TimeControl® Online Security Architecture

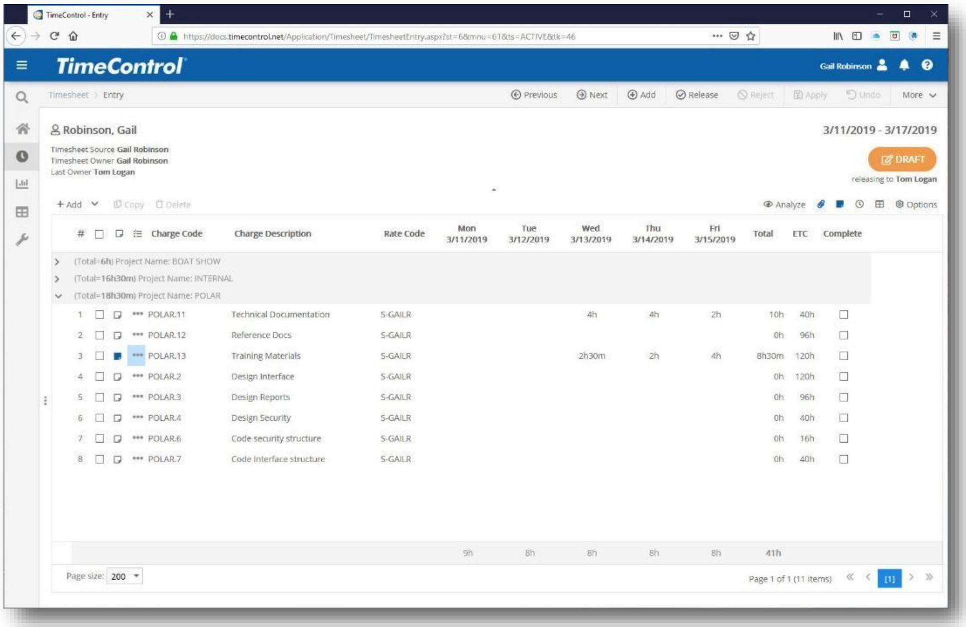
For more information contact:
HMS Software
189 Hymus, Suite 402
Pointe-Claire, Quebec H9R 1E9
Tel: 514-695-8122
Fax: 514-695-8121
Email: info@hms.ca
Web: www.TimeControl.com

Last update: May 2025

Table of Contents

Overview

HMS has been creating corporate timesheet systems since its inception in 1984. Our clientele includes organizations in both the public and private sector. Whether the client has 10 employees or is a Fortune 1000 multi-national organization, the security of the TimeControl timesheet environment is a critical concern. A timesheet system may be used for only a few minutes per week by most users but the data it contains can be used for the most sensitive requirements including billing, payroll, government regulation compliance or auditable tax purposes. HMS has designed TimeControl with the security of this data in mind.



Robinson, Gail

3/11/2019 - 3/17/2019

Timesheet Source Gail Robinson
Timesheet Owner Gail Robinson
Last Owner Tom Logan

releasing to Tom Logan

#	Charge Code	Charge Description	Rate Code	Mon 3/11/2019	Tue 3/12/2019	Wed 3/13/2019	Thu 3/14/2019	Fri 3/15/2019	Total	ETC	Complete
(Total=6h) Project Name: BOAT SHOW											
(Total=16h30m) Project Name: INTERNAL											
(Total=18h30m) Project Name: POLAR											
1	POLAR.11	Technical Documentation	S-GAILR			4h	4h	2h	10h	40h	□
2	POLAR.12	Reference Docs	S-GAILR						0h	96h	□
3	POLAR.13	Training Materials	S-GAILR			2h30m	2h	4h	8h30m	120h	□
4	POLAR.2	Design Interface	S-GAILR						0h	120h	□
5	POLAR.3	Design Reports	S-GAILR						0h	96h	□
6	POLAR.4	Design Security	S-GAILR						0h	40h	□
7	POLAR.6	Code security structure	S-GAILR						0h	16h	□
8	POLAR.7	Code Interface structure	S-GAILR						0h	40h	□
				9h	8h	8h	8h	8h	41h		

Page size: 200

Page 1 of 1 (11 items) [1]

Security of any corporate data is important, but timesheet data is often among the most sensitive. If the data is used for payroll, timesheet data could contain the salary cost of employees. If it is used for project management, timesheet data could reveal the true actual costs of accomplishing elements of work.

This paper will discuss the security design of the in-the-cloud subscription service of TimeControl and TimeControl Industrial and considers the design of TimeControl and higher. If you are interested in the security architecture of TimeControl or TimeControl Industrial for an on-premise installation, we recommend you read the white paper “TimeControl On-Premise Security Architecture” available from the TimeControl.com website.

Over the coming pages we’ll look at security from several perspectives including database architecture, data encryption, the TimeControl communication layer, TimeControl functionality security, working across the Internet and related topics of interest such as firewalls, authentication and intrusion detection.

This paper was written for those with a good understanding of technical issues such as firewall architecture and Internet Web-based security.

The fundamental driving force behind the TimeControl security architecture is to:

a) deny access to unauthorized personnel to data they have not been granted

b) access to,

c) protect TimeControl data from unauthorized tampering or corruption and;

d) to protect corporate infrastructure from using TimeControl to gain access to gain access to other corporate resources.

HMS Software’s testing of TimeControl follows the testing methodology outlined by the Open Web Application Security Project (OWASP). Information on OWASP can be found at https://www.owasp.org.

Amazon EC2

HMS uses the Amazon EC2 service which is used by some of the most recognizable publishers of software services to deliver a highly robust and reliable system architecture. Information from Amazon on the security compliance of their architecture as well as their numerous certifications and accreditations can be found at aws.amazon.com/security.

TimeControlOnline runs on the Amazon EC2 environment. Information on the network architecture and the layers of security which exist prior to any potential threat even reaching the TimeControlOnline hosted servers can be found at aws.amazon.com/security.

Amazon security certifications

According to Amazon, they have past successfully completed multiple SAS70 Type II audits, and now publishes a Service Organization Controls 1 (SOC 1), Type 2 report, published under both the SSAE 16 and the ISAE 3402 professional standards as well as a Service Organization Controls 2 (SOC 2) report. In addition, AWS has achieved ISO 27001 certification, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). In the realm of public sector certifications, AWS has received authorization from the U.S. General Services Administration to operate at the FISMA Moderate level and is also the platform for applications with Authorities to Operate (ATOs) under the Defense Information Assurance Certification and Accreditation Program (DIACAP). We will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services.

Physical Security

The Amazon infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical controls to prevent unauthorized access.

