUI5 Applications	Security
SAP Gateway	Security Guide
Android – Security	Security

5.2 Data Protection and Privacy

Data protection is associated with numerous legal requirements and privacy concerns. This section describes the specific features and functions that SAP Direct Store Delivery provides to support compliance with the relevant legal requirements and data privacy. It does not give any advice on whether these features and functions are the best method to support company, industry, regional or country-specific requirements. This guide does not give any advice or recommendations about additional features that would be required in a particular environment; decisions related to data protection must be made on a case-by-case basis and under consideration of the given system landscape and the applicable legal requirements.

You can find more information about data protection including a glossary at https://help.sap.com/ → *Product finder → SAP S/4HANA → Product Documentation → Security Guide → Data Protection*

5.2.1 Personal Data and Sensitive Data

SAP Direct Store Delivery processes personal as well as sensitive data as part of its core business process. This data is related to the Business Partner or Employee/Solution User. In addition to the data associated with the main business purpose, additional data is also being processed by the solution. The following table gives an overview of personal and sensitive data and its purpose in SAP Direct Store Delivery:

Process Area	Personal Data	Considered as Sensitive
Finance	Payment/Collection, Pricing, Open Items	Payment method details, for example, credit card number
Marketing	Marketing campaign, Deal Condition, Marketing Attributes	-
Master Data	Names, Titles, Addresses, Email, Phone Number, Target Groups, Partner Functions	-
Sales and Distribution	Listing & Exclusion, Electronic Signatures, Sales Orders, Item Proposals, Deliveries and Invoices, PDF documents	-
Point-of-Sales Inventory	Capture On-Hand	-
Geolocation and Time	GEO- as well as time-stamps of entire tour and visits	-
Trade Assets	Equipment	-

Process Area	Personal Data	Considered as Sensitive
Non-Functional	Numbering, Tour Processor / User	-

Apart from the personal data listed before, the SAP Direct Store Delivery solution provides features and functions which allow generic data processing. These generic functions are:

- Generic Data Transport
- Plant Maintenance Notifications
- CRM Activity Surveys
- CRM Activity Notes
- CRM Marketing Attributes
- Mobile Business Object Extensions (MBO_EXT)

If personal data is being processed by these generic data containers, the customer must ensure that consent is obtained for the same. It must not be used to process any sensitive data.

5.2.2 Consent

For legal reasons, the processing of personal data may require a certain purpose. It is assumed by the SAP Direct Store Delivery solution that the purpose / consent for processing personal data has been obtained (provided by the data controller), for example, based on available business contracts between the SAP Direct Store Delivery customers and their business partners or based on employee contracts between the SAP Direct Store Delivery customers and the solution users.

Apart from the core business process of SAP Direct Store Delivery, additional processes are supported by the solution but can be deactivated in case no purpose / consent exists. These functions are:

- Geolocation tracking: Applies to business partner as well as mobile user
- Deal Condition: Applies to business partner
- Signature Capturing: Applies to business partner as well as mobile user
- Generic Data Transport: Applies to business partner as well as mobile user
- Capture on-Hand: Applies to business partner
- PDF document processing: Applies to business partner
- CRM Activity Management: Applies to business partner
- CRM Marketing: Applies to business partner

The associated functionalities are not available if set to inactive. Activation must be maintained in Customizing under *Logistics Execution → SAP Direct Store Delivery → Data Privacy and Protection → Define Consent Settings.*

> **Caution**
>
> These switches are by default disabled. Enable them only if a purpose or consent by the respective persons is available.

5.2.3 Read Access Logging

Read access to personal data is partially based on legislation, and it is subject to logging functionality. The Read Access Logging (RAL) component can be used to monitor and log read access to data and provide information such as which business users accessed personal data (for example, fields related to bank account data), and when they did so. In RAL, you can configure which read-access information to log and under which conditions.

In SAP Direct Store Delivery, sensitive personal data is accessible from the Information Report (see Reporting on Personal Data). The business configuration set `/EMSE/RAL_SHOW_DATA` , which is part of the solution, accommodates the RAL configuration for the aforementioned report and should be applied in order to enable logging for it. Once RAL for the information report is enabled, you can find the corresponding logs in the RAL monitor.

For more information about Read Access Logging, go to https://help.sap.com/ → *Product finder → SAP S/4HANA → Product Documentation → Security Guide → Data Protection → Read Access Logging.*

5.2.4 Reporting on Personal Data

SAP Direct Store Delivery provides a report which shows all personal data being processed. The report can be accessed from the SAP Easy Access screen under *SAP Menu → Logistics → Logistics Execution → SAP Direct Store Delivery → /EMSE/SHOW_DATA.*

The report can be entered using either a Business Partner, Driver ID or System User ID. In case the user is authorized to view this data, the report displays an overview section with the number of records per process area of SAP Direct Store Delivery. The authorization for this report can be setup as follows:

- Single user: The current system user can only view the personal data related to himself
- Superuser: The current system user can view the personal data related to himself, to the business partners in the assigned sales organizations and to the mobile users in the assigned driver groups

A drilldown interaction per process area is available in order to see each data record in detail.

The following process areas provide a navigation option to branch off into changing transactions:

- Finance: Change of SAP DSD specific BP data
- Marketing: Change of Deal Condition data
- Non-Functional: Change of configuration data, for example, numbering

5.2.5 Logging of Changes to Personal Data

Changes to personal data made using SAP Direct Store Delivery are logged using change documents. The following change document objects are provided by SAP Direct Store Delivery:

- /EMSE/DC: Used for changes of Deal Condition data
- /EMSE/DEBI: Used for changes of DSD specific Business Partner data
- /EMSE/DPP: Used for changes of DSD consent Customizing as well as changes to settlement interim accounting data

The created change documents can be viewed using transaction SCDO.

