amadeus

Amadeus Hospitality - APMA

User manual

amadeus

Table of Contents

amadeus

Document control

Security level	Public			
Company	Amadeus Hospitality Netherlands B.V.			
Department	Amadeus Hospitality – InMarket PMS (Property Management Systems)			
Author	Jan-willem VAN KAMPEN, Jeroen VAN DIJK			
Reviewed by	Jan-willem VAN KAMPEN		Date	2024-11-20
Approved by	Jeroen VAN DIJK		Date	2021-02-15
Version	Date	Change	Comment	By
1.0	2020-11-11	Initial version		JWvK
1.1	2021-02-15	Added, * APMA & IDPMS Differences * User management		JvD
1.2	2024-11-20	Reviewed user management section(s)		JWvK

amadeus

System requirements

Amadeus Property Management – Advanced (APMA) is cloud based and has various components which you as a customer can utilize. We've outlined some requirements which will help you get the best experience possible when using our product.

Portal access

For access to the APMA (web)portal users will need an internet connection and a browser on a Windows PC, Mac, Chromebook, tablet or mobile device. A mobile device is also needed for the Duo Authentication (2-factor provider) that is required.

Any of the most common browsers (Microsoft Edge, Google Chrome, Mozilla Firefox) will work.

FullPMS access

FullPMS access requires a (Microsoft Windows or Mac) device capable of running a Remote Desktop Protocol (RDP) session. Minimal Requirements are a high-speed internet connection and a minimum screen resolution of 1280 x 1024.

OS Support

The recommended Remote Desktop application is Microsoft Remote Desktop. It can be found on the following operating systems:

- Windows, no known issues exist with the Windows remote desktop application, the minimum Windows version is Windows10
- Chrome OS, Chromebooks can run the Remote Desktop client but due to limitations in the Remote Desktop application for Chrome OS it will not be possible to print and errors might occur in the FullPMS when creating reports and confirmations.
- Android, Android devices can run the Remote Desktop client but due to limitations in the Remote Desktop application for Android it will not be possible to print, and errors might occur in the FullPMS when creating reports and confirmations.
- MacOS (Apple), no known issues exist with the MacOS remote desktop application

Windows OS client recommendations

Microsoft has been changing the behavior of RDP and RemoteApp connectivity in the last Windows versions. Not all these changes are in favor for secure operations and the overall user experience when using these technics. Both desktop and server

versions of Windows are affected and are now more actively caching user credentials used for connectivity on the RDP client's user session.

Amadeus is aware that sometimes properties use shared workstations, specially at front office positions this could lead into issues when switching APMA users on the FullPMS option. As the last user's credentials are then cached and used to (re-) connect to APMA. This results in starting an APMA session without proper login prompt and the new user working under its predecessor's user code and authorization.

This is inconvenient for the user, but also poses a security risk.

GPO rules advised for mitigation,

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client

- Allow .rdp files from valid publishers and user's default .rdp settings
  - Enabled
- Do not allow passwords to be saved
  - Enabled
- Specify SHA1 thumbprints of certificates representing trusted .rdp publishers
  - F092BC7EF311F18CED156FF2B52A4D51D039C15A
    (changes in thumbprint will be published on the APMA product site)

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host

- Automatic reconnection
  - Disable

Computer Configuration > Administrative Templates > System > Credentials Delegation

- Allow delegating saved credentials
  - Disabled
- Allow delegating saved credentials with NTLM-only server authentication
  - Disabled

Caveat

Please note that the APMA FullPMS is intended for desktop use with mouse and key-board, therefore the experience on touch-only devices might not be optimal.

Amadeus IoT – Gateway (f.k.a OrangeBox)

As a hotelier you'd likely have multiple supporting systems like keycard management, pay-tv or phone systems. The APMA product offers the Amadeus IoT – Gateway solution for any on-premise system which needs to connect to our APMA cloud product.

