



The Retail Innovators

SAP Dynamic Pricing by GK

Security Guide

Version: v4.0.0



COPYRIGHT

© 2022 SAP SE or an SAP affiliate company. All rights reserved. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

1. You may not use the SAP Material for a purpose competitive with SAP or its products unless otherwise clearly permitted by applicable law.
2. You may not use the SAP corporate logo.
3. No use of other SAP trademarks is granted under this section. For information regarding use of SAP trademarks, see <http://www.sap.com/corporate/en/legal/trademark.html>.

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

Internal Document Information: 1223593647 | 2022-03-02

TABLE OF CONTENTS

1	Introduction	4
2	Security of the Platform	4
2.1	Security Patches	4
2.1.1	Security Patches: Infrastructure	4
2.1.2	Security Patches: Application	4
2.2	Storage Protection	4
2.2.1	Cloud Scenario	4
2.2.2	On-Premises Scenario	4
3	User Management and Authentication	5
3.1	User Management	5
3.1.1	Overview	5
3.1.2	Roles and Permissions	5
3.1.2.1	Permissions	5
3.1.2.2	Roles	5
3.1.3	Business Units	5
3.2	Authentication	6
3.2.1	Password Policy	6
3.2.1.1	Passwords Management	6
3.2.2	Default User	6
3.2.2.1	Cloud Scenario	6
3.2.2.2	On-Premises Scenario	7
3.2.3	Security of Storage	7
3.2.3.1	Cloud Scenario	7
3.2.3.2	On-Premises Scenario	7
3.3	Database User Management	7
4	Key Management	8
5	Administration Users in the Web Client	8
5.1	Authentication Options	8
6	Network Security	9
6.1	HTTP/HTTPS	9
7	Alerting	10
7.1	Security Alert Stream	10

1 Introduction

The security concept of the AIR platform is a combination of different security mechanisms such as encryption, secure data storage, permission handling and user management.

2 Security of the Platform

2.1 Security Patches

2.1.1 Security Patches: Infrastructure

- Java Runtime: We update the docker image and the container → Minimal downtime
- Tomcat: We update the docker image and the container → Minimal downtime
- Linux: We update the docker image and the container → Minimal downtime
- Database: Cloud-provided service update

2.1.2 Security Patches: Application

Security patches are provided as patch releases of the server platform or of individual plugins. Because of our plugin environment, we are able to provide patches only for parts (plugins) of the whole platform.

There is no server downtime if we need to switch plugin versions.

Instead of the whole server, only a single plugin service has to be deactivated to deploy the new plugin versions.

2.2 Storage Protection

All data of the platform is stored in protected data stores: Operating system in container or database security.

Configuration and master data is stored in a database which has its own permission and user administration.

Type	Encryption
Database credentials	public/private key*
User credentials	hash*
Interface credentials	public/private key*

* = See details in chapters below.

2.2.1 Cloud Scenario

It is possible to provide database connections at startup of the server by environment so there is no need for local data store for such connection credentials.

2.2.2 On-Premises Scenario

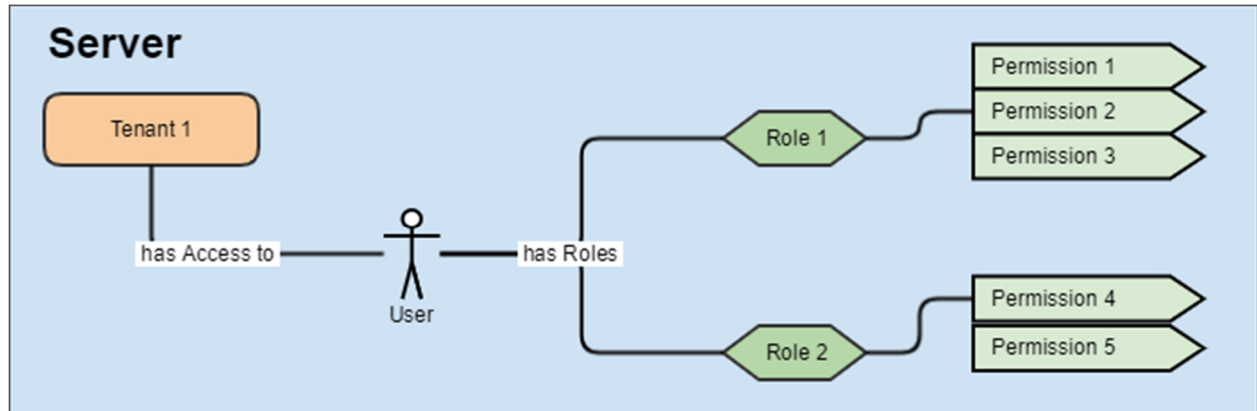
File system data is protected by operating system access control.