For more information about Logging using Change Documents, go to https://help.sap.com/ → *Product finder → SAP S/4HANA → SAP NetWeaver for SAP S/4HANA → Security Guide → Security Aspects for Lifecycle Management → Auditing and Logging → Logging of Specific Activities → Logging Using Change Documents*

5.2.6 Blocking and Erasure of Personal Data

Personal data processed by SAP Direct Store Delivery may be subject to legal requirements related to data protection and privacy in specific countries. (see SAP Note 1825544).

For legal reasons, it may be necessary to retain personal data related to a business partner or user in the system for a specified period of time, which is called as Retention Period. The retention period is the total of the residence period and the blocking period. As soon as the residence period is exceeded, the business partner or user can be blocked and the blocking period starts. In this case, if the business partner or user is blocked, access to the personal data is limited and is allowed only for users with special authorization. After the blocking period expires, which is also the end of the retention period; personal data of blocked business partners and users can be destroyed completely so that it can no longer be retrieved.

SAP Information Lifecycle Management (ILM) can be used to control the blocking and deletion of personal data being processed by SAP DSD. For using ILM, the following business functions must be activated:

- ILM
- ILM_STOR
- ILM_BLOCKING
- ILM_RULE_GENERATOR
- BUPA_ILM_BF
- DA_COCKPIT_ILM

SAP Direct Store Delivery provides/uses the following ILM objects:

ILM Object	Description
/EMSE/DC_HEAD_DESTRUCTION	Destruction of Deal Conditions
/DSD/HH_RAHD_DESTRUCTION	Destruction of Route Accounting data
/DSD/ME_TOUR_HD_DESTRUCTION	Destruction of Connector data
/DSD/SL	Archiving of Settlement data
FI_DOCUMENT	Financial Accounting Documents
RV_LIKP	Deliveries
SD_VBAK	Sales Documents
SD_VBRK	Billing Documents
CA_BUPA	Archiving of Business Partners

The following ILM specific settings must be maintained in order to determine end of business/residence period, end of purpose/blocking period and retention period:

- Definition of application rule groups (transaction *IRM_CUST_CSS*)

- Definition of application rule variants (in Customizing under *Cross-Application-Components → Data Protection → Blocking and Unblocking of Data → Business Partner → Define and Store Application Rule Variants for EoP Check*)
- Maintenance of ILM policies (transaction *IRMPOL*), audit areas (transaction *ILMARA*) and rules (transaction *IRMRULE* or directly in *IRMPOL*)
  - Retention period for all application-specific ILM Objects (see table about ILM Objects used by SAP Direct Store Delivery)
  - Residence period for master data ILM Object CA_BUPA (with audit area BUPA_DP)

SAP Direct Store Delivery utilizes the framework of the central business partner for masking and blocking of personal data. The solution provides a default set of objects and fields which comprise personal data and are blocked / masked accordingly. These objects and fields are part of the business configuration set /EMSE/MASK_BLOCKED_DATA. It is highly recommended to apply this set. Additional objects and fields (for example, custom fields) which comprise personal data should be added via Customizing under *Cross-Application-Components → Data Protection → Blocking and Unblocking of Data → Business Partner → Settings of Masking of Blocked Data → Define Fields for Masking of Blocked Data*.

The DSD Application Log Monitor visualizes a set of tables while data is in transit. As these tables, might contain personal data, the system must be made aware on how to identify the Business Partner / Mobile User from these tables. Is this BP / Mobile User in blocking period, the personal data is masked. The reference fields for identification of the BP / Mobile User must be maintained in customizing under *Logistics Execution → SAP Direct Store Delivery → Data Privacy and Protection → Define Reference Fields for DPP relevant Tables*.

Data which is in the blocking or retention period or data that is not even available in the system anymore might still reside in the mobile component of SAP Direct Store Delivery. Once the mobile application accesses the SAP DSD back end in S / 4HANA, the system carries out an end of purpose check based on the tour information provided by the mobile component. If no purpose exists, the tour is purged from the mobile device automatically. This behavior is enabled by default. It can be deactivated by navigating to the Customizing for *Define Consent Settings* under *Logistics Execution → SAP Direct Store Delivery → Data Privacy and Protection* in case obsolete tours might still comprise business critical data..

For more information about Data Protection, Blocking and Deletion of personal data as well as End of Purpose, go to https://help.sap.com/ → *Product finder → SAP S/4HANA → Product Assistance → Cross Components → Data Protection*

You can find more information about ILM at https://help.sap.com/ → *Product finder → SAP S/4HANA → Product Assistance → Cross Components → SAP Information Lifecycle Management*

5.3 User Administration and Authentication

SAP Direct Store Delivery for Android uses the user management and authentication mechanisms provided by the SAP NetWeaver platform, in particular, SAP Web Application Server ABAP. Therefore, the security recommendations and guidelines for user administration and authentication as described in the SAP Web AS Security Guide for ABAP Technology also apply to *SAP Direct Store Delivery for Android*.

In *SAP Direct Store Delivery*, a mobile user represents an SAP S / 4HANA back end standard user. This user must be mapped to a DSD driver, which is a customer with some DSD-specific settings (for more information, see the configuration guide for SAP Direct Store Delivery on the SAP Help Portal at https://help.sap.com/dsd).

Mobile users require an online connection for initial authentication; from then on, they can log in in offline mode. The data synchronization should be done in a secure environment, for example, over the company intranet. The supported authentication methods are as follows:

- Logon with client certificate → recommended method
- Basic authentication is done over HTTPS – Plain HTTP is not supported.

