PUBLIC
SAP Work Manager
Document Version: 6.6 – 2021-10-13

SAP Work Manager Security Guide

THE BEST RUN SAP

Content

Document History

Before you begin reading this guide, be sure that you have the latest version. Find the latest version at https://help.sap.com/viewer/p/SAP_WORK_MANAGER.

The following table provides an overview of the most important document changes.

Document Version	Release Date	Description of Changes
1.0	JUL 2021	Original release of the *SAP Work Manager Security Guide*, version 6.6.
1.1	OCT 2021	Changed problematic language (ex: user master to user data)

1 Introduction

Provides an overview of the security-relevant information that apply to SAP Work Manager.

About This Document

The Security Guide provides an overview of the security-relevant information that apply to the SAP Work Manager solution, and can be used as a reference for security requirements of non-SAP on premise components.

Target Audience

- Technology consultants
- Security consultants
- System administrators

This document is not included as part of the User Guide. Such guides are only relevant for a certain phase of the software lifecycle, whereas the Security Guide provides information that is relevant for all life cycle phases.

Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, ensure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation of your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Work Manager. To assist you in securing SAP Work Manager, we provide this Security Guide.

2 Required and Essential Authorizations

2.1 Mobile User Essential Authorizations

A mobile user running the SAP Work Manager application, or any other SAP Mobile Platform based application, must have the essential authentications to call the SAP Mobile Platform through the SAP Gateway.

The following table lists the authorization objects required to run using the SAP Mobile Platform:

Authorization Object	Authorization Attribute	Value
S_SERVICE	SVR_TYPE	HT
	SVR_NAME	*

2.2 Required Authorizations for Mobile Add-On for ERP for System Utilities

The Mobile Add-On for ERP generates certain data to support mobile application integration with SAP systems as well as for administration and monitoring purposes.

A set of system utility programs are provided to allow the purge of data generated by the Mobile Add-On for ERP. Some of the utility programs are listed here:

- `/SYCLO/CORE_PURGE_UTILITY_PROG`: Allows the deletion of the mobile user record
- `/SYCLO/CORE_EXCH_PURGE_PROG`: Allows the deletion of the XChange table records
- `/SYCLO/CORE_PUSH_PURGE_PROG`: Allows the deletion of push instance records
- `/SYCLO/CORE_SYSSTAT_PURGE_PROG`: Allows the deletion of system statistic records
- `/MFND/CORE_CLNT_ST_PURGE_PROG`: Allows the deletion of client state records
- `/MFND/CORE_DEPOBJ_Q_PURGE_PROG`: Allows the deletion of dependent object queue records
- `/MFND/CORE_SVR_PAGE_PURGE_PROG`: Allows the deletion of server paging package records

The authorization object required to run the system utility programs is as follows:

Authorization Object	Authorization Attribute	Value
/SMFND/A01	/SMFND/APP	Relevant mobile application ID
	ACTVT	06

2.3 Required Authorizations for the Mobile Add-On for ERP ConfigPanel

To use the Mobile Add-On for ERP ConfigPanel, the following minimum user authorizations are required:

Authorization Object	Authorization Attribute	Value
S_START	AUTHPGMID	R3TR
	AUTHOBJTYP	WDYA
	AUTHOBJNAM	/SYCLO/CORE_CONFIG_WB
	AUTHOBJNAM	/SYCLO/CORE_CONFIG_WB_DISP
S_ICF	ICF_FIELD	SERVICE
	ICF_VALUE	SYCLOADM

The Web Dynpro application `/SYCLO/CORE_CONFIG_WB_DISP` is the display only version of the ConfigPanel.

2.4 Required Authorizations for the Mobile Add-On for ERP Administration and Monitoring Portal

To use the Mobile Add-On for ERP Administration & Monitoring Portal, the following minimum user authorizations are required:

Authorization Object	Authorization Attribute	Value
S_START	AUTHPGMID	R3TR
	AUTHOBJTYP	WDYA
	AUTHOBJNAM	/SYCLO/CORE_ADMIN_MONI_PORTAL
	AUTHOBJNAM	/SYCLO/CORE_CONFIG_WB_DISP
S_ICF	ICF_FIELD	SERVICE
	ICF_VALUE	SYCLOADM

3 Enabling Mobile-Specific Authorization Checks

Define optional mobile specific authorization checks using the Mobile Add-On for ERP ConfigPanel.

The additional authorization checks are performed in addition to the standard authorization checks performed by the standard SAP business process and business APIs.