Secure Services

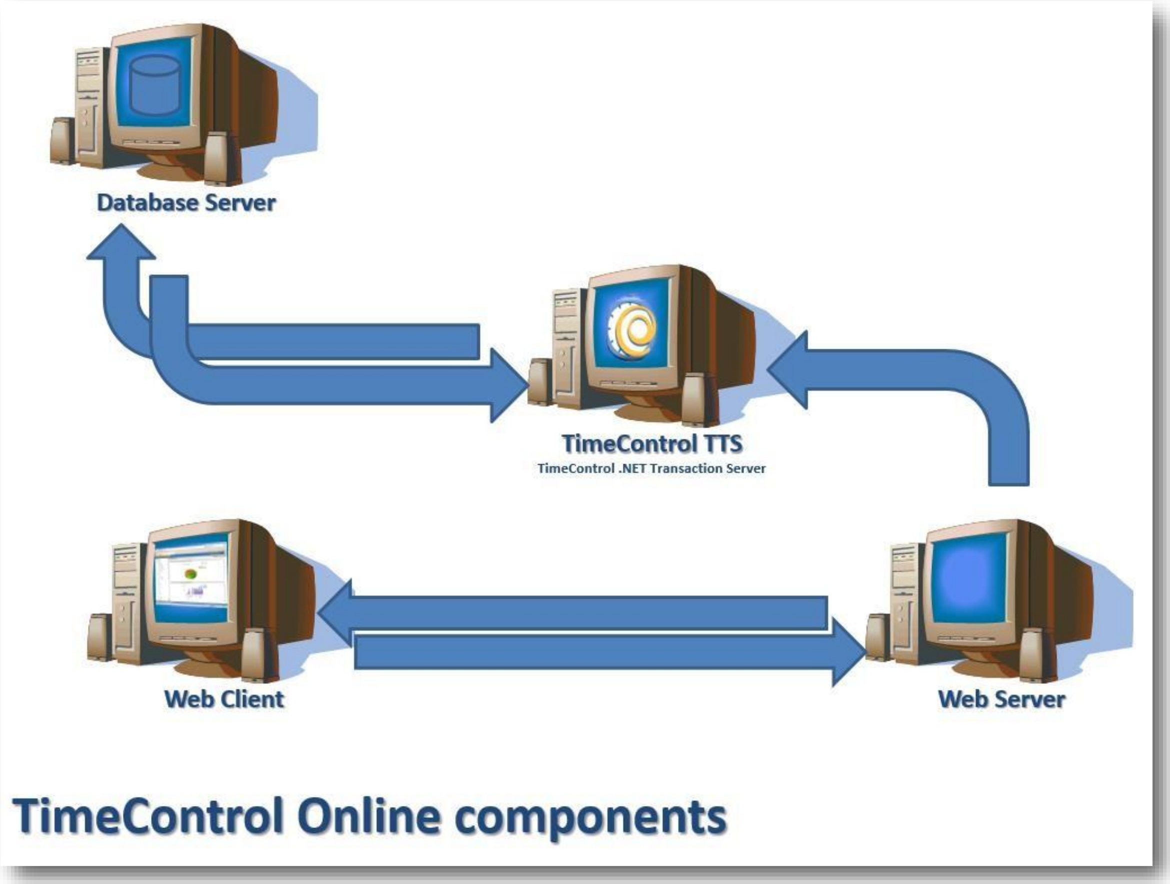
Each of the services within the Amazon EC2 environment contains a number of capabilities that restrict unauthorized access or usage.

For more information on the physical security, secure services that are automatically part of the EC2 environment and how Amazon monitors and defends against external threats, visit aws.amazon.com/security.

TimeControl Components Overview

TimeControl has some key components that are critical to its system operations and HMS has used these components to implement TmeControlOnline as a service. TimeControl is an n-tier application with a design that allows for the system to be infinitely scalable. The key components include a Database Server, the TimeControl Administration Transaction Server middle-ware, the TimeControl Transaction Server Middleware Web Server components and

the web-based client. We'll describe these components in more detail here.


Database Server
TimeControl TTS
TimeControl .NET Transaction Server
Web Client
Web Server
TimeControl Online components

Database Server

TimeControlOnline stores all of its data in a MySQL database. This database is housed on a server which is internal to the TimeControlOnline network.

TimeControl Transaction Server (TTS)

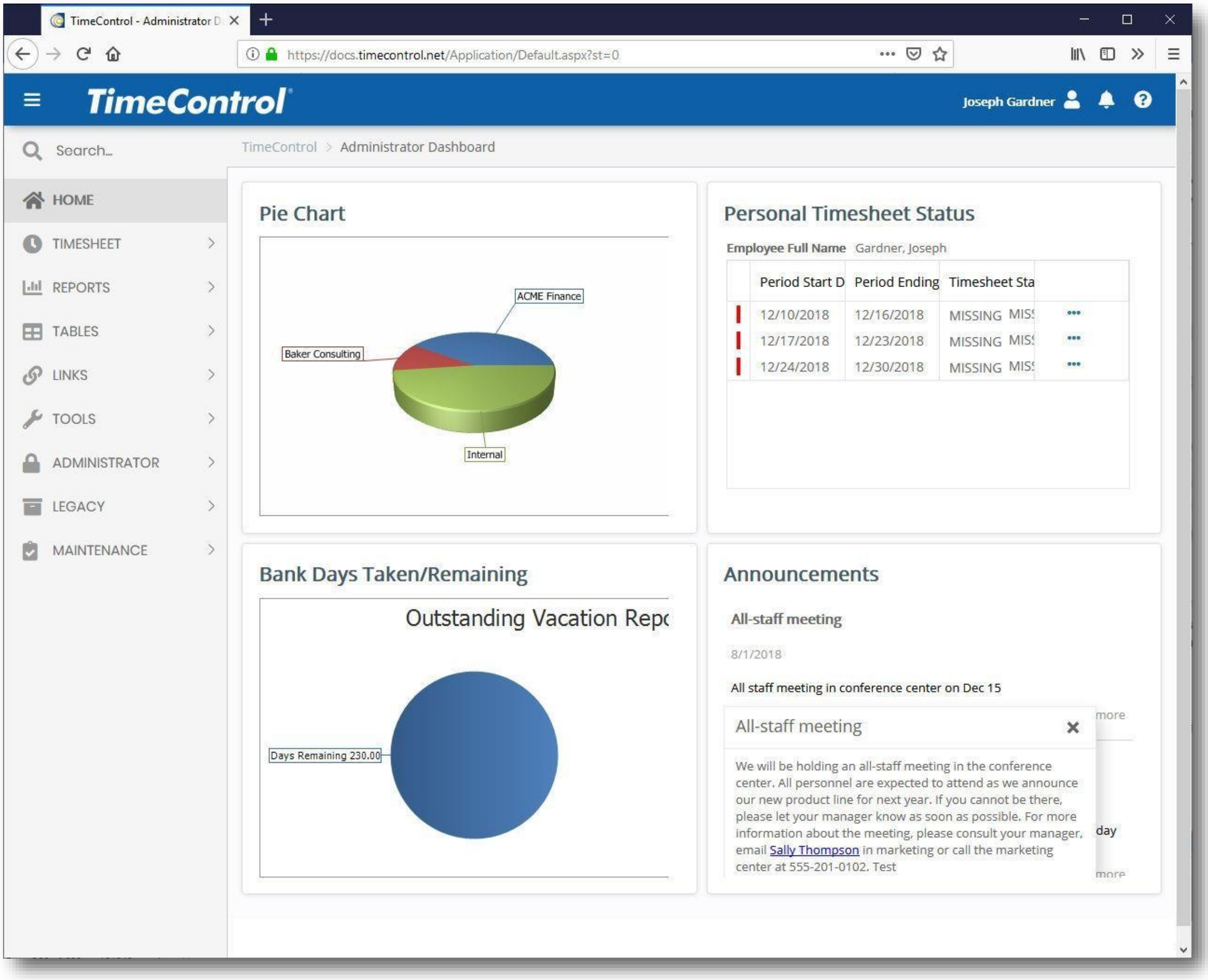
TimeControl includes a middleware component called the TimeControl Transaction Server or TTS. The TTS is a .Net web service which interfaces with web-based .Net components and interacts with the database. The Microsoft .Net architecture is highly secure. The TTS runs as a Windows Service in TimeControl Online.