If certificate-based authentication is configured on the mobile device (see Configuration Settings), the root certificate(s) of the mobile clients must be imported into the SAP S/4HANA back end (see https://help.sap.com/ → *Product finder → SAP NetWeaver 7.5 → SAP NetWeaver Security Guide*). The client certificate containing the private key itself must be copied onto the respective Android device. The certificate can be stored either manually or via a Mobile Device Management system (see, for example, Configuration Discovery Service of SAP Mobile Secure). The *SAP Direct Store Delivery for Android* mobile app must be configured in order to identify the client certificate that was imported to the mobile device (see Configuration Settings).

Caution

The certificate containing the private key must be protected using the password of the mobile user. As soon as the certificate of the mobile is copied to the mobile device, this device must be considered as bound to that particular user. If a different mobile user wants to use this device, the certificate of the previous key must be removed from the device.

If basic authentication over HTTPS is used, the root certificate containing the public key of the back end must be copied onto the mobile device. The current version of DSD for Android only supports either SSL certificates issued by an official Certificate Authority (CA) which is trusted by the Android operating system or SSL certificates issued by a corporate CA. In case of a corporate CA, the public key of the issuing certificate (i.e. the .cer file of the CA or the lowest intermediate authority) must be imported to the Android device's trust store (Settings → Security → Credential Storage → Install from SD card).
Self-signed certificates are not supported as Android doesn't support importing such a certificate into its trust store.

After successful initial authentication, the user's password is encrypted using the Password-Based Key Derivation Function 2 (PBKDF2) and the cipher is stored in the local database. Along with the authentication confirmation, the SAP S/4HANA back end exposes two profile parameters that are used by the mobile device for controlling offline authentication. These parameters are as follows:

- login/fails_to_user_lock
- login/failed_user_auto_unlock

The first parameter controls the number of failed login attempts up until the mobile user is locked. The other parameter indicates whether automated unlocking of the mobile user is enabled. It this is enabled, the mobile user is unlocked after a configurable length of time (see Configuration Settings).

After a data package has been successfully downloaded, the mobile device is then linked to the registered user. To release the device, a reset must be done. You can perform the reset either after successful end-of-day data upload or manually from the navigation menu of the mobile app.

We recommend that you choose a strong password and password policy. The password can be changed from the login screen of the mobile app. Resetting the password from the mobile device requires connectivity to the SAP S/4HANA back end.

The SAP Direct Store Delivery for Android Tour Monitor is based on the *SAP NetWeaver* User Interface Services and the pertinent user administration and authentication capabilities.

For more information on SAP S/4HANA user and password management, see https://help.sap.com/ → *Product finder → SAP NetWeaver 7.5 → SAP NetWeaver Security Guide*.

5.4 Authorizations and Logging

SAP Direct Store Delivery for Android uses the authorization concept provided by SAP NetWeaver. Therefore, the recommendations and guidelines for authorizations as described in the SAP NetWeaver AS Security Guide ABAP also apply for *SAP Direct Store Delivery for Android*.

The following authorization objects specific to *SAP Direct Store Delivery for Android* are delivered/used with the mobile app:

Authorization Object	Description	Fields
/EMSE/CDAT	Description: This authorization object is used to handle the display of DSD Connector data tables in the SAP Direct Store Delivery Application Log Monitor. The second part of this authorization object is used to manage the actions for the DSD Connector data tables	ACTVT /EMSE/ACT /EMSE/CTAB
/EMSE/ALM	This authorization object is used to handle the start behavior of the SAP Direct Store Delivery Application Log Monitor. A user can only start the monitor if he has the relevant authorization.	/EMSE/ACT
/EMSE/STYP	This authorization object is used to handle the display of tours in the SAP Direct Store Delivery Application Log Monitor as well as in the Tour Monitor. The user only gets tours for his shipment type.	/EMSE/STYP
/EMSE/TUSR	This authorization object is used to handle the activity of a mobile user communicating via HTTP/S (for example, data upload from mobile device to S/4HANA). Every mobile user needs to have this authorization object assigned.	/EMSE/ACT
/EMSE/STAT	This authorization object is used in SAP Direct Store Delivery to control the maintenance of deal conditions by the deal condition status. This allows you to have a different person for creation and approval of the deal condition.	ACTVT
/EMSE/PROM	This authorization object is used in SAP Direct Store Delivery to control the maintenance of deal conditions by assignment fields.	VKORG VTWEG SPART WERKS VKGRP ACTVT
/EMSE/DCPP	This authorization object is used in SAP Direct Store Delivery to control the evaluation of deal conditions per period.	VKORG VTWEG
/EMSE/CRMR	This authorization object is used in SAP Direct Store Delivery to control the execution of the 360° activity view report.	/EMSE/ACT
/EMSE/DPPS	This authorization object is used in *SAP Direct Store Delivery* to control whether the user is allowed to view personal data of other users/business partners in report /EMSE/SHOW_DATA	TCD /EMSE/DPPS

Authorization Object	Description	Fields
/EMSE/GROU	Driver groups (from DSD Connector Cockpit) for display of personal data in transaction /EMSE/SHOW_DATA. All mobile users who belong to the assigned group can be viewed in the report.	/EMSE/GROU ACTVT
/EMSE/STTL	This authorization object is used in SAP Direct Store Delivery to control the execution of settlement overview report.	SHTYP /DSD/VPTYP /EMSE/BSO /EMSE/SLTY
/EMSE/VKOR	Sales Organizations for display of personal data in transaction /EMSE/SHOW_DATA. All business partner who belong to the assigned sales organizations can be viewed in the report.	VKORG ACTVT
/EMSE/TMON	This authorization object is used in SAP Direct Store Delivery to control the execution of the tour monitor transaction.	/EMSE/ACT
D_SDM	This authorization object is used in SAP Direct Store Delivery to control the execution of RFC enabled function modules in the DSD Connector.	ACTVT = '02'

It is strongly recommended to keep the authorizations of the mobile users to the bare minimum in order to protect the system in case user credentials are stolen.

