SIMPLIFY TIME TRACKING WITH

TIMEDOCK™

An intuitively simple to use ID-badge time tracking system, for your phone.

http://timedock.com | Phone (09) 444 1384

Scan in with barcode ID's or Near Field (NFC)

Exceptionally simple-to-use mobile time tracking, without all the fiddly buttons associated with other mobile apps.

By using our web-based system TimeDock, with apps for iOS and Android, field-based organisations significantly improved accuracy of staff hours, and decreased administration by up to 60%.

- ✓ Fast - 0.1 seconds per scan
- ✓ Scalable - Any number of staff
- ✓ Convenient - View hrs online
- ✓ Portable - Use your phone/s
- ✓ Affordable - No big overheads

How it works

Managers swipe or tap employee ID badges to their phone as they arrive to site. Simple as that!

$5 per employee per month. No initial outlay.

Phone (09) 444 1384

International : +64 9 444 1394

http://timedock.com | Mon-Fri 9am to 5pm NZT

Contents

About TIMEDOCK

TIMEDOCK is a web-based timesheet system with a 'traditional' swipe-card user interface.

We offer an exceptionally simple-to-use mobile *and* fixed-device experience for time-keeping, without all the fiddly buttons and select-boxes of common mobile apps and systems.

By using our cloud-based service, in conjunction with our finely-tuned apps and devices, organisations benefit from improved accuracy in staff hours, increased intelligence with real-time reporting and managed support, updates and infrastructure, and less user overhead than any other mobile time keeping service*****.

Swipe-cards, or 'badges', can be in the form of one or more of the following:

QR Barcode

Staff ID cards with a QR Barcode can be printed on-the-spot and used immediately****** from any QR-reading app or device.

NFC cards / badges

Contactless cards and badges can be used in conjunction with NFC-enabled Android devices, and any other supported App/Device. Badges can be purchased blank or pre-programmed via the TIMEDOCK web portal.

Using a card/badge-based system offers significantly increased usability compared to other *mobile time keeping apps* that employ more cumbersome methods of time capture such as pin/password entry or manually selecting from a list of employees.

Using a card-based interface with our iPhone and Android app, it is very realistic to expect each team leader to clock in dozens of staff in under a minute, at any location.

For a 14-day trial visit http://timedock.com/signup

***** based on a selection of 'apps' and 'systems' available at the time; and also depending on other factors such as implementation, industry, staff etc. All in all our aim is to provide the most streamlined time-keeping system for our intended field-based niche. We realise that there are others out there equally as great (and more feature-rich), but we strongly believe our system to be of great advantage to the field-service niche who require high accessibility, scalability, portability and simplicity.

****** devices and apps often require a short period, usually 5 – 60 minutes, to update information with the server before they can begin swiping in on the device. Many apps/devices such as TIMEDOCK for Android utilise push notifications –a technology that allows us to 'push' out the new employee/swipe-card information to connected devices almost instantly.

Architecture / Interface

Cloud-based 'Software as a Service' (S.A.A.S.) model, with supporting client applications and devices:

TIMEDOCK is primarily a cloud-based system -meaning it is running on a web server connected to the internet- and exposes functionality through various interfaces which can be 'docked' simultaneously to TIMEDOCK in any number of configurations.

In essence: Apps and Devices act as data-capture terminals for in/out transactions with the TIMEDOCK database and web application serving as the core for collating the data into a useful time-sheet format, ready for review and export to payroll software.

Web Portal

All administration and reporting is done through the web portal. Administrator users may log in to view, amend and manage various aspects of the data such as time-sheets, employees, users, settings and more.

> *For Users:*
> *This means logging in via a web browser, using your email ID and password. Multiple admin users can be configured to access this 'management' area.*
>
> *For IT:*
> *The 'web portal' is architected the same as any common web-application front-end and exposes information via single-factor authentication (user ID & password) with 2048-bit SSL encryption.*
>
> *Roadmap: Future plans include a secondary mobile app purpose-built for advanced team-leader management such as leave request, manual adjustment requests etc. Until such a time, one or more designated Admin users must use the web portal to perform such functions.*

Connected Apps/Devices

Employees' time is accrued via a 'swipe-in/swipe-out' system which is facilitated by one or more connecting applications or devices.