TimeControl Scheduler Service

There are several automated functions which can be run as scheduled events within TimeControl. These include unattended emails sent on a schedule, for example, when timesheets are missing and overdue or the posting of timesheets or linking of TimeControl to server-based project management tools.

Web Server

TimeControl users are presented with a browser-based web interface written in an AJAX (Asynchronous JavaScript and XML) structure. To deliver this interface to the browser, TimeControl uses Microsoft's Internet Information Services (IIS) which is used to deliver TimeControl Online.



Personal Timesheet Status

Employee Full Name Gardner, Joseph

	Period Start D	Period Ending	Timesheet Sta	
▌	12/10/2018	12/16/2018	MISSING MIS!	•••
▌	12/17/2018	12/23/2018	MISSING MIS!	•••
▌	12/24/2018	12/30/2018	MISSING MIS!	•••

Announcements

All-staff meeting

8/1/2018

All staff meeting in conference center on Dec 15

All-staff meeting ✕

We will be holding an all-staff meeting in the conference center. All personnel are expected to attend as we announce our new product line for next year. If you cannot be there, please let your manager know as soon as possible. For more information about the meeting, please consult your manager, email Sally Thompson in marketing or call the marketing center at 555-201-0102. Test

Timesheet Web Client

The TimeControl web interface requires a web browser. Numerous browsers and hardware platforms are supported. TimeControl works with Edge, Internet Explorer, Firefox, Chrome, Safari and Mozilla.

Communications: .Net

TimeControl's user web client uses Microsoft's .Net architecture to communicate between the web page and the TimeControl TTS middleware service. This is a highly secure, encrypted environment which uses a streaming object protocol to package data and transmit it quickly from one end to the other.

Database Access

TimeControl's data is stored in a relational database. It does do calculations but is primarily designed to collect, summarize and report on data that has been collected in a very structured and stable manner. Access to and protection of the data is, therefore, our primary concern.

The TimeControl data architecture is designed with a 2-database structure. The primary database contains all the tables, fields, indices, constraints etc. that are required to operate the program. A secondary database is used for gateway purposes and contains only one table with one record and two fields.

One of the HMS design team's concerns was allowing access to this database to anyone who could reach the server.   The use of a security gateway database was designed to defeat this. The gateway database contains a single username and password used to gain complete access to the main TimeControl database where all the TimeControl data is contained. The security data is encrypted with a method hard-coded into the TimeControl applications. This provides an additional level of insulation of the main database.

When starting, the TimeControl middleware the TimeControl Transaction Server (TTS) starts up and looks in its startup definition for the location of the security database. It along is given a username and password to access this database. Once the TTS has reached the security database, it decrypts the username and password contained there to determine how to make a connection to the main database. The TTS then establish a connection to the database and stands by for requests from the client-access controls such as a TimeControl .Net control to make a data request. All data is brokered through the middleware. No TimeControlOnline end-user or Administrator is given any knowledge of the database location and no user ever makes a direct connection to the database.

TimeControl testing follows OWASP standards. Using ZAP, an OWASP approved tool, HMS has checked and ensured a pass for the following tests:

Name	Rule Type	Threshold	Strength	Test Status
.htaccess Information Leak	Active	Medium	Medium	Passed
Directory Browsing	Active	Medium	Medium	Passed
Server Side Code Injection	Active	Medium	Medium	Passed
CRLF Injection	Active	Medium	Medium	Passed
Remote OS Command Injection	Active	Medium	Medium	Passed
Path Traversal	Active	Medium	Medium	Passed
Remote File Inclusion	Active	Medium	Medium	Passed
Parameter Tampering	Active	Medium	Medium	Passed
Server Side Include	Active	Medium	Medium	Passed
SOAP Action Spoofing	Active	Medium	Medium	Passed
SOAP XML Injection	Active	Medium	Medium	Passed
Cross Site Scripting (Reflected)	Active	Medium	Medium	Passed
Cross Site Scripting (Persistent)	Active	Medium	Medium	Passed
Script Active Scan Rules	Active	Medium	Medium	Passed
Cross Site Scripting (Persistent) - Prime	Active	Medium	Medium	Passed
Buffer Overflow	Active	Medium	Medium	Passed
Cross Site Scripting (Persistent) - Spider	Active	Medium	Medium	Passed
Format String Error	Active	Medium	Medium	Passed
SQL Injection	Active	Medium	Medium	Passed
External Redirect	Active	Medium	Medium	Passed
Cross Site Scripting (DOM Based)	Active	Medium	Medium	Passed
ELMAH Information Leak	Active	Medium	Medium	Passed
Source Code Disclosure - /WEB-INF	Active	Medium	Medium	Passed
Private IP Disclosure	Passi	Medium	-	Passed
Session ID in URL Rewrite	Passi	Medium	-	Passed
Cookie without SameSite Attribute	Passi	Medium	-	Passed
CSP	Passi	Medium	-	Passed
X-Debug-Token Information Leak	Passi	Medium	-	Passed
Username Hash Found	Passi	Medium	-	Passed
X-AspNet-Version Response Header	Passi	Medium	-	Passed
Insecure JSF ViewState	Passi	Medium	-	Passed
Script Passive Scan Rules	Passi	Medium	-	Passed
Stats Passive Scan Rule	Passi	Medium	-	Passed
Vulnerable JS Library	Passi	Medium	-	Passed
Charset Mismatch	Passi	Medium	-	Passed
Cookie No HttpOnly Flag	Passi	Medium	-	Passed
Absence of Anti-CSRF Tokens	Passi	Medium	-	Passed
Cookie Without Secure Flag	Passi	Medium	-	Passed

