Door Tablet Security
Features to Keep your Business Safe

DOOR TABLET

The Importance of a Secure System

When choosing a workspace management system, you may not have considered whether or not it is secure.

However, once security becomes an issue for you, it is probably already too late - your system has been hacked, sensitive information stolen, or data is being held to ransom and you now face a world of pain and recriminations…

A booking system that can be hacked is a potential commercial disaster for any company - don't risk it.

We built the Door Tablet system with comprehensive security features in mind, not as a mere afterthought. Enhanced security elements have always been integrated into our software and our purpose-built hardware. We are proud that a wide variety of data-sensitive companies around the world trust Door Tablet.

Summary of Security Features
- Runs on your premises or in your private cloud - you have complete security control of your system
- Administrator-controlled security features:
  - Booking security/privileges
  - Room and meeting security for entry
  - Meeting confidentiality
- Hardware security features:
  - No on-device password storage
  - Single purpose device
  - Hard to steal
  - Hardened hardware available "out of the box" for maximum security settings

Maximum System Security

Door Tablet runs on your premises or in your private cloud, so you have complete security control of your system. Door Tablet ensures that no one has any access to your data at all.

You always have full control of the Door Tablet system. It runs solely on your infrastructure and/or your cloud. Door Tablet will never be a "weak link" within your software ecosystem.

Room Security

The Door Tablet system alerts the room booker when uninvited users check into a room. If door unlocking is enabled, Door Tablet can physically restrict room entry depending on authentication. We supply a General Purpose Input Output (GPIO) Device that works with your own existing magnetic door locking mechanism. Rooms can then be simply unlocked by PIN passcode or RFID/ NFC.

End-user Security

Door Tablet offers different levels of authentication and authorizations for users. Security restrictions can be applied at:
- System level
- Device level – individual rooms or groups of rooms

You decide what functions are enabled for different rooms. For example, you may want to block a specific touchscreen from being used to book rooms unless the user is authorized.

Different users can be allocated different booking privileges via PIN numbers or RFID/NFC.

You decide which rooms are available, at what time and where these rooms may be booked – from the booking system, or solely on the touchscreens outside the room.

Hardware Security

Door Tablet runs opaque on the network - by default our devices do not respond to any information other than the Door Tablet server.

No on-device credentials storage

Our software does not store usernames or passwords on devices – so if they are stolen, they cannot be used to inflict harm on the organization. All information is stored solely on the Door Tablet server - not any end-points. We recommend selecting our robust, purpose-built displays to take advantage of their extended security features.

Single purpose device

Since all our devices are purpose-built to be used only with Door Tablet, they have no value to the casual thief. Unlike an iPad or Samsung Galaxy tablet, our devices do not have resale value and are not a temptation for dishonest people.

Hard to remove

Even if someone is tempted, our devices are hard to steal because secure wall mounts and 3M stick tack makes them nearly impossible to remove.

Security-hardened hardware

We offer "hardened" versions of our devices that are classified to handle a Rogue Admin. This applies to the Door Tablet AIO, TC and SL.

Hardened devices are built so that no one can gain physical access to them via ports or interfaces, which is especially important for banks and security conscious organizations. This hardening of the units ensures no sensitive eavesdropping devices or other malware can be installed on our devices. Like all our Door Tablet products, our hardened devices work "out of the box".

Administrator Security

Administrators have full control of the Door Tablet system and can finetune the levels of security and authorizations. They can enable/disable security features as needed, including booking and meeting information security.

Confidentiality

Sometimes you may not want visitors or employees to know who is coming to a meeting or what a meeting is about. Administrators are in complete control of what information the system will show on display devices.

All Door Tablet layouts are fully customizable which means that you can decide how much detail you want to give about what may be happening in that room. This discretion can also be applied to all our Wayfinding services.

Server Stability and Fail-safes

As well as being a secure environment, Door Tablet has robust system durability.

By taking advantage of multiple servers, the Door Tablet servers can replicate each other, providing powerful redundancy. If one server goes down, all the endpoints notice and they automatically switch to an alternate server, maintaining seamless functionality. After this event, the system will try to revert back to the original server, at 10 minute intervals, to maintain load balancing.

DOOR TABLET