To define mobile-specific authorization settings, navigate to *Implementation Guide (IMG)* > *Agentry SAP Framework Configuration* > *Security Settings*.

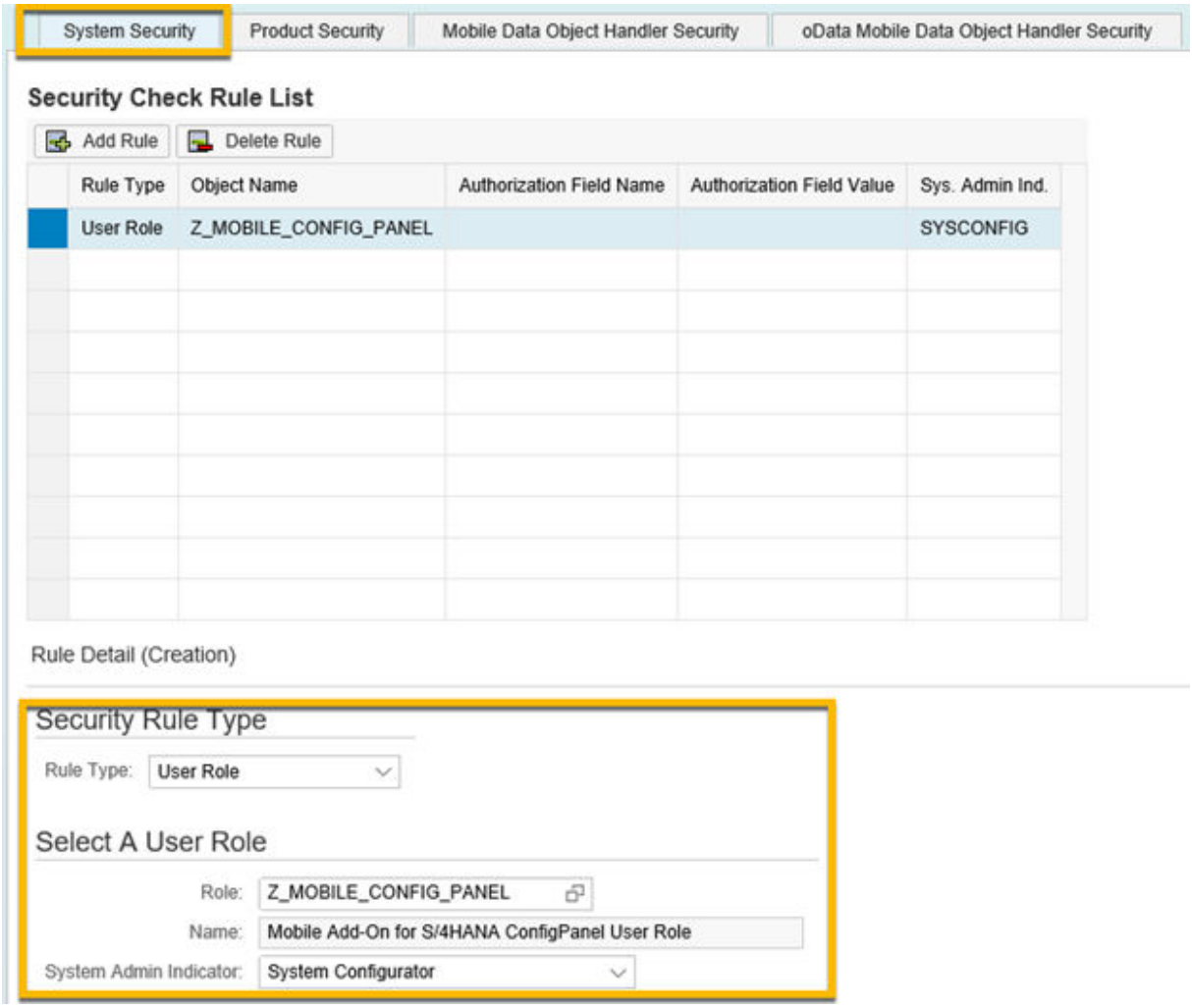
3.1 Defining Additional User Roles Required for the Mobile Add-On for ERP ConfigPanel

To perform configuration duties on the ConfigPanel, a user needs additional roles assigned to them through the Security Settings tab of the ConfigPanel.

From the *Implementation Guide (IMG)* > *Agentry SAP Framework Configuration* > *Security Settings*, then in that panel navigate to *Mobile Authorization Settings*.

Define system security rules by adding a new user with a *System Admin Indicator* of `<System Configurator>`.