For Mobile

The focus of our apps is to provide a 'time-clock terminal' for which employees can swipe in/out using ID cards/badges. For mobile this generally consists of one or more designated 'team leaders' whom have the app installed and authenticated on their device, and can thereby swipe employee ID cards as they are presented.

For this purpose, dedicated apps have been specially built for iPhone and Android.

> ***Roadmap:*** *Future plans include a secondary mobile app purposefully built for employee self-service to enable individual employees to start/stop their own shift (providing the appropriate organisational policy/setting) however ETA is not yet defined.*

Fixed Device (i.e. wall-mounted)

Location-fixed options include a purpose-built tamper-resistant device that utilises Near Field Communication (contactless) swipe-cards for automating the in/out process.

The device, known as TimeTablet™, is assembled from an NFC-capable tablet, housed within a tamper-resistant wall-mountable VESA 75 enclosure, and has been 'locked down' with stock Android interfaces removed to prevent alternative use by staff members (i.e. it cannot be used to run other applications, browse the internet, etc.).

Application Programming Interface (API)

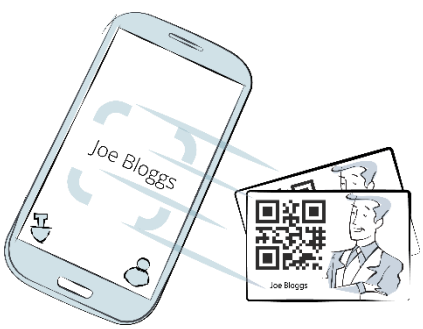
An API has been developed for interfacing third-party apps/devices however we have yet to *officially* release access to a third party.

To request/discuss early-access options please contact support@timedock.com

Clocking In/Out

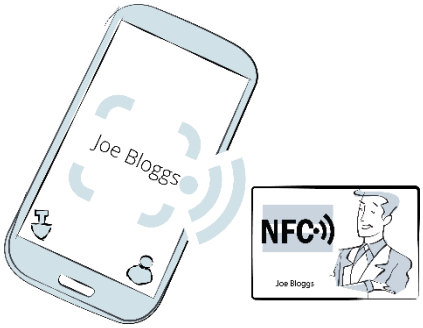
The most important aspect, *difference*, of our time-capturing system is to replicate the user-simplicity of a traditional card-based time-clock, *anywhere*.

Swiping In With a Mobile Device



QR-barcode

Mobile App uses device's camera to scan unique barcode-ID's to identify the employee and swipe in/out.



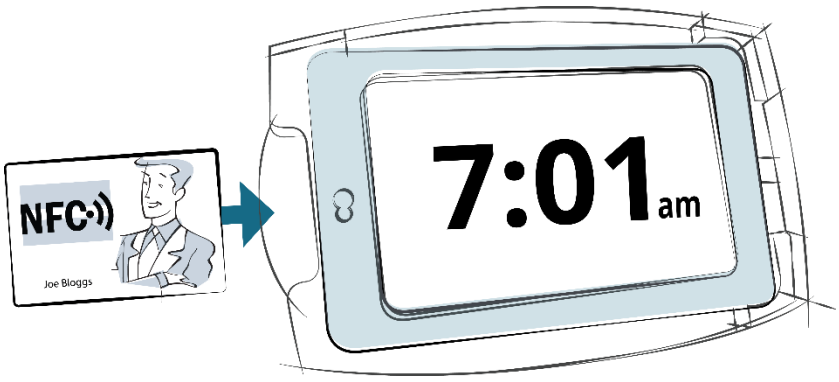
NFC / Contactless

NFC-capable devices (Android only) can 'swipe' staff in/out by 'bumping' the device to their NFC card/badge

Swiping In With a TimeTablet™

NFC / Contactless Cards

Staff can 'swipe' themselves in/out by 'inserting' their NFC ID card into the designated card-slot on the TimeTablet™.



Accessibility

"For maximum adoption, it should be quicker and easier than jotting hours on a paper time-sheet"

–Founder Le-roy Staines, TIMEDOCK.

Time-keeping should be easier and quicker than writing start/stop times on a paper time-sheet.

Instead of requiring heavy multi-screen navigation, clicks, dropdowns, typing and employee searches, all on a tiny screen and interface, our apps require only the wave of a printed ID card to operate.