Name	Rule Type	Threshold	Strength	Test Status
Incomplete or No Cache-control Header	Passive	Medium	-	Passed
Cross-Domain JavaScript Source File	Passive	Medium	-	Passed
Content-Type Header Missing	Passive	Medium	-	Passed
Anti-clickjacking Header	Passive	Medium	-	Passed
X-Content-Type-Options Header	Passive	Medium	-	Passed
Application Error Disclosure	Passive	Medium	-	Passed
Information Disclosure - Debug Error	Passive	Medium	-	Passed
Information Disclosure - Sensitive Information in URL	Passive	Medium	-	Passed
Information Disclosure - Sensitive Information in HTTP Referrer	Passive	Medium	-	Passed
WSDL File Detection	Passive	Medium	-	Passed
Loosely Scoped Cookie	Passive	Medium	-	Passed
Timestamp Disclosure	Passive	Medium	-	Passed
Viewstate	Passive	Medium	-	Passed
Cross-Domain Misconfiguration	Passive	Medium	-	Passed
Server Leaks Information via "X-Powered-	Passive	Medium	-	Passed
Secure Pages Include Mixed	Passive	Medium	-	Passed
Weak Authentication Method	Passive	Medium	-	Passed

1. **Internal TimeControl user and password authentication**
   TimeControl includes a server-side authentication of a user name and encrypted password stored in the combination to determine if a) the user has an authenticatable login and, b) what rights the user has. Then the TimeControl server establishes a session ID and returns that session ID to the client station. The ID allows session variables to be maintained and for authentication to be remembered.
2. **Single Sign on**
   TimeControl supports the use of Microsoft's single sign-on using Active Directory.
3. **LDAP**
   TimeControl supports the use of other LDAP compliant technology to use user name and password combinations which are authenticated by the TimeControl Server to the LDAP.
4. **SAML**
   TimeControl supports SAML 2.0

No authentication status of the user is ever stored and submitted from the client side for any module so exploiting an "authenticated" parameter is impossible. TimeControl's middleware server checks for each and every access to a module based on who the user is to ensure that the user has the appropriate access at that time. If a user's right to a module were to be revoked by a TimeControl Administrator, the next time the user would attempt to access that module, even a few moments later, they would be denied.

There is never information included in a transaction to TimeControlOnline that would allow sensitive information to be intercepted in the URL and then used by anyone to gain access to something they didn't have rights to.

It is important to remember also that someone would need to get this string even to be able to start manipulating it. If someone were able to defeat the SSL encryption and capture this string, all they would have is the menu call for a module of TimeControl. Without also having a) a valid login to TimeControl and b) having that login have the rights to this menu item, they would have no access to TimeControl at all. Even to capture this information, the intruder would need to either get physical access to the client station as its being used or try to intercept the data as it is transmitted to the server and that data is encrypted both by Windows .Net and by the Secure Socket Layer (SSL) encryption.

Secure Socket Layer Security in TimeControl Online

Access to the TimControlOnline site is encrypted using SSL (Secure Socket Layer) just as you would in a banking or purchasing website. This technology results in all traffic to and from the page being encrypted by the web server. Even the movement of the user name and password to be encrypted before it arrives at the server.

TimeControlOnline's SSL Certificate

Testing of the TimeControl.net SSL Certificate was done at: www.ssllabs.com.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1	
Subject	*.timecontrol.net Fingerprint SHA256: e36f3ebb2d4f142f04b4ee85143e457a1707d1b2f078c1d08e558d022118766a Pin SHA256: TVHGleYY+F5GUevRMR8M27Jg/NJb8VycB0cNBNOgPP4=
Common names	*.timecontrol.net
Alternative names	*.timecontrol.net timecontrol.net
Serial Number	00ad8efba6792b844aa12ae10aa0417f0e
Valid from	Mon, 25 Nov 2024 00:00:00 UTC
Valid until	Tue, 23 Dec 2025 23:59:59 UTC (expires in 6 months and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Sectigo RSA Organization Validation Secure Server CA AIA: http://crt.sectigo.com/SectigoRSAOrganizationValidationSecureServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No

Server Key and Certificate #1	
Revocation information	CRL, OCSP CRL: http://crl.sectigo.com/SectigoRSAOrganizationValidationSecureServerCA.crl OCSP: http://ocsp.sectigo.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Password Encryption

In TimeControl the internal TimeControl password system is used, giving each user access to TimeControl based on a user name and a password stored within the TimeControl database.

The password values are encrypted within the database so that even if someone were to get inadvertent reporting access that table, they will not be able to read the password entry for a user.

Once the login is complete, control of TimeControl communications is now passed to the TimeControl Transaction Server Middleware. TimeControl determines through its User Profiles what menu items the user should have access to and presents a menu with only those items.

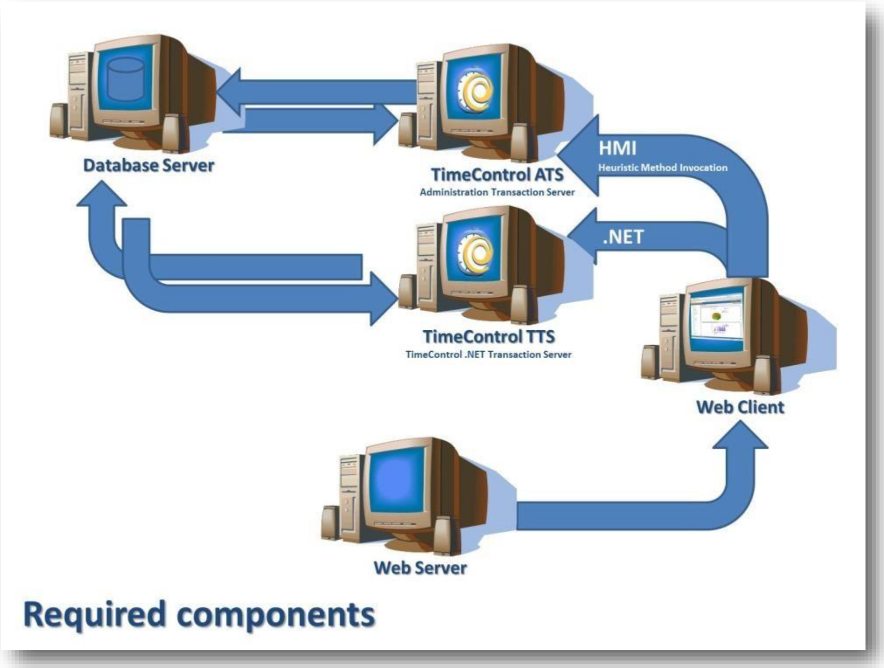
Access to the system is then controlled by a random server-generated session variable token for as long as the browser session is active. Once logged in, the user name and password are not transmitted again.