Once saved, add the additional user role to the SAP user data of the user so they can user the ConfigPanel. The user role is required in addition to the authorization as described in Required Authorizations for the Mobile Add-On for ERP ConfigPanel [page 6].

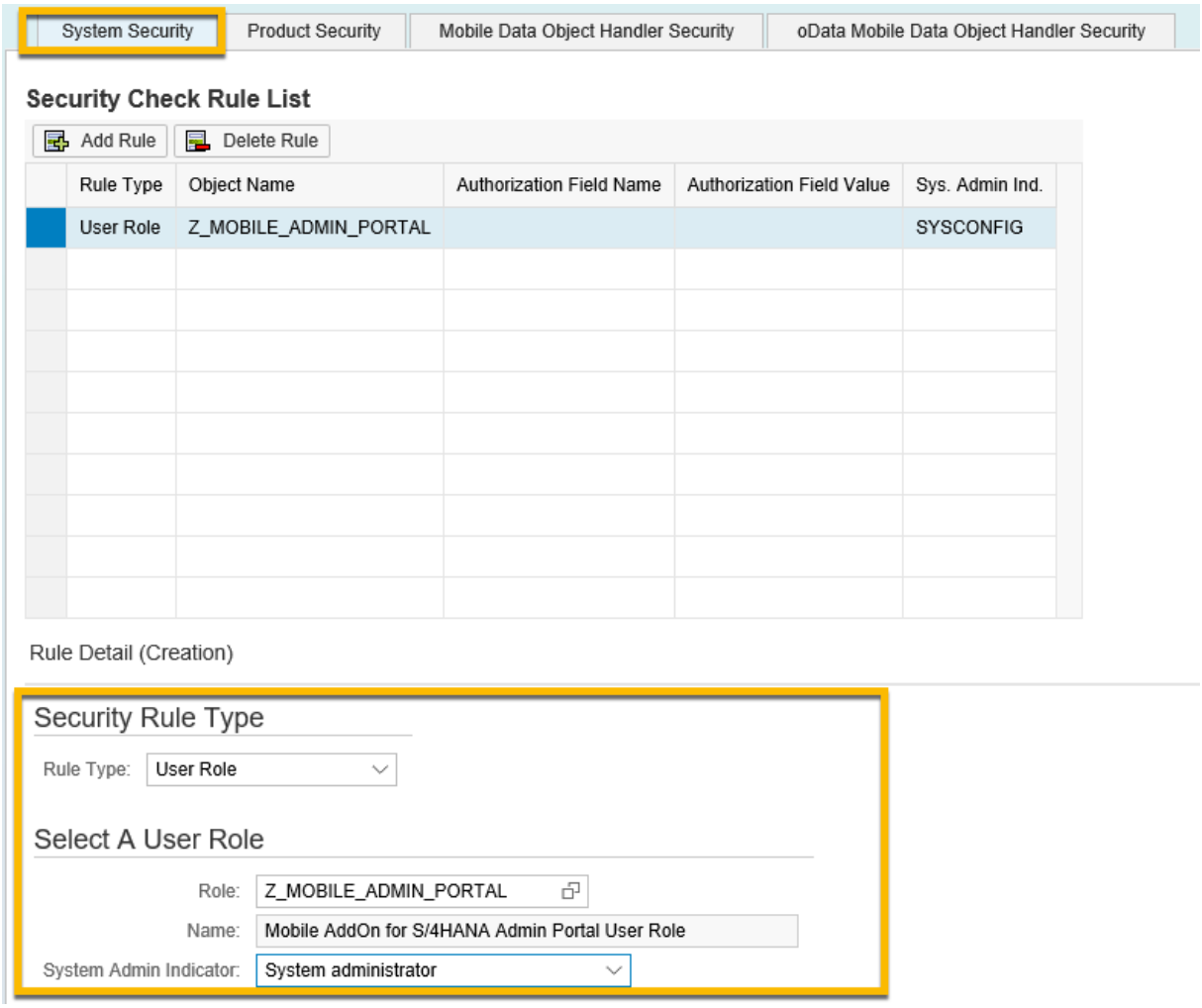


3.2 Defining Additional Roles Required for the Mobile Add-On for ERP Administration and Monitoring Tool

In the ConfigPanel, navigate to *Security Settings* > *Mobile Authorization Settings*, and define *System Security* rules with a *System Admin Indicator* of `<System Administrator>`.

Once you have saved this rule, assign the new additional user role to the SAP user admin so the user can use the Administration & Monitoring tool.