For these specific hotel system integrations that are working within your hotels local network or rely on a serial (RS232) connection a IoT - Gateway needs to be obtained. This physical device will handle connections between on-premise based systems and APMA.

amadeus

User management

Amadeus takes security very seriously and works hard to protect customer data. We are constantly striving for improvement and work to protect your data in a safe, secure and high-availability manner consistent with industry standards and best practice.

Amadeus provides each user with a unique username and password and will enforce further levels of user security based on the user's role and permissions like a additional 2-factor authentication requirement upon login.

User credentials

Secret passwords are the primary means of protecting our application. This document establishes the minimum requirements for passwords and protecting them from being compromised.

Password construction

The construction of passwords is a balance between something simple enough to remember the password without having to write it down and difficult enough so that only you know it. To ensure that passwords meet minimum requirements the following standards must be followed. Regardless of the technical capabilities or features of the system, each user is responsible for complying with each of the password standards, as long as it is technically possible to do so.

- Passwords must be difficult to guess
- Passwords must have at least eight (8) characters
- Passwords must be alphanumeric containing at least one numeric and alphabetic character. Where technically possible passwords should contain special characters
- Passwords must not contain the User-ID's name or parts of it
- Blank or null passwords are not allowed
- Words in a dictionary, a derivative of the user-ID, and common character sequences such as "12345678" or repeating characters "AAAAAAAA" must not be employed
- Personal details such as spouse's name, license plate, social security number, any government issued identification number, and birthday must not be used
- User-chosen passwords, passphrase must not be any part of speech or any language including slang, dialect, jargon or foreign. This includes but is not limited to proper names, geographical locations, common acronyms or buzzwords
- Passwords must not be constructed that are substantially similar to passwords previously utilized

amadeus

Changing passwords

We advise that your passwords must have a limited lifetime. This provides a limited window of opportunity for abuse from the time the password would be compromised (exposed / shared / cracked etc.) to the time the password is changed.

- All users are advised to change their passwords at least once every ninety (90) days
- Amadeus provides users with the opportunity to change their passwords through our (web)portal which is a secure mechanism and enforces these manual and compliance policies
- Your password cannot be changed until at least 1 day since it was last changed. This is to restrict users from cycling through a series of passwords to effectively maintain the same password continuously
- Whenever an unauthorized party has compromised your system or if the password(s) have been disclosed to unauthorized parties, you must inform Amadeus and you must immediately change every password used on the APMA product. Even suspicion of a compromise likewise requires that all passwords be changed immediately. Similarly, under either of these circumstances, all recent changes to the user will be reviewed by Amadeus following our incident response process

Password protection

Passwords must be provided appropriate protections, the APMA systems and the trust relationships are depending on the fact that only the appropriate users will have the password in question. Providing extreme protection for a resource and little protection for a password totals only little protection for the resource.

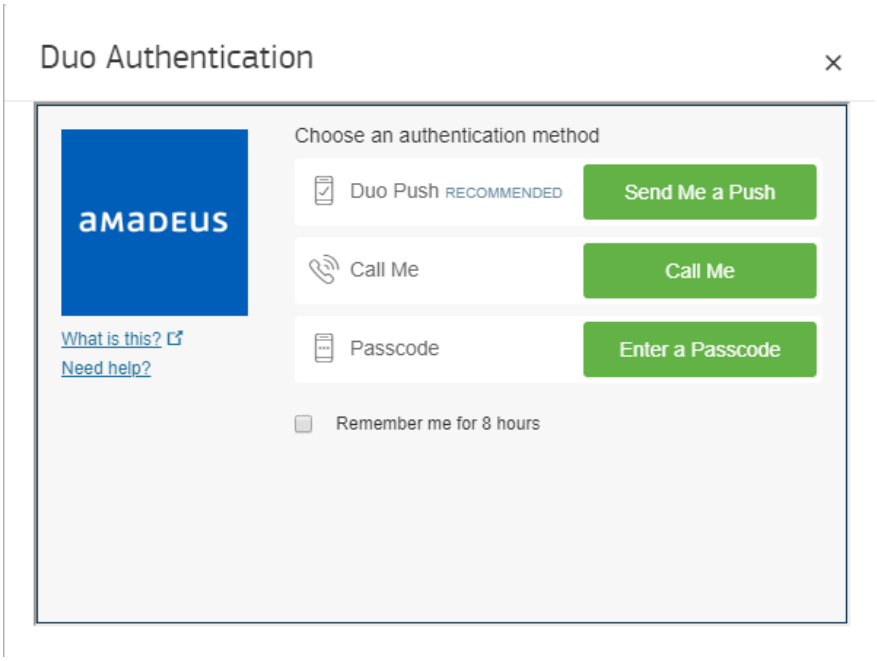
- You as an end user must not share passwords with anyone (that includes management, Amadeus support staff, family members, co-workers or in any form)
- The display and printing of passwords must be masked, suppressed, or otherwise obscured so that nobody will be able to observe or subsequently recover the passwords
- Users must not use the "Remember Password" feature of applications (e.g., Edge, Chrome or Internet Explorer)
- Users must not reveal any password on questionnaires or security forms or in email *(Note: this does not apply to the Amadeus application automation who send "one time passwords" to users in compliance with internal policies and standards.)*
- Amadeus support processes shall not require requesting a user's password for troubleshooting purposes
- Passwords must not be documented (e.g. on, under, around, or near the computer or any of its components), not even temporarily
- Users shall protect their passwords (and other authentication credentials) with extraordinary diligence. This includes, but is not limited to:

