amadeus

APMA System Requirements

Index

General

Portal access

For access to the APMA 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 Autentication that is required.

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

PMS access

PMS access requires a (Microsoft Windows) device capable of running a Remote Desktop 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. 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 PMS 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 PMS when creating reports and confirmations.

MacOS (Apple)

No known issues exist with the MacOS remote desktop application

iOS (Apple)

iOS devices can run the Remote Desktop client but due to limitations in the Remote Desktop application for iOS it will not be possible to print, and errors might occur in the PMS when creating reports and confirmations.

Caveats:

Please also note that the APMA PMS is intended for use with mouse and keyboard, therefor the experience on touch-only devices might not be optimal.

Orange Box

For specific hotel interfaces that are working within the hotel network or rely on a serial connection, an Orange Box needs to be obtained. The Orange Box will handle connections between Hotel based systems and APMA.

Multi Factor Authentication

For Multi Factor Authentication a mobile phone number per user is needed.

E-Mail

To be able to send mails from the PMS a mail account with SMTP server (and credentials) are needed (for example Microsoft Office365).

As the PMS will be unable to process 2-Factor Authentication this option will have to be disabled in the mail account. Alternatively, an App-Password can sometimes be set in the mail account. For more information on how to do this in Office365, use this link.

Firewall

Please note that all outbound network and internet connections will be blocked (e.g. SMTP-mailing) unless the designated ports are opened in the firewall.

APMA Client recommendations

Microsoft has been changing the behaviour of RDP and RemoteApp connectivity in the last Windows versions. Not all these changes are in favour for secure operating 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 client's user session.

We are aware that sometimes properties use shared workstation specially at front office positions this could lead into issues when switching APMA users on the "Full PMS" option. As the last user's credentials are then cached and used to (re-)connect to APMA. Resulting in starting an APMA session without proper login prompt and the new user working under its predecessor's user code and authorisation.

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

GPO rules advised;

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