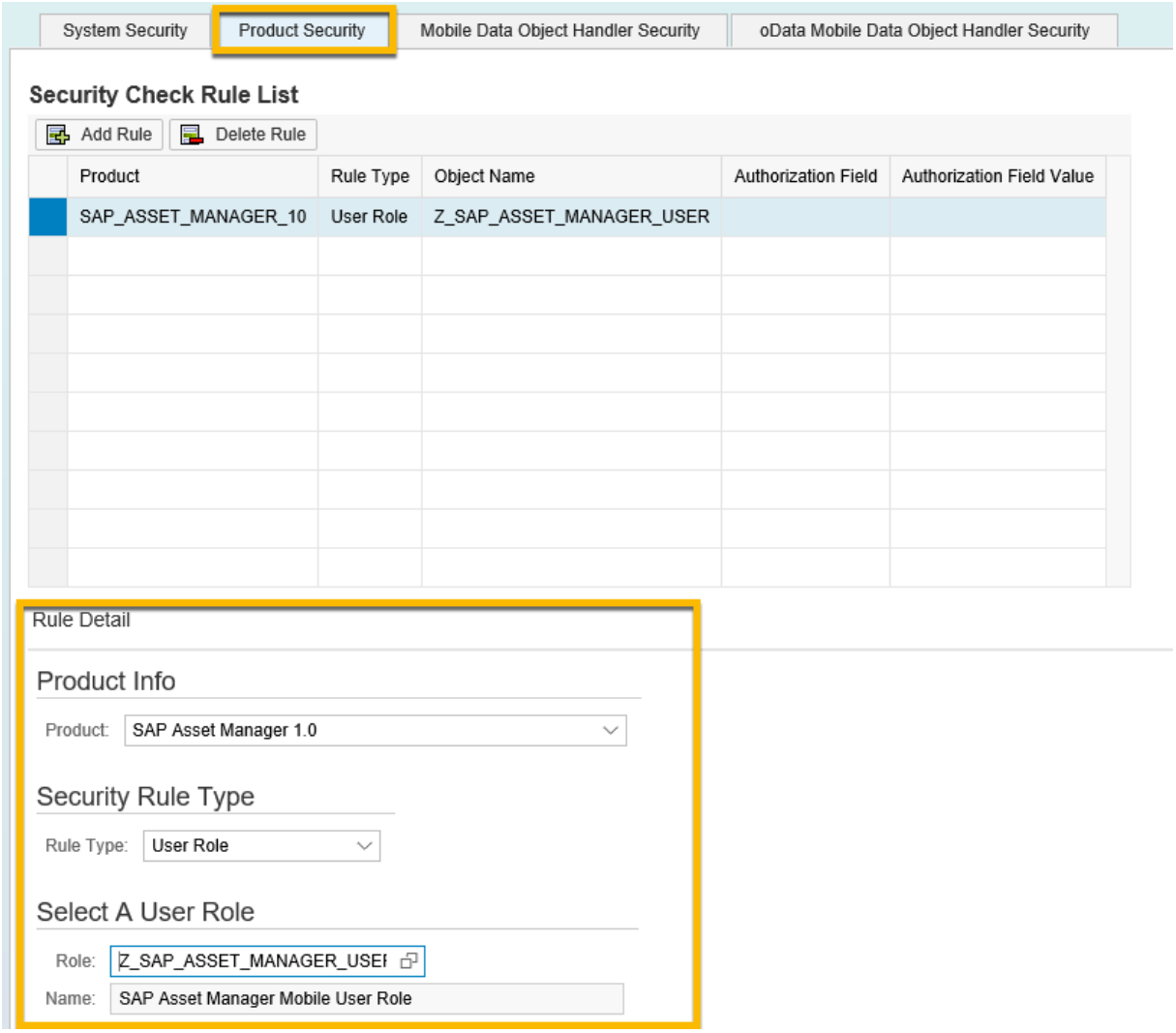
These user roles are required in addition to Required Authorizations for the Mobile Add-On for ERP ConfigPanel [page 6].



3.3 Defining an Additional User Role Required for a Mobile Application User

In the ConfigPanel, navigate to *Security Settings* > *Mobile Authorization Settings*, and define *Product Security* rules for a specific mobile application.

Once saved, assign the additional user role to the SAP user data of the user so that the user can run the mobile application from their device. These user roles are required in addition to the authorizations required in Mobile User Essential Authorizations [page 5].