For more information refer section "Clocking In/Out".

Portability

Using mobile technology, we've upgraded the traditional card-based time-clock to *everywhere*.

All Mobile Devices

We've built streamlined apps for the iPhone and Android, as well as a clever fall-back allowing any other internet-connected smartphone to use any QR-reader app to scan in.

Tip: Simple QR scan is password-protected to prevent employees scanning themselves.

Anywhere Online, and Offline

All apps and devices connected with TIMEDOCK send their data immediately to our secure database through a secure (SSL) internet connection.

In an out-of-coverage situation, or if the user has turned their data off temporarily, then the data will persist on the device and retry later, after a connection becomes available.

> *Tip: Admins can view from the web dashboard which apps/devices have not recently communicated with TIMEDOCK servers.*

***** On-site *and* off-site restrictions impose limitation at some levels. For more than 500 employees and/or high jobs through-put or exceedingly many time-capturing devices, we recommend conducting a business requirement analysis.

In some instances a controlled piloting simulation may also be suitable.

DISCLAIMER: In some instances a business analysis and piloting simulation and/or trial may incur significant expense at which a prior one-off cost may be incurred by, and billed to, the prospect. In all instances this cost would be identified and agreed upon before engaging in the pre-implementation activities.

Organisational Scalability

Any* number of apps and devices can be used together to form a single networked time-keeping system across your whole organisation, regardless of location fragmentation.

Apps/Devices

All supported apps and devices work together by 'docking' into TIMEDOCK, and any* number of personnel may traverse between them.

Multiple-time-clocks example:

7:00 am – John arrives at head office and clocks in (to no particular job) using a *wall-mounted TimeTablet™ device*.

10:00 am – John arrives at a job across town. He approaches the site manager who scans him onto that job, *using his iPhone*.

2:30 pm – John leaves site and the site manager *swipes him off the job, but not out completely*.

3:30 pm – John is just leaving the office and *inserts his card into the TimeTablet™ to clock out for the day*.

The end result (simplified):

Name	Date	Hours	Job
John	1/05/15	3	N/A
John	1/05/15	4.5	Site A
John	1/05/15	1	N/A

Or, in time-sheet format:

Name	Monday	Tue...
John	8.5	...

Server Scalability

The core Database, 'web portal' and web API technologies are hosted on Microsoft's Windows Azure Cloud platform –a highly configurable, secure, and *scalable* cloud hosting environment.

With Windows Azure we can scale up (and down) on-demand. That means if we're facing an unusual spike in activity, or more simply we've just on boarded a particularly large customer, then we can quickly and easily scale the server resources to meet the demand.

Service-Level Agreement

This Service-Level Agreement (this "Agreement" or this "Service-Level Agreement"), effective for the full duration of service provided, including free accounts and trials, is made by and between the customer and TIMEDOCK, a company organized and existing in New Zealand, with offices located at 20 Florence Ave, Auckland, New Zealand ("Supplier").

WHEREAS, the Customer has utilized, and continues to utilize, services and products provided by the Supplier; and/or

WHEREAS, the Parties have entered into an agreement effective for the full duration of service as outlined above, (the "Contract") for the provision by Supplier of the Services (as defined therein) (the "Services"); and

WHEREAS, the Contract states that a service level agreement is a condition precedent to any extended term of the Contract; and

NOW, THEREFORE, in consideration of the foregoing, and of the terms and conditions and the Service Levels, the Parties hereby agree as follows:

1. SERVICE LEVELS & SERVICE CREDITS

The Supplier shall at all times during term of this Agreement provide the Services to meet or exceed the Service Level Performance Measure for each Service Level Performance Criterion, as defined herein below.

The Supplier acknowledges that any failure to meet a Service Level may have a material adverse impact on the business and operations of the Customer and that it shall entitle the Customer to the rights set out in this Agreement below, including the right to any Service Credits (as defined below).

The Supplier acknowledges and agrees that any Service Credit is a price adjustment reflecting the value (subscription cost) of any lost service caused by failure to meet a Service Level. Both Parties agree that the Service Credits are a reasonable method of price adjustment to reflect poor performance.

Other than the Customer's termination rights as set forth in the Terms Of Service, A Service Credit shall be the Customer's exclusive financial remedy for a failure to meet a Service Level.