When each TimeControl component is accessed by the user, TimeControl determines if the session token is still appropriate for this component. If so, it displays the component to the user. This prevents a situation where someone could capture a URL to a specific function and then try to access it later at a different terminal.

Session tokens are designed to time-out after a set period of time so that even if the user leaves their screen open to TimeControl inadvertently, the log in session will expire automatically. This time out is configurable in the configuration file of the TimeControl middleware on the server.

Middleware Architecture

Modern web-based interfaces are either all server-based, which means that all the processing occurs at the web-server and the client only sees what looks like a web page or they are thin-client architecture which means that some of the work occurs on the server and some of the work occurs at the client's station. TimeControl is a thin-client design.


Database Server
TimeControl ATS
Administration Transaction Server
HMI
Heuristic Method Invocation
.NET
TimeControl TTS
TimeControl .NET Transaction Server
Web Client
Web Server
Required components

With some of the work occurring in-between the client and the database, TimeControl's architecture has multiple levels. Each level is usually called a 'tier'. Because TimeControl has been designed to have an unlimited number of middle tier installations, TimeControl is defined as an n-tier application.

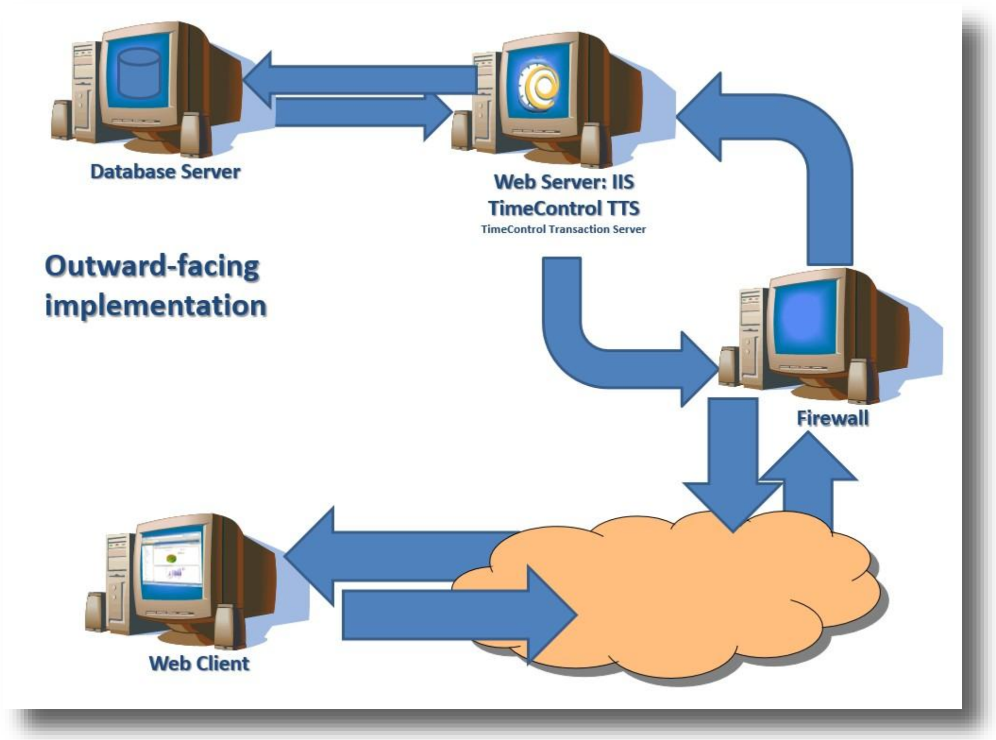
N-Tier design is important when we talk about security as it allows us to restrict access to corporate resources. Regardless of whether or not a firewall is implemented, end user components are connected only to the TimeControl middle tier, not ever directly to the database server allowing us to protect the database server much more stringently.

The sequence of events in making TimeControl function is as follows:

1. The end-user web browser accesses the TimeControl login web page on the web server.
2. A TimeControl component at the Web Server communicates with the TimeControl Transaction Server (TTS) to determine if the user should be granted access and, if so, what menu items should be displayed
3. The Web Server sends the TimeControl menu back to the client's web browser with instructions to the TimeControl components on how to connect to the middleware
4. The TimeControl components are activated by the end user by selecting a menu item The component communicates via the web server and the .Net protocol which is also completely encrypted.
5. The TimeControl middleware brokers any traffic and makes the appropriate interaction with the database server.

At no time does the end user machine communicate directly with the database server.

In TimeControlOnline, a firewall is in use. This allows us to insulate servers of the TimeControlOnline environment such as the database servers and other components using NAT (Network Address Translation) which further protects key elements of the system.



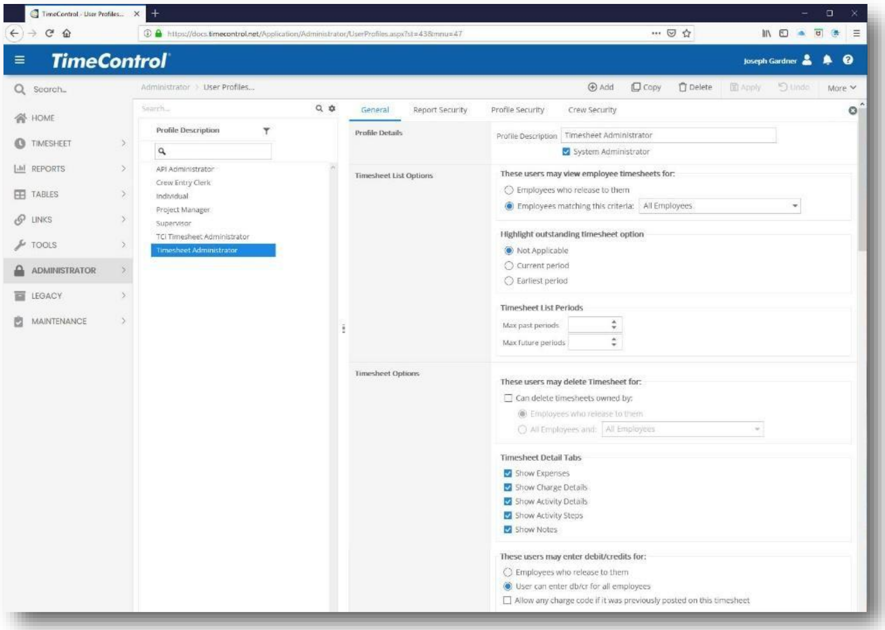
This is a very secure environment. The only area which is even vulnerable to attack is traffic on its way from the web browser client outside the network to the middleware machine inside the network. A worst- case scenario is that traffic to or from the middleware would be corrupted through malicious intent and this traffic is encrypted with an advanced encryption algorithm. Since the middleware only accepts data that meets the proper business rules, this type of attack would, at worst, cause an erroneous transaction, which would be rejected by the TimeControl transaction server.