The *SAP Direct Store Delivery for Android* Tour Monitor uses services provided by SAP Gateway 2.0. Therefore, the guidelines and means with regards to authorization and logging in SAP Gateway 2.0 apply.

In the mobile app, specific business actions or changes to the local configuration require a role password to be entered. Which settings are supported and can only be changed using special authorization is described in Configuration Settings. All changes to the configuration are logged and a backup of the version prior to the changes is created. Only changing the configuration in the navigation menu/drawer of the mobile app is supported.

The *SAP Direct Store Delivery for Android* solution provides different logging capabilities. In order to have full traceability of changes to the mobile app and system configuration, the corresponding means of the underlying SAP NetWeaver infrastructure in the back end as well as the client log on the mobile device is appropriately configured (see Configuration Settings).

The local log files from the mobile app, including the pricing engine log, can be uploaded into the Application Log Monitor. They can be viewed by selecting the corresponding application log message.

In the back end, changes to mobile app-specific configurations are logged and can be visualized using transaction code SCU3. Any security relevant actions in the back end can be audited using the Secure Audit Log. The SAP NetWeaver provides a variety of Auditing and Logging mechanisms.

The Data Storage and Mobile Device Security section describes how the client configuration is protected from any unauthorized changes.

5.5 Network and Communication Security

We strongly recommend that you use a secure communication channel and well-defined network topology for data synchronization. This applies for the communication between SAP S/4HANA and the mobile devices as well

as between the different components of SAP S/4HANA and the SAP CRM. The network protocol used between SAP S/4HANA and the mobile devices is HTTP being secured using SSL/TLS (for more information, see the Related Operations Information section in this Administrator's Guide). In order to be able to validate the SAP S/4HANA server certificate while establishing an SSL/TLS connection, the root certificate(s) of the SAP S/4HANA server must be imported to the Keystore of the respective Android device. The certificate can be imported either manually from storage (see Security Settings description of the Android device) or via a Mobile Device Management system if the same provides corresponding functionalities.
The current version of DSD for Android only supports either SSL certificates issued by an official Certificate Authority (CA) which is trusted by the Android operating system or SSL certificates issued by a corporate CA. In case of a corporate CA, the public key of the issuing certificate (i.e. the .cer file of the CA or the lowest intermediate authority) must be imported to the Android device's trust store (Settings → Security → Credential Storage → Install from SD card).
Self-signed certificates are not supported as Android doesn't support importing such a certificate into its trust store.

The *SAP Direct Store Delivery for Android* front end can be configured in order to be able to pin the server certificate that was imported to the devices' Keystore. The certificate thumbprint must be configured in the settings of the mobile app (see Configuration Settings).

> **Caution**
>
> The certificate pinning is only supported if SAP Mobile Secure is used as the certificate thumbprint can only be added to the configuration file that is deployed using the Configuration Discovery Service of SAP Mobile Secure.

It is highly recommended to use mutual SSL instead of simple SSL. The same system setup as described in User Administration and Authentication for certificate based authentication must be applied as well but a different parameter in the mobile app configuration settings must be used (see Configuration Settings).

Authentication is recommended to be configured as described in User Administration and Authentication and the Related Operations Information.

The *SAP Direct Store Delivery for Android* mobile app is based on the SAP NetWeaver platform, in particular, the SAP Web Application Server ABAP. Therefore, the recommendations and guidelines for network security as described in the SAP Security Guides for AS ABAP also apply to *SAP Direct Store Delivery for Android*.

The mobile devices connect to the *SAP S/4HANA* back end using HTTPS. In order to protect the SAP S/4HANA back end, it is strongly recommended to use one or more firewalls (Router/Packet filter) as well as a SAP Application-Level Gateway separating the systems into different network zones. To reduce the risk of server attacks, for example, Denial-of-Service, the parameters of the Internet Communication Manager is set to appropriate values. These are amongst others:

- icm/<PROT>/max_request_size_KB
- icm/conn_timeout
- icm/HTTP/auth_<xx>
- icm/max_conn
- icm/max_threads
- icm/max_services
- icm/security_log
- icm/trace_secured_data
- icm/HTTPS/verify_client
- icm/HTTP/server_cache_<xx>

- icm/HTTP/logging_<xx>

This is just a subset of all available parameters and should illustrate the various options to increase system protection.

In the SAP S/4HANA back end, *SAP Direct Store Delivery for Android* consist mainly of two major components, the DSD back end and the DSD Connector. The DSD Connector is a staging area for the data that is to be sent to mobile devices. The communication between the DSD back end and the DSD Connector is based on Remote Function Call and IDoc Interface/ALE. This allows you to deploy the DSD Connector component on a separate SAP NetWeaver Web Application Server ABAP and have an additional firewall (Router/Packet filter) as well as a SAP Application-Level Gateway separating the systems into different network zones. The separation of the DSD back end and DSD Connector into different network zones is highly recommended.

The mobile device sends the captured tour data in JSON format. In order to increase security of the SAP S/4HANA back end, a Virus Scan Interface is provided in all back end communication interfaces that are processing data sent by the mobile devices. It is strongly recommended to use external virus scanners and configure the Virus Scan Interface accordingly.