- Never leaving hints to the password in unprotected areas (e.g. obscurely hidden text files, smart phone, cloud storage).
- Saving passwords outside the original authentication mechanism only in password vaults using compliant and strong cryptography.
- Changing passwords immediately if there is any suspicion the password could be compromised.

2-Factor authentication

Access to Amadeus Property Management - Advanced (APMA) will be based on your user role and permissions require use of 2-factor authentication using the vendor DUO security. This requires an application to be installed on a smartphone, an installation link will be sent by SMS to the supplied mobile phone number when a new user is created or updated. Please install this application.

After successful verification of username and password, users will be asked to verify their identity via this DUO application on their mobile phone as well. The 2-Factor Authentication request will look similar this,



The options for "Send me a push" and "Enter Passcode" will only be available after installing the DUO-app on the cellular device.

- Send me a push
  - will result in a push message being sent to the cellular device. This push message should be approved to get access
- Call me

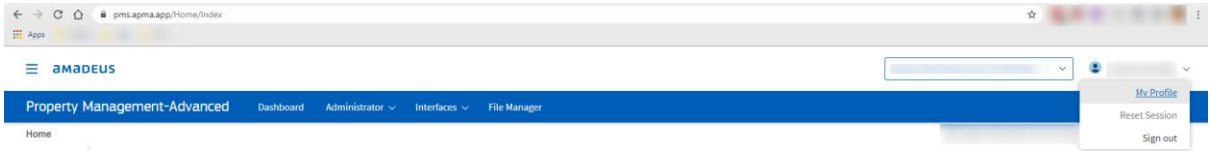
  - an incoming call will be received from DUO to authenticate the user
- Enter a passcode
  - requires entering a passcode that can be found in the DUO app on the cellular device
- Remember me for 12 hours
  - logging in will not require DUO authentication for the designated account for the next 12 hours. After that period has expired authentication will be needed again.

This 2-factor authentication applies to the APMA (web)portal based on the user's role and permissions. Apart from starting the FullPMS (RemoteApp) connection, in this case all users will have to use 2-factor authentication.

To avoid front office employees, as example your lobby receptionist to have to use their mobile phone each time, we allow every customer (hotel property) in case they have a internal network with a static external IP to supply us with this IP-address as a form of 2-factor authentication for the user.

Resent DUO Security activation

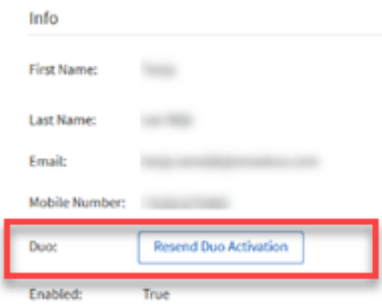
When logged into the APMA (web)portal, you can navigate using the top bar menu to see and manage your own user profile.