HMS closes all ports in the middleware server which are not required for TimeControlOnline use in order to further harden the server.

Functional Access Control with TimeControl User Profiles

Once in TimeControl itself, there are extensive security structures in place to ensure that users are presented only with the functionality and data they require. The most significant of these is managed through the User Profile area. User Profiles is part of each of the TimeControl editions. This architecture ensures that users are not required to wade through areas of the system that are of no interest to them trying to find the functionality that they do require. This makes end users more effective when using TimeControl.

This same architecture ensures that only the data appropriate to that user is visible. The User Profile area is divided into two sections. The Data Section determines which open timesheets and which posted timesheet data can be viewed. An Administrator can define roles such as a supervisor who can see only data for people below them in a release structure or define the data explicitly through the use of filters.



API Administrator
Crew Entry Clerk
Individual
Project Manager
Supervisor
TCI Timesheet Administrator
Timesheet Administrator

Profile Description: Timesheet Administrator
☑ System Administrator

These users may view employee timesheets for:
○ Employees who release to them
● Employees matching this criteria: All Employees

Highlight outstanding timesheet option
● Not Applicable
○ Current period
○ Earliest period

Timesheet List Periods
Max past periods
Max future periods

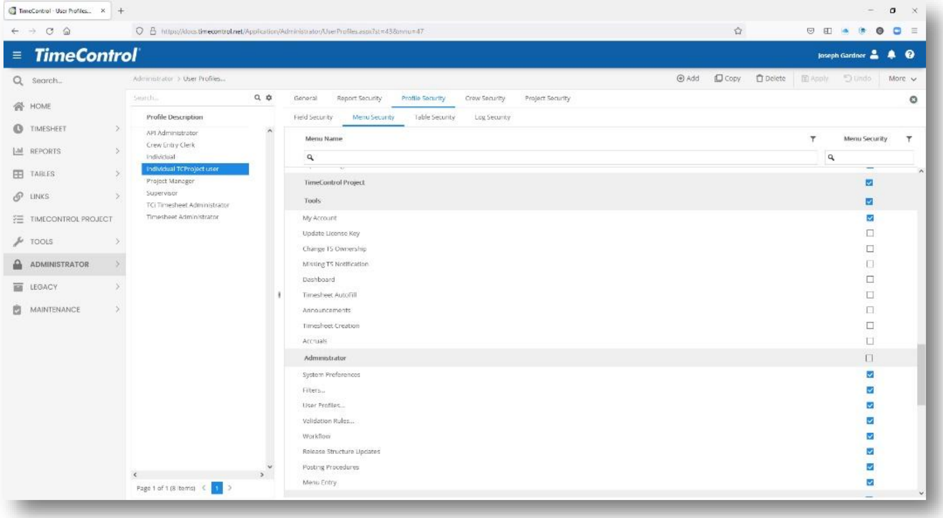
These users may delete Timesheet for:
☐ Can delete timesheets owned by:
● Employees who release to them
○ All Employees and: All Employees

Timesheet Detail Tabs
☑ Show Expenses
☑ Show Charge Details
☑ Show Activity Details
☑ Show Activity Steps
☑ Show Notes

These users may enter debit/credits for:
○ Employees who release to them
● User can enter db/cr for all employees
☐ Allow any charge code if it was previously posted on this timesheet

In addition to the data restrictions put on reporting and exporting by User Profiles, end users can also be restricted during data entry from seeing different project and charge code selections by imposing employee-level filters in the employee tables. This ensures that only data that is appropriate to the proper level of use is seen.

The second area of User Profiles is a lower level of detail. The Details tab controls first the functions that are available to each user. This allows an administrator to hide completely any aspect of the program including such things as table access, exporting functionality, project linking functionality, definition and configuration areas etc. This type of function-by-function security is essential in such an application.



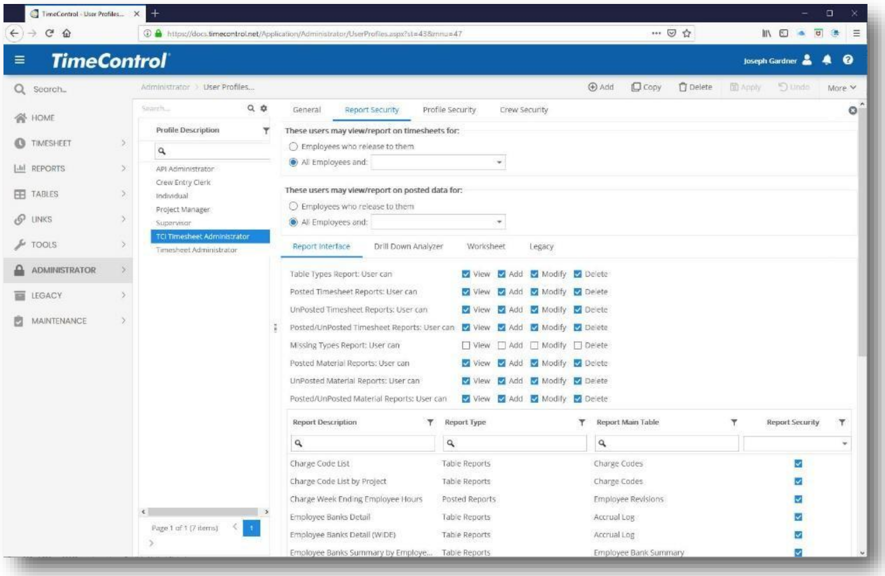
Profile Description
API Administrator
Crew Entry Clerk
Individual
Individual TCProject user
Project Manager
Supervisor
TCi Timesheet Administrator
Timesheet Administrator

Page 1 of 1 (8 items)

Menu Name	Menu Security
TimeControl Project	☑
Tools	☑
My Account	☑
Update License Key	□
Change TS Ownership	□
Missing TS Notification	□
Dashboard	□
Timesheet AutoFill	□
Announcements	□
Timesheet Creation	□
Accruals	□
Administrator	□
System Preferences	☑
Filters...	☑
User Profiles...	☑
Validation Rules...	☑
Workflow	☑
Release Structure Updates	☑
Posting Procedures	☑
Menu Entry	☑

The Menu Security area can be defined at any level of the menu. Top level entries result in that entire tree of the menu structure to be made invisible. If a particular user requires use of a menu item somewhere in the tree (for example just one of the tables), each other item in that area must be made invisible.