2. PERFORMANCE MONITORING

The Supplier shall implement all measurement and monitoring tools and procedures necessary to measure, monitor and report on the Supplier's performance of the provision of the Services against the applicable Service Levels at a level of detail sufficient to verify compliance with the Service Levels.

The Supplier shall immediately notify the Customer in writing if the level of performance of the Supplier of any element of the provision by it of the Services during the term of the Contract is likely to or fails to meet any Service Level Performance Measure.

3. OBJECTIVES

The objectives of the Service Levels and Service Credits are to:

1. Ensure that the Services are of a consistently high quality and meet the requirements of the Customer;

2. Provide a mechanism whereby the Customer can attain meaningful recognition of the Supplier's failure to deliver the level of service for which it has contracted to deliver; and

3. Incentivise the Supplier to comply with and to expeditiously remedy any failure to comply with the Service Levels.

4. SERVICE LEVELS

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Credit for each Service Period affected
Availability of the Service (accessing data and critical software functions)	Availability	99.5%	5% Service Credit gained for each percentage under the specified Service Level Performance Measure
Availability of Customer Service and Support	Availability	Between the hours of (published under "Business Hours" at: http://timedock.com/help/) and of the Supplier's Time Zone, exclusive of public holidays, or otherwise overridden by individual service agreement	Service credit to be defined by the breach of other service level performance criterion, caused by a failure to meet the service level performance measure.
Persisted Data	Retention	100% retention from first use of the service, during the lifetime of the service, and beyond the lifetime of the service (accessibility determined by the availability of service, feature "restrictions" of the service, and the availability of the Customer account (non-suspension or cancellation).	5% (based on 1 month subscription cost) gained for each day-date period of non-persisted data (not including client-device-data not-yet-persisted to TIMEDOCK database and/or Database backups).

5. SERVICE CREDITS

Service Credits are required to be credited to the account in the event that the Service Level achieved falls below the Service Level Performance Measure in a Service Period.

The Service Credit is determined by the Service Level achieved, the Service Level Performance Measure, and is calculated by using the straight line formula below:

1. Availability:

Service Credit $ = ((a-x)*c)*d)

where,

"a" is the Service Level Performance Measure (%) below which Service Credits become payable;

"x" is the Achieved Service Level (%) for a Service Period;

"c" is the Service Credit (%) payable if the Achieved Service Level falls below the Service Level Target; and

"d" is the amount payable in respect of the Services during the Service Period.

6. DATA

The Customer is granted *indirect use of* the Provider's database storage, through the availability of the exposed data access functions of the service (i.e. Web Portal, Web API), and within the bounds of the intended use, for long-term storage, access and processing of the data collected and modified by functions of the service.

The Customer receives the right to view, modify and append the data, *through the use of* the exposed interfaces and functions of the service. Utilising the service, including the generation and storage of relevant data, does not constitute ownership of any hardware, software, infrastructure, data files, or other non-intended exposure, access, modification or exclusive "rights" to the data, outside the bounds of the normal function of the service and service agreement.

The Customer entrusts the Provider to maintain data availability and validity to an exceptional standard, as outlined in the "Service Levels" clause, and is responsible for regularly filing independent copies of business-critical data, through the exposed means of various reports and data exports of the service features.

The Provider will implement internal procedures and infrastructure to ensure Customer data remains private and exclusive to the Customer; however the Customer acknowledges that the following instances may warrant the provider to access, modify, copy or review the data:

1. The Provider may review, modify, delete or append data in the interest of servicing that customer’s specific request.
2. The Provider's software and services may review, modify, delete or append data in the interest of providing the features of the service.
3. The Provider's automated (non-human) functions may review Customer data to calculate non-identifying statistics for internal and public use.

Security

Data Centre / Servers

Excerpt from TIMEDOCK's cloud services provider of Database, Application, Cache, Service Bus etc.

Through cutting-edge security practices and unmatched experience running some of the largest online services around the globe, Microsoft delivers enterprise cloud services customers can trust.

Design and Operational Security

Microsoft has developed industry-leading best practices in the design and management of online services, including:

Security Centers of Excellence. The Microsoft Digital Crimes Unit, Microsoft Cybercrime Center, and Microsoft Malware Protection Center provide insight into evolving global security threats.