The Application Log Monitor component of the *SAP Direct Store Delivery for Android* solution is built in SAP Web Dynpro ABAP and Floorplan Manager. It is running on the DSD Connector instance. The recommendations and guidelines as described in the Web Dynpro ABAP Security Guide also apply for the Application Log Monitor component.

For the *SAP Direct Store Delivery for Android* Tour Monitor, the network and communication security as well as session security protection recommendations and configuration options from SAP Gateway 2,0 apply.

5.6 Data Storage Security and Mobile Device Security

SAP Direct Store Delivery for Android data is stored at different storages depending on the usage scenario.

Business data is stored in the database of the SAP S/4HANA and SAP CRM back end systems. For offline functionality, data is synchronized to the mobile device SQLite database.

The data that is replicated to the mobile devices is distributed to the specific mobile user. When data is downloaded from the SAP S/4HANA back end to the mobile device, only the data that has been assigned to the mobile user is downloaded to the mobile user's device. Once the data has been downloaded, the device is tightly coupled with this specific user and no other user can log in and access this data. After having finished an end-of-tour/day data upload, all data in the client database is deleted. The corresponding data in the DSD Connector is deleted asynchronously after successful transmission into the Route Accounting Database (RADB) of the DSD back end. After final settlement of the DSD tour, the RADB should be purged using transaction code */DSD/HH_RA_DELE*.

> **Caution**
>
> After deletion of data from RADB, the corresponding tours are no longer visible in the *SAP Direct Store Delivery for Android* Tour Monitor.

Sensitive personal data (for example, credit card numbers) are always encrypted after the confirmation of the corresponding business process. This data is encrypted in all layers (for more information, see the section Related Operations Information).

In order to secure the data residing on the mobile device, it is strongly recommended to enable the full disk encryption of the entire mobile device. In addition, the *SAP Direct Store Delivery for Android* mobile app encrypts the mobile SQLite database by default. Using the mobile app's settings, this encryption can be disabled.

The Android devices provide a kernel-level Application Sandbox. This allows security between mobile apps and protects the mobile apps and all their artifacts. It is strongly recommended to not compromise the Application Sandbox, for example, by Rooting of Devices. All mobile apps should keep the minimum Android Permissions as far as possible.

To protect the mobile app and device from any harm while the device is in idle time (no user interaction with the mobile device), it is strongly recommended to activate the auto-screen lock function of the mobile device with a minimum idle time.

The security of the mobile app as well as the mobile device can be significantly increased by using the Mobile Device Management System, for example, SAP Mobile Secure. SAP Mobile Secure protects the mobile device by application wrapping which allows you, for example, to control how the enterprise network is accessed, how confidential data is handled, and to restrict locations in which users can use mobile apps (see more information in the Mobile Application Protection Guide). It allows the central deployment of a wrapped version of the *SAP Direct Store Delivery for Android* mobile app to the mobile devices too.

Third party libraries such as enhancement plugins are only loaded dynamically into the mobile app if their signature has been successfully verified. To sign plugins, the *SAP Direct Store Delivery for Android* Plugin Signer must be used. More information on the Plugin Signer is provided in the *SAP Direct Store Delivery for Android* Enhancement Guide.

5.7 Enabling Encryption of Sensitive Personal Data

The SAP Direct Store Delivery solution provides encryption of certain sensitive personal data, for example, credit card numbers. This encryption is mandatory and requires the following steps to be performed in order to enable the encryption:

- The latest version of SAP CommonCryptoLib must be installed – See note 1848999
- The profile parameter `ssf/lib_codepage` must be set to 0
- A new entry, based on the template entry DFAULT, in table `SSFAPPLIC` must be maintained. The description of the new record should be *SAP DSD Mobile*.
- A new value for parameter subject `SUP` and parameter key `STRUST_APPLIC` must be maintained in Customizing under *Logistics Execution* à *SAP Direct Store Delivery* à *General Parameters* à *Maintain General Parameter Values*. This value must have the same name as the key that was maintained in table `SSFAPPLIC` in the preceding step.
- For the newly created key in table `SSFAPPLIC` new SSF parameters must be created. This can be done in transaction `STRUST` à *Environment* à *SSF Parameters.*
  New entry for the `SSFAPPLIC` key must be created and saved without any changes
  Predefined values should be:
  - Security Product: SAPSECULIP
  - SSF Format: PKCS1-V1.5 international standard PKCS#1
  - Hash Algorithm: SHA1
  - Encryption Algorithm: DES-CBC
  - Only the flag *Distribute PSE* must be activated
- A new PSE file in transaction `STRUST` must be created:
  - Select the newly created SSF application in the left-hand menu, invoke the context-menu and select *Create*
  - Select algorithm *RSA with SHA-1*
  - Select key length *2048* and press `Enter`

In *SAP Direct Store Delivery,* cancelled payments are available in the database table `/EMSE/HH_COLL_CA`. The payment information is stored in encrypted form. If this data is consumed by a custom functionality, the method `/emse/cl_payment_encrypt=>collection_dec` must be used to decrypt the information.