System Security
Product Security
Mobile Data Object Handler Security
oData Mobile Data Object Handler Security
Security Check Rule List
Add Rule
Delete Rule
Product
Rule Type
Object Name
Authorization Field
Authorization Field Value
SAP_ASSET_MANAGER_10
User Role
Z_SAP_ASSET_MANAGER_USER
Rule Detail
Product Info
Product:
SAP Asset Manager 1.0
Security Rule Type
Rule Type:
User Role
Select A User Role
Role:
Z_SAP_ASSET_MANAGER_USEI
Name:
SAP Asset Manager Mobile User Role

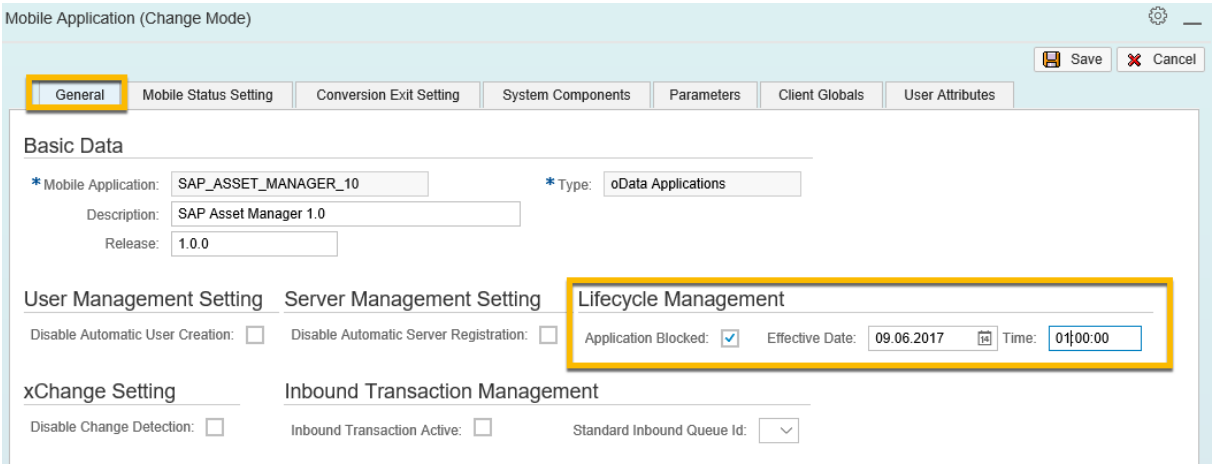
4 Disabling a Mobile Application in the SAP System

Once an application is disabled in the SAP system, all processes related to the application are disabled. No users can access the application from their mobile devices.

Change detection processes and push processes are also disabled for the mobile application.

To disable a mobile application, use the ConfigPanel of the Mobile Add-On for ERP. Navigate to *Implementation Guide (IMG)* > *Agentry SAP Framework Configuration* > *System Settings* > *Define Mobile Applications*.

Once the ConfigPanel opens in a Web browser, select your desired mobile application in the *Mobile Application* field. Then in the *General* tab in the *Lifecycle Management* section, set the *Application Blocked* to *True*. Optionally, set an *Effective Date* and *Time*. If no date and time are specified, the mobile application is disabled immediately.



5 Data Protection and Privacy

Describes the specific features and functions that SAP provides to support compliance with data protection legal 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.

This section and any other sections in this Security Guide do not give any advice on whether these features and functions are the best method to support company-, industry-, regional-, or country-specific requirements. Furthermore, this guide does not give any advice or recommendations with regard to 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.

> **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.

Glossary

Term	Definition
Personal data	Information about an identified or identifiable natural person.
Business purpose	A legal, contractual, or in other form 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 is no longer usable.
Retention period	The time period during which data must be available.

Term	Definition
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.

> ⚠ 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.

GeoLocation Data

When the user starts SAP Work Manager for the first time, and begins work on a maintenance order for an asset, they are asked interactively if they want to allow the application to use geolocation. The geolocation functionality does not collect, store, or use the geolocation data for any reason other than to show the route to the respective assets on the map.

User Consent

SAP Work Manager does not provide separate consent management, as only work-related data, such as work orders, service orders, notifications, and readings are processed by application users. User ID is used for logon, to retrieve data and process transactions. When attached documents are enabled, it may be required to access some device capabilities, such as the camera or photo library, or to access business-related documents. Before using any device capabilities, the user is asked for consent by the operating systems of Apple and Android devices. For devices running Windows, the user is not explicitly asked for consent when using device capabilities. Data collection for the purpose of executing work-related data is covered by the employee contract.