Security Development Lifecycle (SDL). Since 2004, all Microsoft products and services have been designed and built from the ground up using its Security Development Lifecycle - a comprehensive approach for writing more secure, reliable and privacy-enhanced code.

Operational Security Assurance (OSA). The Microsoft OSA program provides an operational security baseline across all major cloud services, helping ensure key risks are consistently mitigated.

Assume Breach. Specialized teams of Microsoft security engineers use pioneering security practices and operate with an 'assume breach' mindset to identify potential vulnerabilities and proactively eliminate threats before they become risks to customers.

Incident Response. Microsoft operates a global 24x7 event and incident response team to help mitigate threats from attacks and malicious activity.

Security Controls and Capabilities

Azure delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure.

24 hour monitored physical security. Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.

Monitoring and logging. Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts. In addition, multiple levels of monitoring, logging, and reporting are available to provide visibility to customers.

Patching. Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.

Antivirus/Antimalware protection. Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.

Intrusion detection and DDoS. Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.

Zero standing privileges. Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems that store customer data is strictly controlled via lock box processes.

Isolation. Azure uses network isolation to prevent unwanted communications between deployments, and access controls block unauthorized users. Virtual Machines do not receive inbound traffic from the Internet unless customers configure them to do so.

Azure Virtual Networks. Customers can choose to assign multiple deployments to an isolated Virtual Network and allow those deployments to communicate with each other through private IP addresses.

Encrypted communications. Built-in SSL and TLS cryptography enables customers to encrypt communications within and between deployments, from Azure to on-premises datacenters, and from Azure to administrators and users.

Private connection. Customers can use ExpressRoute to establish a private connection to Azure datacenters, keeping their traffic off the Internet.

Data encryption. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to implement the methods that best meets their needs.

Identity and access. Azure Active Directory enables customers to manage access to Azure, Office 365 and a world of other cloud apps. Multi-Factor Authentication and access monitoring offer enhanced security.

Internal IT / Procedures

Production Data (i.e. Live Customer Data), protected by strong security implemented on the servers which they are hosted, still pose potential risk with outside interfaces (i.e. 'the human element').

To minimize risk we:

- Implement strong identity and password-based authentication at many stages between the development, staging and deployment environments.
- Never download or share live data with any of our development or staging environments.
- Implement demilitarized-zones for segregating departments, and people.
- Run extensive manual and automated testing, before deploying production features that could expose or harm tenant data.
- Educate all staff, even the receptionist, on common fail-points such as rogue emails, unknown attachments, suspicious phone calls, USB drives of unknown origin, etc.
- Implement other standardised IT practises (i.e. Antiviruses, Firewalls, regular security update checks, etc.).

Data Backup

To minimize risk of data loss and corruption we utilize several strategies, standardized for a cloud-based setup.

1. Geolocation redundancy –Databases are replicated (near-live) on up to four secondary instances to ensure high availability and disaster continuity.
2. 14-day point-in-time database recovery
3. Location-independent offsite backups, with a three month retention.

Note: As per the SLA customers are required to back up their own data, as a secondary measure, by utilizing reporting and data export functions made available by the service.

Limitation

Whilst we are always streamlining performance, usability and functionality, there are known limitations with our system that we feel obliged to 'confess'. Of course, we are always working to minimise these 'limitations' and a number of initiatives are already under way, as detailed below.

Known limitations, as at January 2015:

1. Administration, reporting and management becomes less efficient, due to only basic reporting and management functions, for organisations with several hundred or more employees.
   Tip// early-mid 2015 we are significantly expanding functionality in the area of automated administration and reporting, to better serve our larger customers.
2. Responsiveness, particularly of the web portal and older mobile devices, can start to become 'laggy' at 1000 – 2000+ employees, depending on the setup.
3. Our largest *production* deployment sees around 700 – 800 employees clocking in/out under a single organisation. Whilst the organisation continues to find our system valuable, we can clearly see vast improvements (as per #1 above) at this level.
4. Our largest in-house *test* deployment to date is 2000 employees clocking in/out once per day (not onto jobs). Timesheet performance on the web portal held well at 8 seconds to load, and the Android devices held well in terms of scanning performance.
5. The iPhone app (on iPhone 5 and lower) begins to fail intermittently at 300 – 500 employees. Major performance enhancement is currently under way, with an ETA of late February 2015.