This page will give you the option to resent an activation for DUO Security, our 2-factor authentication provider.

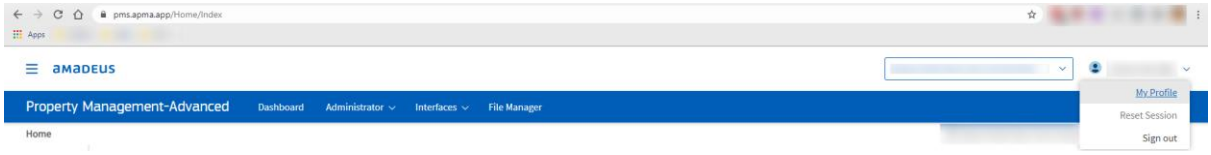
It will "reset" your DUO mobile device registration, when the previous DUO registration link has expired or when you get a new phone for. You can resend the DUO activation message by clicking on the resend DUO activation button.

Please note this resent option will not work when you have a new phone and a new phone number. In that use-case please change the Mobile Number on the same page and save your profile, this will trigger the actions to (re-)register your new device and number in our systems.

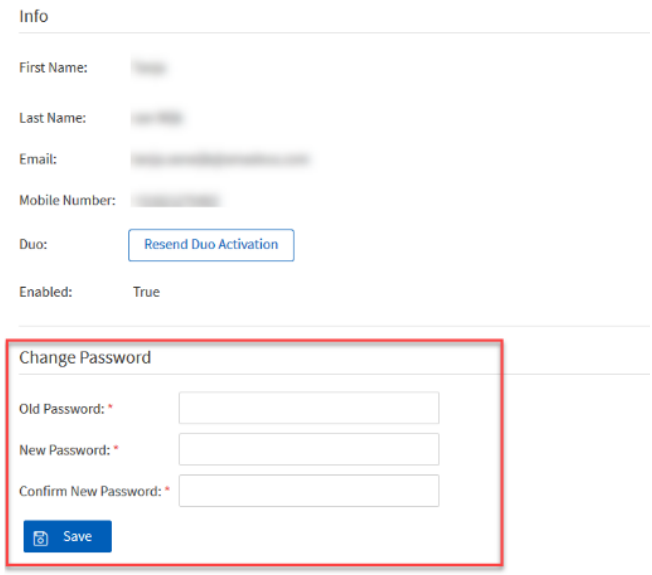


Change password function

When logged into the APMA (web)portal, you can navigate using the top bar menu to see and manage your own user profile.