Additional information on payment card security in SAP S/4HANA including Logistics Execution-Direct Store Delivery can be found at https://help.sap.com/ → *Product finder* → *SAP S/4HANA* → *Product Documentation* → *Security Guide* → *Payment Card Security*

6 Related Operations Information

The general operations information for the following areas is covered in the operations guides of SAP S/4HANA, SAP CRM, and SAP NetWeaver:

- Technical system landscape
- Overview of technical runtime scenarios, which result from setting up the corresponding business scenarios
- Logging and tracing
- Technical configuration
- Backup and recovery
- Periodical tasks
- High availability concept
- Starting and stopping (by which means and in which sequence)
- Scenario administration concept (possible dependencies between scenario components)
- Concept for monitoring, error handling, restart and recovery of interfaces
- Software change management
- Scenario maintenance concept
- Concept for handling customer development
- Support desk management
- Troubleshooting

You can find more information about the corresponding operations guides of SAP S/4HANA, SAP CRM, and SAP NetWeaver in the following table:

Content	Location
Installation and operations information for SAP S/4HANA	http://service.sap.com/instguides → *SAP Business Suite Applications* → *SAP S/4HANA*
Installation and operations information for SAP CRM	http://service.sap.com/instguides → *SAP Business Suite Applications* → *SAP CRM*
Installation and operations information for SAP NetWeaver	http://service.sap.com/instguides → *SAP NetWeaver*
Installation and operations information for SAP Gateway	Installation Guide Operations Guide

For a complete list of the available SAP Operations Guides, see http://service.sap.com/instguides.

The operations information that is specific to *SAP Direct Store Delivery for Android* is included in the application help of SAP Direct Store Delivery 1.0. These topics are related to the monitoring and data archiving. For more information, see application help for SAP Direct Store Delivery on the SAP Help Portal at https://help.sap.com/dsd and choose the paths below to access the following topics:

- For Application Log Monitoring see topic *Changes to Standard Functions and New Features in the Back End*
- For Data Archiving, see topic *Changes and New Features in Support Packages*

6.1 Removal and Reprocessing of Mobile Relevant Data

The *SAP Direct Store Delivery for Android* front end is designed to be capable of running completely disconnected from the SAP S/4HANA back end. This requires you to replicate initially the data set needed by the mobile user from the back end to the mobile device. At the end of the mobile user's work day, the data captured on the mobile device is synchronized back to the SAP S/4HANA back end.

The Application Log Monitor provides different actions on all tours (mobilized data sets per user) that have been pushed into the staging area or mobile devices respectively. These actions can be used to reprocess data in case of an error or remove it from the back end components. The execution of these actions requires the role /EMSE/APPL_LOG_MON_ACTION.

- Tour Actions
  - Remove Tour - Purge tour entirely from DSD Connector and staging tables. If the tour was already downloaded to the mobile device, it must be removed there as well by selecting Reset App from the navigation menu/drawer.

    
    Caution

    Data that was already maintained on the mobile device is lost afterwards.
  - Resend Tour - A tour that was already sent to the mobile device is prepared and staged again in order to be able to download it to the mobile device.

    
    Caution

    This would allow you to download the data to a different device and would lead to inconsistencies and data loss if the same tour is processed concurrently on different devices.
  - Force Tour Upload - The tour data that was uploaded by the mobile device and stored in the DSD Connector can be pushed into the Route Accounting Database once again, for example, if an error was encountered before.
  - Force Tour Upload to CRM - The data relevant for the SAP CRM back end that was uploaded by the mobile device and stored in the DSD Connector can be pushed into SAP CRM once again, for example, if an error was encountered before.

- OCS Actions
  - Remove Last Delta - Similar to Remove Tour but can be executed only on Delta Tour packages
  - Resend Last Delta - Similar to Resend Tour but can be executed only on Delta Tour packages
  - Force Last Delta - Similar to Force Tour Upload Tour but can be executed only on Delta Tour packages
- Reload Actions
  - Reload Status - Refresh of reload status
  - Delete Reload Queue - Removal of all reloads that are staged in the DSD Connector
- Queue Actions - You can start the Restart Unit function call only if there is a tour with a queue status error, this is, an error during the upload process within the background remote function call (bgRFC) process before data was stored in the DSD Connector.

The entire database of the mobile app can be purged by executing Reset App from the navigation menu/drawer. This deletes the entire business data as well as user context from the mobile device, for example, if the corresponding tour was removed from the DSD Connector as well. A specific SUPERVISOR authorization is required to perform this action.

Caution

Data that was already maintained on the mobile device is lost afterwards.

6.2 Activation of Business Function

Some *SAP Direct Store Delivery for Android* functionality in the SAP S/4HANA can be controlled by a pertinent Enterprise Business Function which comprises one Switch.

Enterprise Business Function / Switch	Description
EBF - /EMSE/ACTIVATE_FIELDS	Activates the selection options *DSD or SAP Direct Store Delivery* in the transactions /DSD/VC_VL and /DSD/VC_VP
Switch - /DSD/EMSE	Activates some SAP CRM related fields in the transactions /DSD/VC_VL and /DSD/VC_VP
Switch - /EMSE/DEAL_CONDITIONS	Activates deal conditions in the *Sales and Distribution* process in the SAP S/4HANA back end

This Enterprise Business Function must be activated that implicitly activates the corresponding Switches.

SAP Direct Store Delivery for Android is based on the SAP S/4HANA Logistics Execution Direct Store Delivery component which requires additional Enterprise Business Functions to be activated.

6.3 Activation of Services and bgRFC

SAP Direct Store Delivery relies on the Internet Communication Framework (ICF) for communication with the mobile devices. A set of ICF services is provided by the solution which must be active in the DSD Connector. These services are as follows:

- /default_host/sap/bc/DSDng
- /default_host/sap/bc/zcheck_user
- /default_host/sap/bc/webdynpro/emse

When data is sent by the mobile application to the SAP S/4HANA back end system, the data is queued in an bgRFC. From there data is processed into the DSD Connector staging area. In case of errors while data is transferred, the bgRFC can be used to monitor the queue entries, debug and re-process the queue entries.

For more information on the activation of the ICF services as well as setting up the bgRFC interface, see Configuration Guide for SAP Direct Store Delivery.