Mobile Data Usage

Below are *guidelines* to individual mobile data usage incurred, based on several organisational requirement scenarios (as at Jan 2015).

One IN/OUT per person, per day (Mon-Fri):

Employees	Estimated Data Use (per mobile device)
1-25	~25mb per month
26-100	~50mb per month
101-250	~100mb per month
251-1000	~300mb per month
1001-2500	~750mb per month

Including OUT/IN for lunch (Mon-Fri):

Employees	Estimated Data Use (per mobile device)
1-25	~50mb per month
26-100	~100mb per month
101-250	~200mb per month
251-1000	~600mb per month
1001-2500	~1500mb per month

OUT/IN for Lunch plus job-switching 3 times per employee, per day (Mon-Fri):

Employees	Estimated Data Use (per mobile device)
1-25	~100mb per month
26-100	~200mb per month
101-250	~400mb per month
251-1000	~1200mb per month
1001-2500	~3000mb per month

Support

Below are our currently available support options. For larger organisational contracts we are more than happy to negotiate account-specific resource options.

For more info contact info@timedock.com

Method	Availability	Plan-restriction
Phone support.	9am – 3pm New Zealand Standard Time, Mon-Fri.	Available to anyone.
Email support.	First response within 12 hours in most cases, 7 days per week.	Available to anyone.
Community Forums	First response, from an organisational support person, within 12 hours Mon-Fri (New Zealand Standard Time).	Available to anyone.

Standard Pricing

Our standard self-service model, suitable for organisations under 500 employees, is based (at Jan 2015) on a pay-monthly per-active-employee automated billing structure.

Currency: Please note that all prices are in United States Currency (1 NZD = 0.77 USD at 14 Jan 2015)

Tax: New Zealand customers only, will incur GST over and above the amount stated in all prices below.

Features	Standard Plan
Base Fee	No base fee
Active Employees / users	$5 each, per month
PVC ID cards	$1 each
Print-your-own ID cards	Free
Activities / Jobs	No restriction
Payroll integration	*Please enquire*
(optional) TimeTablet™ devices ex. Shipping / installation	$350 each, or use our mobile app for free instead.
Support option	Phone support during NZ business hours, Email, Online chat widget

Volume Licensing

For larger organisations (250+), a volume-licensing plan can be a more cost effective and forecastable option.

Organisations can effectively load as many employees as they wish into the system, which is also highly beneficial for organisations with many temporary staff, or high churn rates.

Plans available include 50k, 75k, 100k and 250k transactions per month.

Currency: Please note that all prices are in United States Currency (1 NZD = 0.77 USD at 14 Jan 2015)

Tax: New Zealand customers only, will be charged GST over and above the amount stated in all prices below.

Large Organisations:

Features	V100	V250
Raw transactions (per month)	100,000	250,000
= *approx. staff (basic)*	*~1000*	*~2500*
= *approx. staff (with jobs)*	*~500*	*~1250*
Mobile data estimate (per device)	300mb	750mb
Cost, per month	USD$2249	USD$3499

Medium-Large Organisations:

Features	V50	V75
Raw transactions (per month)	50,000	75,000
= *approx. staff (basic)*	*~500*	*~750*
= *approx. staff (with jobs)*	*~250*	*~375*
Mobile data estimate (per device)	200mb	250mb
Cost, per month	USD$1249	USD$1799

Payment

Standard Plans

Standard plans are automatically invoiced at the end of each billing month, to be paid within 14 days.

Payment can be made via credit card with our elected secure payment processing merchant (PayPal as at Mar 2018).

Failure to meet payment within the grace period results in a non-critical suspension of the account.

-*Staff will continue to be able to clock in/out via external apps/devices however administrator access becomes blocked until the overdue payment made. All data is preserved.*

Custom / Volume Plans

All fixed-value plans (i.e. volume-based and custom plans) are billed month in advance, with a four week grace period.

Payment can be made via credit card with our elected secure payment processing merchant (PayPal as at Mar 2018).

Failure to meet payments within 28 days of invoicing will result in non-critical suspension of the account.

-*Staff will continue to be able to clock in/out via external apps/devices however administrator access becomes blocked until the overdue payment made. All data is preserved.*