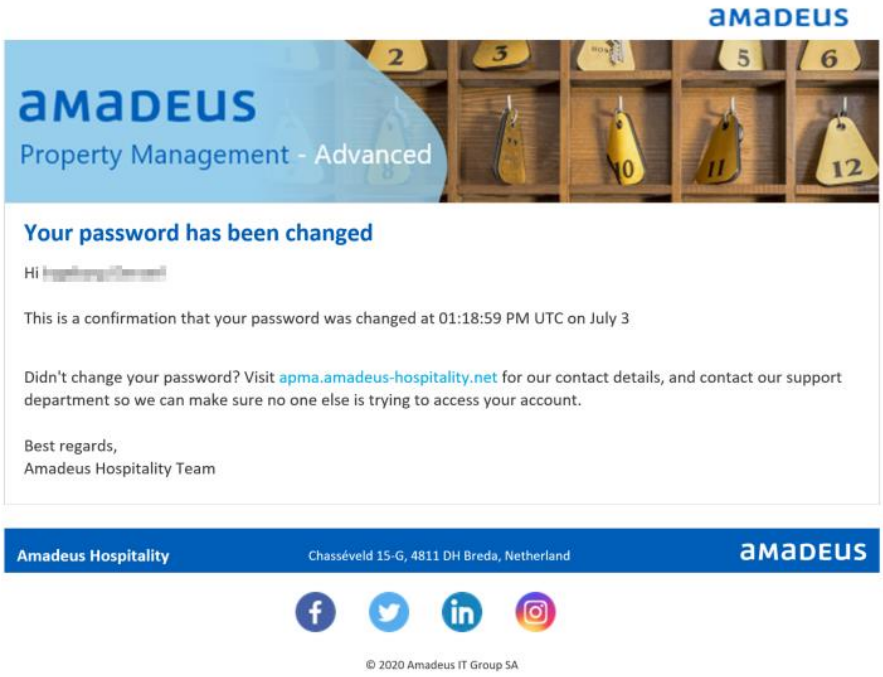


This page will give you the option to change your current password.



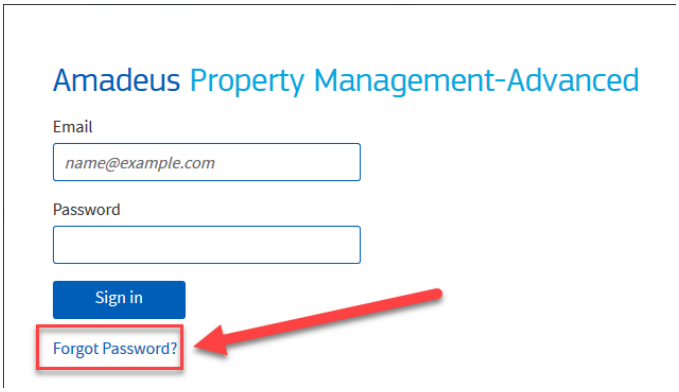
The new password must comply with the password policy, shown when typing a new password. When clicking on save, the new password is saved, and you will be logged out so that you can log in with your new password on the APMA (web)portal.

When the password is successfully changed an email will be received that your password has been changed.

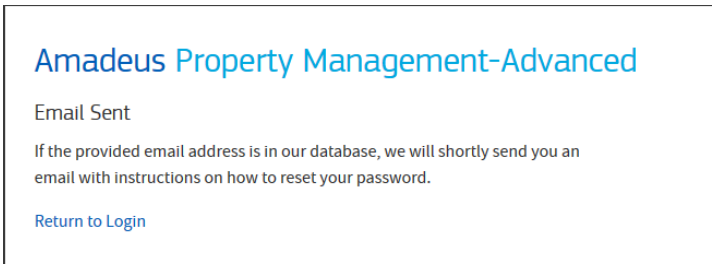


Forgot password function

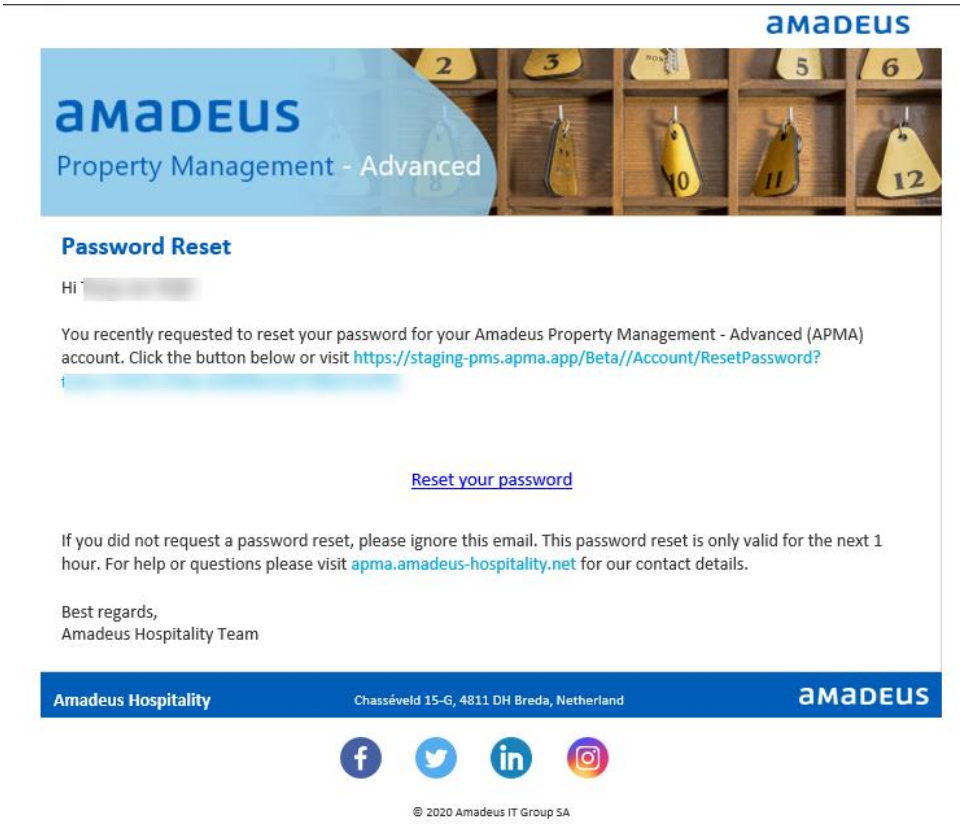
When you do not remember your password anymore or you are locked, you can click on “Forgot Password?” on the (web)portal login screen to set a new password.