Sensitive Person-Related Data

SAP Work Manager is not designed to store sensitive person-related data. Therefore, there is no logging of sensitive person-related data.

Displaying Person-Related Data

All person-related data for SAP Work Manager is retrieved to the mobile device based on the user ID of the user. Personal data includes user ID, name, phone number, and e-mail address of the technician or technicians assigned to the work orders and operations. Business partner data such as name, address, phone number, and e-mail is also personal data if the entity is a single-member company.

Change Log for Person-Related Data

HR-based time data, through the use of the Time Sheets module, can be enabled for the SAP Work Manager application.

Person-related data created with SAP Work Manager is logged and stored on the SAP ERP on-premise system in the customer environment. See the CATS regular/Record Working Time (Web Dynpro) topic for more information.

5.1 Data Protection Aspects

Provides an overview of data protection aspects involved within the SAP Work Manager application.

> **i** Note
>
> For a complete guide to Agentry security, see the *SAP Mobile Platform Sever Guide*, section " "Security Administration | Application Security | Agentry Security".

SAP Work Manager is a business application for business-owned devices. A unique device ID, or GUID, is generated for each client device logging into the destination server through the URL of the server. The user ID can only connect to one device at a time.

Application data and business data used to process work orders and service orders is locally persisted on the device. The data is encrypted using 256-bit AES encryption.

Personal Data

Technicians log into the application through a client device with their user ID and password. While their user ID is stored in plain text on server logs and on the client, their password is encrypted and is not stored on the client. The server validates the password of the user against the back end, where it is stored.

Data is then retrieved from the server based on their user ID and associated profile and sent to the client application so they can perform their tasks. The user ID is written to some transactional data.

The *Push User* and the *Service User*, when configured upon application installation, have passwords that are viewable in the `JavaBE.ini` file. Optionally, you can encrypt these passwords in the file. However, both of

these users are intended to have minimal permissions on the client application and are not meant for daily application use.

Technicians may process the contact information of real persons that are suppliers or customers associated with work orders or service orders. Crew leaders or supervisors may view work order data assigned to other technicians.

History Data of User Input

Dates recorded are transaction times. The user ID is written for transaction data and is available to view in plain text in the server logs.

Application Logs

Active and saved user IDs are written in plain text to the `xxx-smp-server.log`. The push and service user IDs are written in plain text to the `JavaBE.ini` file. Because these IDs are written in plain text, limit dissemination and viewing of these files to administrators of the application.

5.2 Deletion of Person-Related Data

A user cannot delete individual, replicated, person-related, protected data that originates from SAP ERP in SAP Work Manager.

If the user deletes the SAP Work Manager application from the mobile device, or performs a reset of the application, performing those actions delete all person-related protected data in their local data store.

SAP Work Manager 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.

End of Purpose (EoP) Check

An end of purpose check determines whether data is still relevant for business activities based on the retention period defined for the data. The retention period of data consists of the following phases:

- **Phase one:** The relevant data is actively used.
- **Phase two:** The relevant data is actively available in the system.
- **Phase three:** The relevant data must be retained for other reasons.
  If an object is deleted by a user or by the synchronization job, it is blocked but still available in the database. Blocking of data prevents the SAP Work Manager users from displaying and using data that may include person-related data and is no longer relevant for business activities.

Blocking of data can impact system behavior in the following ways:

- **Display:** The system does not display blocked data.
- **Change:** It is not possible to change blocked data.
- **Create:** It is not possible to create objects connected to a blocked project or work package.
- **Search**: It is not possible to search for blocked data.

Deletion

Time sheet data is deleted from SAP ERP by authorized processes. Time sheet entries over the configured expiration time are added to the list of records that are automatically deleted when they are synced after a set period of time. By default, automatic deletion for time sheet records is set to two weeks. The length of time the SAP Work Manager application retains the data is determined by the configuration set by your system administrator. The application retains time sheet data for a user for a set amount of time specified in the ConfigPanel. After that period of time has passed, the system sends a tombstone, or instructions for the client application to delete the record, the next time the application syncs.

Users can request the removal of their person-related data from SAP Work Manager any time through their system administrators.

Uninstalling the app follows the standard process for your type of mobile device, and requires no special handling. When the app is uninstalled, all locally stored data is deleted as well.

We recommend that customers implement a Mobile Data Management service to forcibly uninstall the app as may be required for lost or stolen devices, or terminated employees.

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