The Report Security works just like the Menu Security area except that it occurs at the report listing level. This allows an administrator to give access to some report but not all reports and define the access, report by report. Remember, that the Data Security already discussed comes into effect whenever a report is offered. This ensures that even if a report format is available to a user, they will not be able to see data to which they do not have rights.



Profile Description
API Administrator
Crew Entry Clerk
Individual
Project Manager
Supervisor
TCi Timesheet Administrator
Timesheet Administrator

Page 1 of 1 (7 items)

These users may view/report on timesheets for:

○ Employees who release to them
● All Employees and:

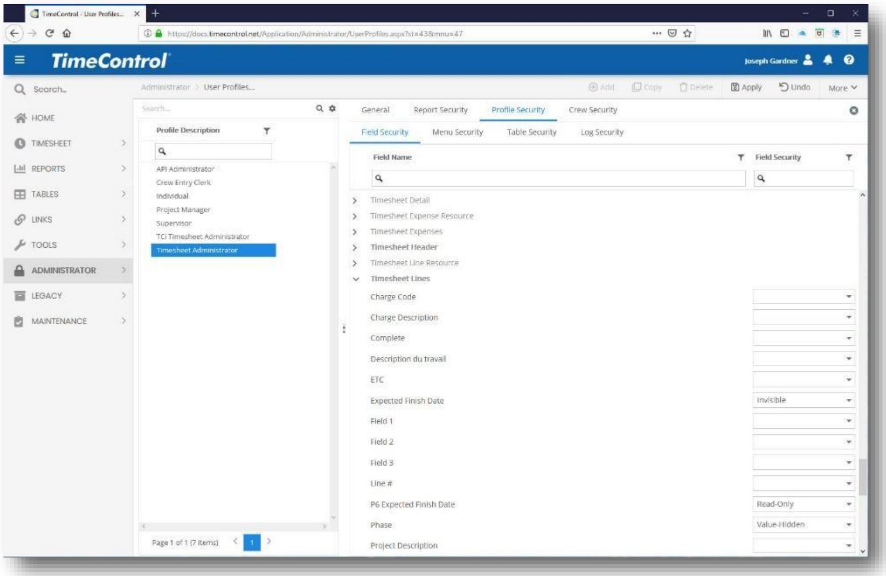
These users may view/report on posted data for:

○ Employees who release to them
● All Employees and:

Table Types Report: User can	☑ View	☑ Add	☑ Modify	☑ Delete
Posted Timesheet Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete
UnPosted Timesheet Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete
Posted/UnPosted Timesheet Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete
Missing Types Report: User can	□ View	□ Add	□ Modify	□ Delete
Posted Material Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete
UnPosted Material Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete
Posted/UnPosted Material Reports: User can	☑ View	☑ Add	☑ Modify	☑ Delete

Report Description	Report Type	Report Main Table	Report Security
Charge Code List	Table Reports	Charge Codes	☑
Charge Code List by Project	Table Reports	Charge Codes	☑
Charge Week Ending Employee Hours	Posted Reports	Employee Revisions	☑
Employee Banks Detail	Table Reports	Accrual Log	☑
Employee Banks Detail (WIDE)	Table Reports	Accrual Log	☑
Employee Banks Summary by Employe...	Table Reports	Employee Bank Summary	☑

The last area is quite unusual in an application like TimeControl. It allows security to be established field-by-field. The Field Security area of TimeControl allows virtually any field to be declared Read-only, Value-hidden, or Invisible. Declaring the field “Read-only” makes the field non-editable in any table where it is displayed for this user. Declaring it “Value-hidden” leaves the field visible buy won’t show the value within the field. This will also result in data not being displayed for this field if the field is contained in a report run by this user.



Profile Description
API Administrator
Crew Entry Clerk
Individual
Project Manager
Supervisor
TCi Timesheet Administrator
Timesheet Administrator

Field Name	Field Security
Timesheet Detail	
Timesheet Expense Resource	
Timesheet Expenses	
Timesheet Header	
Timesheet Line Resource	
Timesheet Lines	
Charge Code	
Charge Description	
Complete	
Description du travail	
ETC	
Expected Finish Date	Invisible
Field 1	
Field 2	
Field 3	
Line #	
P6 Expected Finish Date	Read-Only
Phase	Value-Hidden
Project Description	

Declaring a field “Invisible” makes not only the field, but also the field’s label to not be displayed. If the field exists in a report definition, the field column and data will be suppressed at run time when run by a user with this restriction.

Here’s an example, of where Field Security might be critical:

TimeControl supports approximately 1300 rate codes per employee. For each rate code, TimeControl maintains 2 values. These values are often used to track internal costs such as actual salaried costs vs. external costs such as billing or project costs. A project manager might be given access to the external cost fields within the rate table but not be allowed to scroll through the rates to see the salaries of all the employees. For the project manager, the 2nd field would be made invisible. Yet a human resources employee might be given access to the rates table to update the actual salaried costs. For this person, the project field would be made read-only to ensure the billing value would not be updated inadvertently.

24x7 Monitoring of TimeControl Online

As an online service, TimeControl can be accessed by users from anywhere in the world in any time zone possible. We use multiple monitoring services to check on TimeControlOnline 24 hours a day, 7 days a week and, in the case of an emergency, automatically update key HMS staff regardless of the time.

Amazon Monitoring

Amazon's EC2 provides a service called CloudWatch which HMS uses to monitor the health of the TimeControlOnline environment. The service currently makes available 26 different metrics. HMS uses the Cloud Watch service to monitor the TimeControlOnline service in real-time for events such as the stoppage of service as well as the server experiencing overload from, for example, denial of service attacks which Amazon might not have intercepted. Alarms from CloudWatch generate emails which are sent to the 3 HMS Staff with the authority to access the server and determine the nature of the difficulty.

Independent Monitoring Service

In the event that a problem with Amazon that would have TimeControlOnline not be available has also affected the Amazon CloudWatch service, HMS uses an independent monitoring tool to check on the availability of TimeControlOnline 24 hours a day. This service is capable of determining if a key page has been manipulated and if that page is being served at a reasonable speed. Any variant from this results in emergency emails to key HMS personnel who can intervene regardless of the time.