1. Fill in your email and click on "send"
2. The message below will appear on your screen. The entered email if you have an existing user account for APMA you will receive an instruction email on how to continue to recover your password.



3. Follow the instructions in the email and click on the "Reset your Password" link



4. Enter the new password and click "Send". The password needs to comply with the same password requirements as if you would change via "Change Password"
5. When successful you will get a DUO message on your phone to verify the change, and you will see the below. Login with your new password and you will receive an email that the password has been updated.

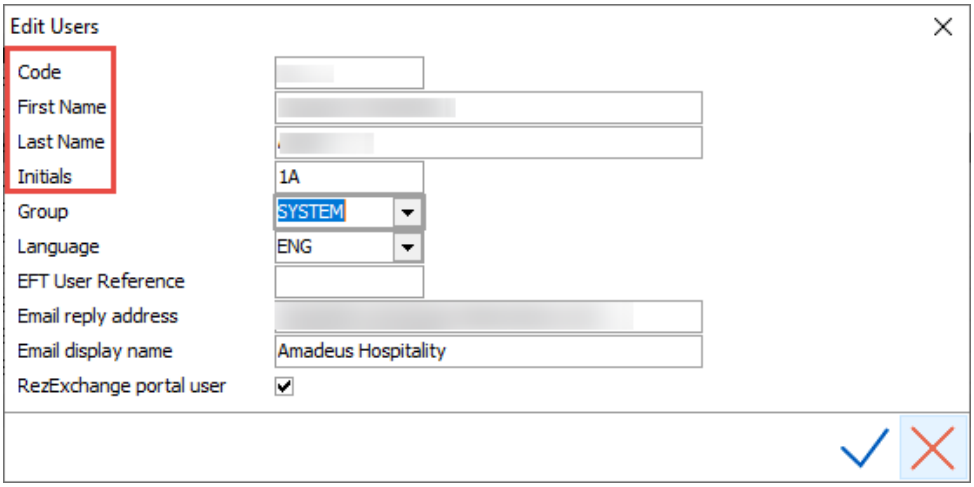
Differences between APMA FullPMS and IDPMS products

The FullPMS option delivered through RemoteApp functionality within the Amadeus Property Management – Advanced (APMA) product line is based on a modified version of Amadeus Property Management – IDPMS product typically run on-premises by the customers themselves.

There are, however, a few differences as working in the cloud brings some advantages and due to Amadeus PCI-DSS compliance also some constraints. Therefor when switching from on-premise IDPMS to our APMA cloud product functionalities may work differently.

User management

It is not possible to create or modify users directly within the FullPMS option, this must be done through the APMA (web)portal. User profiles are accessible in APMA FullPMS, but the fields for user code, first name, last name and initials are read-only.



User groups, shifts and (FullPMS-) permissions can still be managed from APMA FullPMS.