It is recommended to use encrypted disk volumes on operating system level to protect the data against direct reading of the disk in another computer system.

3 User Management and Authentication

3.1 User Management

3.1.1 Overview



The server platform provides a user management, which allows the management of multiple users with different roles and permissions.

Users have an ID, a name and an email address. It is possible to define as many users as needed.

A user has to be assigned to a tenant to grant basic access to the tenant.

After that you may grant other authorizations using roles, which are collections of permissions.

A user may be assigned to multiple roles. A user without at least one role does not have any permissions.

Users can change their own password as long as they are authenticated, and send the old password with the change request.

3.1.2 Roles and Permissions

3.1.2.1 Permissions

A permission grants access to a server REST API call which contains the HTTP method (GET, PUT, POST, DELETE).

The HTTP method determines the access mode: create, read, update and delete access on REST resources.

3.1.2.2 Roles

Roles must be assigned to users to grant them permissions.

Users cannot get permissions directly, they get them via assigned roles.

Roles are business case driven sets of permissions to allow requests.

A user can have many roles. The full set of permissions of a user is the set of all permissions of all roles that are assigned to a user.

3.1.3 Business Units

Business units separate data for organizational entities (stores, countries, regions) in terms of configuration, master data and transactional data.

To work with a given business unit, you need to grant the business unit permission to the user. Otherwise the user is not able to perform any use case on the business unit.

3.2 Authentication

Authentication against the REST API (and thus for web client login) is done with **HTTP digest authentication** (RFC 7616). Every request must be authenticated with a user and password with digest authentication.

The web client uses the credentials to communicate with the server backend REST API.

If the web client requests a REST call against a resource without permission, a server error with HTTP status 401 "Unauthorized" occurs.

3.2.1 Password Policy

3.2.1.1 Passwords Management

Passwords should be strong. There is an indicator (green, yellow, red) for the password strength in the credentials dialog.

Rules for a strong password are hard-coded:

- At least 8 characters
- At least one uppercase character
- At least one digit
- At least one special character such as %\$?-()

The image shows three instances of the 'Reset Password' dialog box, each with a different password strength indicator. The first dialog shows a green bar, indicating a strong password. The second dialog shows a yellow bar, indicating a medium strength password. The third dialog shows a red bar, indicating a weak password. Each dialog has fields for 'password*' and 'confirm password*', a 'show password' checkbox, and a 'Password Strength' indicator. A tip at the bottom of each dialog reads: 'Tip: Use at least 8 characters, as well as letters, numbers, and special characters.' The buttons 'CANCEL' and 'CREATE' are visible at the bottom of each dialog.

3.2.2 Default User

In both cloud and on-premises scenario, the system creates a default user: admin.

The default administrator is a special user with extended capabilities.

- The requests of the admin user are not checked against permissions, this means that this user has all permissions on all resources.
- This user could change other user passwords without knowledge of the old one.
- It has access to all tenants by default.
- The admin user cannot be deleted.

Aside from that user, it is possible to create other administrator users with customized access rights. These administrators do not have the special capabilities of the default administrator.

3.2.2.1 Cloud Scenario

In the cloud environment there is an initial user called: admin.

The **initial password** for the admin user has to be provided in the container startup (environment variable).

Make sure you pass a strong password for the admin user. If you do not pass a custom password, the system uses the insecure default password: admin.

3.2.2.2 On-Premises Scenario

In the on-premises scenario, the default platform creates a default user "admin" with password "admin".

 This password has to be changed immediately after first login!