6.4 Technical Settings – Front End

6.4.1 Configuration Settings

The *SAP Direct Store Delivery for Android* mobile app provides various technical configuration settings for the front end. These parameters can be maintained from the navigation menu/drawer. Changing some of these settings requires SUPERVISOR authorization (see Authorizations and Logging). They can only be changed after a tour has been downloaded to the mobile device.

The following parameters are provided:

Area	Parameter	Description	Value	Default	Authorization
Connection Parameters	HTTP Connection Timeout	Duration in seconds after the mobile app terminates the HTTP request in case no response was received	Integer	30	SUPERVISOR
	Communication Type	Authentication method while establishing a connection between SAP S/4HANA back end and mobile device	[Mutual SSL/Simple SSL]	Simple SSL	SUPERVISOR
	Authentication Method	Authentication method of the mobile user in the SAP S/4HANA back end	[Certificate/Basic]	Basic	SUPERVISOR
	Enable Tour Polling	Indicates whether the mobile app should poll for new data to be downloaded. If this is set to YES, flexible device pickup is not	[Yes/No]	Yes	SUPERVISOR

Area	Parameter	Description	Value	Default	Authorization
		supported for this particular device.			
	Polling Interval	Duration in seconds after a new download request is sent to SAP S/4HANA back end. Note The minimum duration is 30 seconds.	Integer	60	SUPERVISOR
Location Services	GPS Timeout	Duration in seconds after the application terminates the GPS request in case no response was received	Integer	60	SUPERVISOR
	Map Zoom Level	Zoom level of the map displaying the tour visits	Integer	10	
	Tile Server URLs	URLs of the tile server from which the map functionality should consume the map tiles	List of Strings		
Security	Lock Timeout	Duration in minutes after the mobile user is unlocked after exceeding the maximum number of ailed log on attempts	Integer [1 - 1440]	5	SUPERVISOR
	Server Certificate Thumbprints	List of root certificates which should be used by the mobile app to validate the public key certificate provided by the SAP S/4HANA back end server while establishing a TLS connection	List of Strings		SUPERVISOR

Area	Parameter	Description	Value	Default	Authorization
		Caution This parameter cannot be set from the mobile app itself			
	Client Certificate Path	The name of client certificate which should be used for mutual ssl/certificate based authentication	String - relative path		SUPERVISOR
	Encrypt Database	Encrypts the entire mobile database	[True/False]	True	SUPERVISOR Note This parameter can only be changed using SAP Mobile Secure.
Peripherals	Picture JPEG Quality	Quality of the JPEG in percentage file created as part of the attachments functionality (SAP CRM-specific)	[50 - 100]	92	
	Camera Snapshot Max Pixel Dimension	The maximum pixels used by the camera when taking picture as part of the attachments functionality (SAP CRM-specific)	[Large (1024)/Medium (400)]	Medium	
	Enable Hardware Scanner	Enables barcode scanning using an external device	[True/False]	False	
Logging	Log Level	Severity level for logging	[Fatal /Error/Warning/Info/Debug/Trace]	Error	SUPERVISOR
	Maximum Log File Size	Maximum size of log file in bytes	Integer - maximum is 10485760	5242880	SUPERVISOR
	Maximum Log Folder Size	Maximum size of folder, which accommodates all log files, in bytes	Integer - maximum is 104857600	10485760	SUPERVISOR

Area	Parameter	Description	Value	Default	Authorization
	Log Screen Performance	Logs time and memory taken by each screen transitions as well as counts accesses to the client database	[True/False]	False	
Database	Database Performance Logging	Writes database statements to the log file Caution Enabling this setting logs database queries, which might expose private data	[On/Off]	Off	SUPERVISOR
Plug-ins	Plug-ins Folder	Specifies the path from which the enhancement libraries and their signature are loaded	String - relative path		SUPERVISOR
	Plug-ins Verification Key Path	Specifies the path from which the public key for plug-in signature verification are loaded	String - relative path		SUPERVISOR
International ization	Language	Default language for the mobile app	[English/Spanish/ French/Bulgarian]	English	
	Subculture	Default two-letter subculture code for the mobile app	RFC 4646		
Reporting & Printing	Normal-Size Line Length	The maximum number of characters per line for normal fonts	Integer	80	
	Large-Size Line Length	The maximum number of characters per line for large fonts	Integer	40	
Pricing Engine	ConditionRecordCacheSize	Number of condition records to be cached by the pricing engine	Integer	5000	SUPERVISOR
	AccessSequenceCacheSize	Number of access sequences to be	Integer	50	SUPERVISOR

Area	Parameter	Description	Value	Default	Authorization
		cached by the pricing engine			
	ConditionTypeCacheSize	Number of condition types to be cached by the pricing engine	Integer	50	SUPERVISOR
	PhysicalUnitCacheSize	Number of physical units to be cached by the pricing engine	Integer	100	SUPERVISOR
	UnitsWithDimensionCacheSize	Number of unit with dimensions to be cached by the pricing engine	Integer	100	SUPERVISOR
	PricingProcedureCacheSize	Number of pricing procedures to be cached by the pricing engine	Integer	16	SUPERVISOR
	PricingProcedureNameCacheSize	Number of pricing procedure names to be cached by the pricing engine	Integer	100	SUPERVISOR
	Pricing Analysis Trace	Generates a detailed trace file of the last pricing engine run	[On/Off]	Off	SUPERVISOR
	Log Level	Severity level for logging of the pricing engine	[Tracing/Debug/Info/Warning/Error/Fatal]	Error	SUPERVISOR

6.4.2 Initial Setup of the Mobile App

After the mobile app file is installed on the mobile device, as described in the installation note 2276859, the mobile app must be configured on the very first start up. After pressing the application icon, a configuration wizard appears. You can choose to either maintain a "Direct Connection" or use "SAP Mobile Secure". After the configuration is set up, it can only be changed using the Settings menu, which is available from the mobile app's navigation drawer.

