TimeDock hardware security

Last updated - Jul 12, 2022, at 11:37AM

Web:	https://timedock.com
Email:	info@timedock.com
International:	(+64) 9 444 1384
Local phone:	(09) 444 1384

Table of Contents

Overview 3
Internet traffic requirements 4
URL Allow List 5
Software updates 6
Threat mitigation 7
Lifespan 10

Overview

TimeDock's time clock appliances are assembled from Android-based hardware, sourced and customised from a professional OEM provider of electronic and computer-related technologies since 2002.

Our devices are single-purpose, designed as time clocks and nothing more. This significantly reduces, or almost eliminates, the possibility of introducing malware or other malicious exploits as there are little to no attack vectors for exploitation. Staff cannot load or use other apps, browse the internet, or use it as a regular device. Additionally, the system settings are not easily accessible without a master key or knowledge of how to access it via a hidden series of taps on the screen (designed for quick support over the phone, where couriering a new master key would not be considered timely enough for business-critical changes to the settings).

Internet traffic requirements

The appliance requires outbound access to TimeDock's SSL-secured API endpoints (currently at https://secure.timedock.com) and ideally a Microsoft service for crash logs (refer URL's below) as well as several other URL's for purposes of enhancing the experience.

No remote or inbound access is required for the devices to function, and all inbound traffic can be blocked.

Outbound traffic can be firewalled to allow only the above-mentioned domains and can be obtained via standard Wi-Fi connection or in many instances a Data SIM card, IoT SIM card, or Global IoT SIM card.

Refer to the section URL Allow List for more information.

URL Allow List

The following URL's require outbound traffic.

- secure.timedock.com

  Required for direct communication with TimeDock API's and services.

The following URL's are optional, but recommended for enhancing the functionality of the appliance.

- *.servicebus.windows.net

  Required for push notification functionality, allowing enhanced real-time downstream synchronisation of TimeDock data.

- (Google Cloud Messaging)

  Required for receiving push notifications, which enhance the real-time downstream data synchronisation of TimeDock data.
  https://firebase.google.com/docs/cloud-messaging/concept-options#messaging-ports-and-your-firewall

- *.appspot.com
- *.apps.googleusercontent.com
- *.firebaseio.com

  (All three above). Related to Google Cloud Messaging, for push notifications registration, sending and receiving.

- api.appcenter.ms
- api.mobile.azure.com
- *.appcenter.ms For error logging & crash reporting:

  (All three above). Reports anonymous crash and exception logs that we can use to identify and troubleshoot issues with our application/s on the appliance.

Software updates

The time clock application software, i.e., the primary interface of the device, periodically checks the secure API endpoints for latest versions and installs them automatically. Again, no inbound access is required for this.

The underlying Android operating system cannot be remote-updated, and includes the following modifications:

- Default launcher / home application removed.
- Modified system APK to hide the status bar.
- Custom TimeDock application, and custom launcher, installed as system apps.

Threat mitigation

Here is a list of common security concerns, and our suggested mitigation, minimisation, or elimination.

Potential threat	Suggested action / Remarks	Final severity
Malware Software designed to disrupt, damage or gain unauthorised access may find its way on to the device.	**1.** No client applications besides TimeDock are accessible or installed (i.e., employees have no access to browse the internet, watch videos, open documents or emails, etc.). **2.** Do not sideload other applications for employee use. **3.** Ensure developer mode is turned off. **4.** Do not leave Master Key, for accessing system settings, within reach of public/employees. **5.** Use security-mount to inhibit easy removal from location (i.e., so that staff don't take it home).	**Negligible / Avoidable.** Inbound firewall rules protect the network against incoming traffic or other network segments, namely disallowed connections, malware, or denial-of-service (DoS) attacks. Properly DMZ'd and Firewalled, only deliberate physical access by someone intent on causing harm could load malicious software on to the device.
Remote attacks Network vulnerabilities could allow remote attackers to penetrate the device.	Use a Firewall and DMZ to restrict all incoming traffic from local and wide area networks and isolate from the organisation's private network.	**Avoidable.** Adequately configured, this threat should be eliminated almost entirely (subject to the effectiveness of the organisation's networking security).
Man in the middle attacks Malicious applications or attackers on the organisation's network, or spoofing the network, may intercept communications between the device, and our secured servers.	**1.** All communication uses 256-bit SSL, one of the most secure encryption methods to protect against data being stolen, modified or spoofed. It is the same level of encryption used by online banking, among other high-security transactional applications connected to the internet. **2.** TimeDock application software uses at least TLS 1.2 for transport level security.	**Avoidable.** SSL is a widely implemented and robust standard of security adopted by most internet-connected applications.
Physical access The appliance could be	**1.** Only a shallow copy of data is stored locally (i.e., a list of employee names, and their most recent time	**Negligible / Low impact.** There is little motivation for

removed and exploited directly via physical access. i.e., the data wiped.	entries or unsynchronised entries that have yet to be persisted on our secure servers). **2.** A data wipe or factory reset of the device would not delete or otherwise affect any time entries already persisted to our secure data storage, hosted and maintained by Microsoft within their high-security Microsoft Azure data centers. **3.** Use included wall-mounting bracket with pin torx security screws. **4.** Place in vicinity of security cameras, or common-access areas with high visibility and restricted public access (i.e., in a corporate office or the hallway near a manager's office, not in the public foyer).	theft of the device, or targeted physical exploitation. Refer to the suggested actions and remarks to minimise the threat. In the event that a device became compromised, there is minimal information stored on the device that would be of little use to an attacker.
Data corruption A targeted exploit might corrupt or spoof data or device actions to interfere or falsify time records.	**1.** Mitigating the above points, the threat of a targeted exploit is very low. **2.** Data already persisted on our secure servers cannot be permanently deleted, or irreversibly changed, via our API or any devices connected to it. Whilst data could in theory be "soft-deleted" by a reverse-engineered and recompiled TimeDock application (difficult / very low risk of someone knowledgeable doing this), we can block further exploitation and reverse the changes. Only under specific instruction by an approved organisation representative, and manual intervention by our senior engineers, can permanently deform time entries beyond the point of recognition. That excludes read-only backups, which remain securely archived within Azure data centers as a persisted snapshot for up to 12 months. **3.** We utilise Microsoft Azure's point-in-time live database replication, as well as sequential and incremental backups, to ensure high-level data recoverability in the event of signification loss or corruption.	**Highly unlikely / Low impact.** Highly unlikely and can in most cases be intercepted and remedied. ***Note: the hardware devices themselves do not store any more data than they need, to operate on a day-to-day capacity. All organisational data is persisted in secure data centers managed by Microsoft.***

Exposure to organisational private network	**1.** Implement a DMZ (demilitarised zone) on organisational networks, to isolate the appliance from the rest of the network. **2.** Consider using a separate internet connection, for example an IoT SIM Card designed for low-bandwidth appliances.	**Avoidable.**

Lifespan

Due to the nature of digital computers, we recommend replacing hardware *every five years* to ensure continued improvements of the underlying hardware, system architecture, security certificates and front-end applications that may not be self-updateable.

For this reason, we have priced all hardware as commodity consumer devices at near cost, and we rely solely on the subscription / licensing of the platform to cover our operating expenditures such as ongoing support, improvements, maintenance, etc.