3.2.3 Security of Storage

We store:

1. Roles, users and credentials
2. Database connection credentials

3.2.3.1 Cloud Scenario

Type of Data	Location	Encryption
Roles, users and credentials	database	<ul style="list-style-type: none">• The password is stored as part of digest authentication with an MD5 one-way hash.• All data is stored in an XML blob that is encrypted using AES-192 (GCM)
Database connection credentials	file system	<ul style="list-style-type: none">• XML file<ul style="list-style-type: none">◦ Password is stored in XML file using RSA/None/OAEPWITHSHA-512ANDMGF1PADDING (8192 Bit key)• Server private key:<ul style="list-style-type: none">◦ RSA-Key - 8192 Bit - 2^80 Prime-Strength◦ PKCS8EncodedKeySpec <p>Server provides a resource for public key to allow REST API users to encrypt the passwords before sending them to the server.</p> <ul style="list-style-type: none">• RSA-Key - 8192 Bit - 2^80 Prime-Strength• Base64-PEM

3.2.3.2 On-Premises Scenario

Type of Data	Location	Encryption
Roles, Users and Credentials	file system	<ul style="list-style-type: none">• The password is stored as part of digest authentication with an MD5 one-way hash.
Database Connection credentials	file system	<ul style="list-style-type: none">• XML file<ul style="list-style-type: none">◦ Password is stored in XML file using RSA/None/OAEPWITHSHA-512ANDMGF1PADDING (8192 Bit key)• Server private key:<ul style="list-style-type: none">◦ RSA-Key - 8192 Bit - 2^80 Prime-Strength◦ PKCS8EncodedKeySpec <p>Server provides a resource for public key to allow REST API users to encrypt the passwords before sending them to the server.</p> <ul style="list-style-type: none">• RSA-Key - 8192 Bit - 2^80 Prime-Strength• Base64-PEM

3.3 Database User Management

The server needs a database connection with credentials to connect to the database.

 Please refer to the database user manual on how to create database users. Make sure to use strong passwords for the database users.

4 Key Management

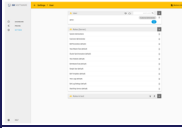
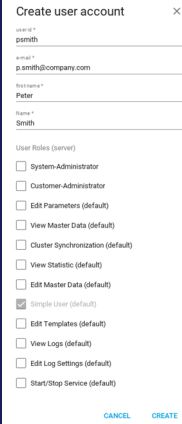

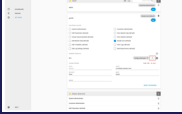
Key	Location	Type
Database password public encryption key	client, requested from server via REST	RSA Public Key - 8192 Bit
Database password private decryption key	server	RSA Private Key - 8192 Bit
Configuration encryption key	server	AES-192

5 Administration Users in the Web Client

5.1 Authentication Options

The user management in the web client allows one to:

- List users and roles
- Create users
- Set/change the password
- Assign user to tenant
- Add roles to user
- Create roles
- Add permissions to roles

Step	Path to screen	Screens	Description
List users and roles	Settings → User		Contains: <ul style="list-style-type: none"> Add user button Add role button
Create user	Settings → Users panel → Add user button [+]		
Set/Change password	Settings → Users → Edit User → Change Password		
Link user to tenant	Settings → Users panel → View user → Add tenant to user (+)		Contains: <ul style="list-style-type: none"> Add tenant to user button
Create role	Settings → Roles panel → Add role button [+]		
Link role to user	Settings → Users panel → View user → Add role to user (+)		Contains: <ul style="list-style-type: none"> Add role to user button
Add permissions to roles	Settings → Roles panel → View role		Contains: <ul style="list-style-type: none"> Add permission checkboxes

6 Network Security

6.1 HTTP/HTTPS

The server runs as web application in an Apache Tomcat which provides the network communication.

There are two options to set up HTTPS:

1. Configure HTTPS in the application's Tomcat server
2. Configure HTTPS in a proxy server

We recommend option 2. In some cloud environments, this option is pre-configured out of the box or can be easily configured.

7 Alerting

7.1 Security Alert Stream

Security issues are tracked in the log stream and marked with a special component name and pattern to filter them in a dashboard.

Tracked issues are:

Type	Reason
Failed authentication	In case of a request without correct credentials. <ul style="list-style-type: none">• Non-existent user• Wrong password for existing user
Unauthorized access	An authenticated user accessed a resource without the necessary permissions.

CONTACT

GK Software SE
Waldstraße 7
08261 Schöneck
Germany

T +49 (0) 3 74 64 84 – 0

F +49 (0) 3 74 64 84 – 15

documentation@gk-software.com

www.gk-software.com