The mobile device must be in connected mode while setting up the mobile app.

6.4.2.1 Direct Connection

When selecting this type of setup, the following details must be provided to the mobile app:

- Host
- Port
- SAP Client

These three parameters should represent the full qualified name of the SAP S/4HANA back end server, the port to be used, and the SAP client of the system in which the mobile app is implemented. These parameters are used for any connection established by the mobile device to the SAP S/4HANA back end.

Once these values are maintained, they cannot be changed anymore for security reasons. Only a redeployment of the mobile app file allows you to enter different connection settings.

Any other configuration setting apart from the SAP S/4HANA connection details must be done individually from the mobile app's navigation menu/drawer.

6.4.2.2 SAP Mobile Secure

The *SAP Direct Store Delivery for Android* mobile app provides an integration of the Configuration Discovery Service of SAP Mobile Secure. This service allows you to deliver the entire application configuration information from a central instance to the mobile front end.

After choosing this configuration type, the following details must be maintained:

- Host
- Application ID
- Domain

The host is the SAP Mobile Secure server to which the configurations were uploaded. Configurations are identified using both the user's email domain and the mobile app's configuration ID that were registered at the SAP Mobile Secure server. The domain allows you to support multiple configurations for the *SAP Direct Store Delivery for Android* mobile app.

6.4.3 Android Permissions

The *SAP Direct Store Delivery for Android* front end requires the following Android Permissions in order to be fully operational:

- Internet
- InstallShortcut
- AccessCoarseLocation
- AccessFineLocation
- Camera
- Bluetooth
- WakeLock

6.5 Map Integration

The *SAP Direct Store Delivery for Android* mobile app supports two different functionalities that are integrating geographical maps:

- Visualization of visits on the mobile app
- Monitoring of tours in the SAP S/4HANA back end

In order to use these features, the setting up a separate tile server/provider is required for both functionalities.

This tile provider must be based on OpenStreetMap (OSM). Instructions on how to set up such a server is provided at SWITCH2OSM.

> **Caution**
>
> The documentation about setting up a tile server is provided under the Creative Commons Public License 2.0.

The Tour Monitor provides the calculation of routes based on geolocation data maintained for customers. In order to use this feature, the setting up of a separate route calculating server is required. This server must be based on the Open Source Routing Machine (OSRM).

> **Caution**
>
> OSRM is provided under the simplified two-clause RSD License.

The Tour Monitor, as well as the mobile app, must be configured in order to use these separate servers as described in the *SAP Direct Store Delivery for Android* Configuration Guide for the Tour Monitor and in the local configuration for the mobile app.

The Tour Monitor is available from the SAP Fiori Launchpad, which must be configured accordingly.

7 References

List of Documents

The following table lists all documents mentioned in this Administrator's Guide.

Title	Where to Find
Application Help	https://help.sap.com/dsd
Scenario Documentation	See the documentation in SAP Solution Manager. For more information about SAP Solution Manager, see SAP Service Marketplace at http://support.sap.com/solutionmanager.
Customizing Guide in SAP S/4HANA system	See Customizing for SAP Direct Store Delivery under *Logistics Execution → SAP Direct Store Delivery*.
Customizing Guide in SAP CRM system	See Customizing for SAP Direct Store Delivery under *Customer Relationship Management → SAP Direct Store Delivery*.

List of SAP Notes

The following table lists all SAP Notes mentioned in this Administrator's Guide.

SAP Note Number	Title	Description
1928776	Release Strategy for Mobile Direct Store Delivery	See this note for information about installing SAP Direct Store Delivery add-on for SAP ERP ABAP 6.0.
2276859	Installation Information for *SAP Direct Store Delivery for Android* 1.0	See this note for information about installing *SAP Direct Store Delivery for Android* mobile app.
2291828	Release restrictions/information for *SAP Direct Store Delivery for Android* 1.0	See this note for information about release restrictions and additional information about installing *SAP Direct Store Delivery for Android*

SAP Note Number	Title	Description
2373655	Installation Information for *SAP Direct Store Delivery for Android* Plugin Signer	See this note for information about installing *SAP Direct Store Delivery for Android* Plugin Signer.
1977108	Restrictions/Features of SAP Direct Store Delivery related to mobile offline pricing	See this note for information about offline pricing functionality of SAP Direct Store Delivery
659222	ED: Performance Index for MSEG and VBFA	See this note for information about optimizing the read performance of the table VBFA. For more information, see the section Related Operations Information.
1955420	EA-APPL corrections necessary for SAP Direct Store Delivery (MOBDSDEI)	
1873573	Enhancements for SAP Direct Store Delivery in SAP_APPL	
1899013	Enhancements for SAP Direct Store Delivery in EA-APPL	
1917902	Enhancements for Add-on SAP Direct Store Delivery in EA_APPL	
1929301	Enhancements for SAP Direct Store Delivery in EA_APPL	
1848999	Central Note for CommonCryptoLib 8 (replacing SAPCRYPTOLIB)	
2135717	Enable new menu items in SD transactions for Add-On SAP Direct Store Delivery (MOBDSDEI)	

8 Media List

All deliverables for *SAP Direct Store Delivery* for SAP S/4HANA are shipped electronically and no shipment is made using DVDs (or any similar data carrier media). The software and documentation download package is available on SAP Service Marketplace at http://service.sap.com/swdc.

9 Release Availability Information

For more information about currently available releases for SAP Direct Store Delivery, and for each release, the SAP standard software required to install and use the solution, see http://www.service.sap.com/fbs/availability.

www.sap.com/contactsap

Material Number