Sending emails

Please note that it is not possible to connect directly from APMA FullPMS to Microsoft Outlook. Any installations of Outlook will be on your local workstation, outside of the APMA product environment. All emails from APMA FullPMS must be send using your email providers SMTP server.

To be able to send emails from APMA FullPMS, an email account with SMTP server needs to be created (for example Microsoft Office365) using an access token or none

2-factor protected SMTP account. As APMA FullPMS will be unable to process 2-factor authentication requests.

File storage

APMA product and its FullPMS option uses only Microsoft Azure "Blob" storage for storing custom reports and exports of various types, instead of a local (network-)folder.

The functionality to upload files to Blob storage is incorporated in the save button on various forms within APMA FullPMS. This also means that it is not possible to directly access your saved files from your local workstation. Files can however be downloaded through the APMA (web)portal.

Settings > Options menu

Within IDPMS it was possible to configure your own file paths using the “Settings > Options > General” menu path in the PMS. On APMA FullPMS this is not possible as these are managed by the APMA (web)portal combined by not having local storage anymore.

Please see “File storage” section for more details.

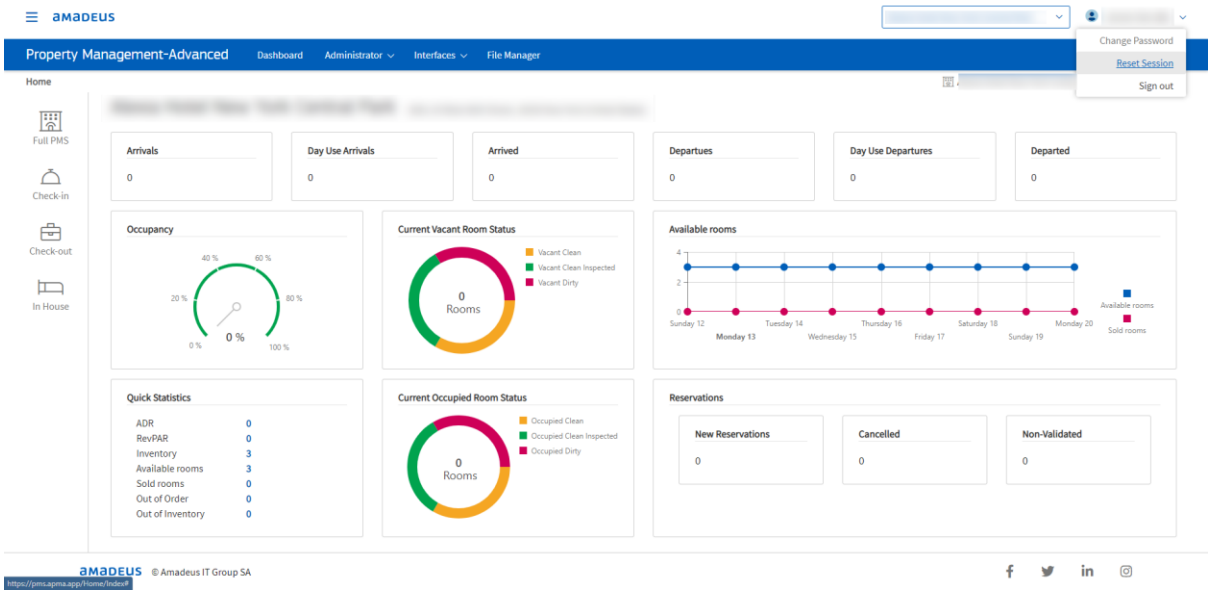
Frequently Asked Questions

Collection of frequently asked questions or problems which can be resolved using the APMA (web)portal as a type of self-service option. In case you have further questions, you can contact your account manager or our support team.

Reset a frozen FullPMS user session

In case a FullPMS user session is frozen, gets stuck or when a user is unable to login to the PMS, please take the following steps:

1. User should log into the APMA-portal and click on "Reset Session" under his/her name. The portal should provide an acknowledgement of the reset and the PMS session should be logged off.



2. The user should start the PMS again
3. When the reset is failed, please contact Amadeus Support and ask for a session reset