TimeControl’s API and the TimeControl Mobile App

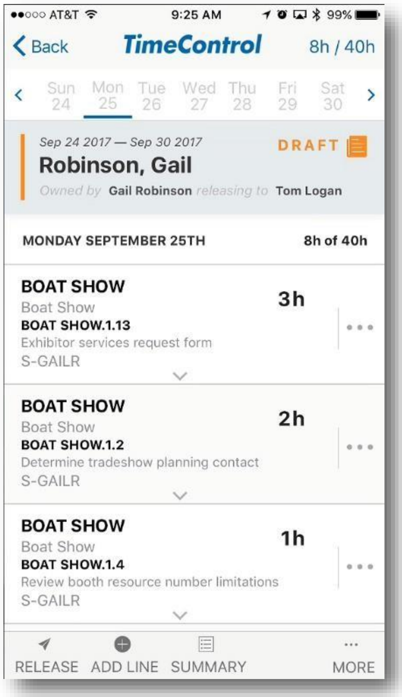
TimeControl includes both a Application Programmable Interface (API) and a Mobile App.

TimeControl’s RESTful API

The TimeControl API is built to allow users to interact with TimeControl resources programmatically. The TimeControl API serves two purposes: Programmatic access to selected elements of TimeControl’s data and process as well as access to the TimeControl Mobile App.

The TimeControl API can be activated or deactivated for any TimeControl Online account through the System Preferences. Then, access to the API is additionally controlled through the User Profile. This allows a client to determine if access through the API is required at all and, if so, to set up a profile for user accounts to access it. Typically, a single user or a small number of users are created specifically for the purposes of accessing the API and then authentication for those users is handled in the same way any other user is authenticated but in this case, the authentication is activated programmatically.

The user which is used to access the API will have access to the data that the User Profile defines. So, if API integration is desired but only for certain tables or certain types of actions (for example, adding Employee records only or reading posted timesheets only) then that can be defined in the User Profile associated to the user account that is accessing the API.



Sep 24 2017 — Sep 30 2017
Robinson, Gail
Owned by Gail Robinson releasing to Tom Logan

MONDAY SEPTEMBER 25TH 8h of 40h

BOAT SHOW 3h
Boat Show
BOAT SHOW.1.13
Exhibitor services request form
S-GAILR

BOAT SHOW 2h
Boat Show
BOAT SHOW.1.2
Determine tradeshow planning contact
S-GAILR

BOAT SHOW 1h
Boat Show
BOAT SHOW.1.4
Review booth resource number limitations
S-GAILR

Traffic through the API is encrypted using TimeControl’s SSL.

The TimeControl Mobile App

TimeControl includes a free Mobile App for use by any TimeControl user with an active license. The App supports both IOS and Android devices and can be downloaded from the Apple App Store or Google Play by searching for “TimeControl Mobile”.

Enabling TimeControl Mobile App access to TimeControl is done by the Administrator in System Preferences. Then access for users is controlled within User Profiles. This allows configurations where some users are allowed to use the TimeControl Mobile App while others are not.

Authentication of the TimeControl Mobile App uses either TimeControl’s internal authentication or corporate LDAP systems. Security access of TimeControl Mobile App features is
controlled by the access of that user. If they have data restrictions in User Profiles, they will have the same restrictions in the Mobile App.

GDPR and UK GDPR – General Data Protection Regulation

On May 25th, 2018, new laws in the European Union called the General Data Protection Regulation (GDPR) came into effect. These rules affect anyone who is from the European Union counties and as a result, anyone who uses TimeControl Online on behalf of their company. In 2021, The United Kingdom adopted the UK GDPR following its exit from the European Union. The TimeControl Online service is fully GDPR and UK GDPR compliant.

As required by the GDPR and UK GDPR regulations, the TimeControlOnline Subscription Agreement includes specific information and guarantees of what will be done with data that includes any personal data of European or British citizens. HMS discloses in the Agreement where data is stored and what sub-processing firms have access to that data and how that data is protected. Further, HMS does not move data between countries for processing.

Prospective Clients who are considering TimeControl Online can request an up to date copy of the TimeControl Master Subscription Agreement including the Addendum contain the TimeControl GDPR and UK GDPR policies. Existing clients can see the TimeControl Online Subscription Agreement and its Addendum directly in the TimeControl application.

Data Location Services

Since the adoption by the European Union of the General Data Protection Regulation (GDPR) and the subsequent adoption of the UK GDPR by the United Kingdom, HMS has offered a “Data Location Option” for TimeControl data to be located and processed in one of a number of countries to comply with local privacy regulations.

Data Location isn’t critical for all organizations. TimeControl is fundamentally a service that is provided on a business-to-business basis directly to organizations rather than directly to clients. However, for organizations where data location is critical, the Data Location Service can be critical.

HMS currently offers their Data Location Service as an annual option to the TimeControl Online subscription system. Currently, HMS offers data locations offered in the US, Canada, the UK, Europe and Australia but other locations are possible.

TimeControl Online is leveraged through Amazon Web Services. TimeControl Online is designed as a multi-server environment so locating data in one of Amazon’s many data centers while maintaining the underlying architecture and security is straightforward from a technical standpoint.

The Data Location Option of TimeControl Online is available to any client on an annual basis. Fees differ based on the number of users and location selected. If this option is important to you please contact an HMS implementation specialist at info@hms.ca.

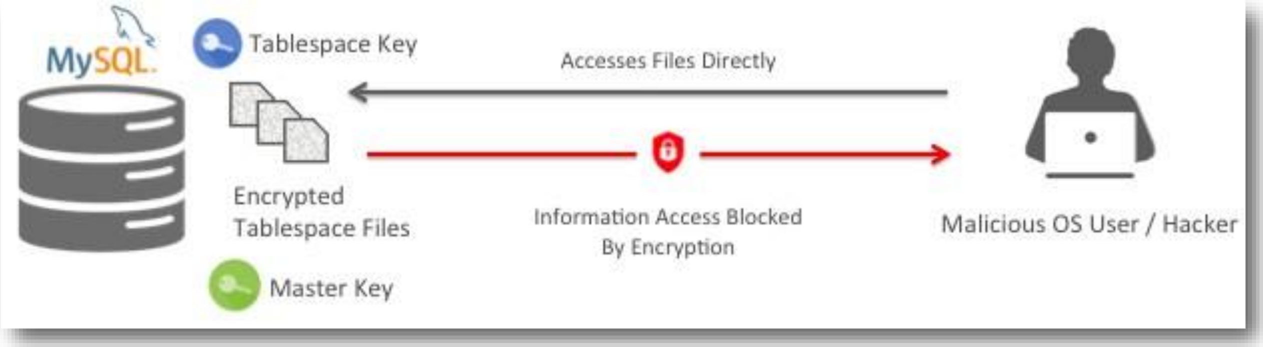
Data Encryption in Transit

TimeControl Online encrypts data in transit using a 2048-bit length private key SSL certificate.

Data Encryption at Rest

TimeControl Online has an option to encrypt data at rest. This option is managed through MySQL. When data is encrypted using MySQL, the TDE features of Enterprise Security and encrypt all tablespace and database files.
The MySQL Enterprise Transparent Data Encryption (TDE) protects critical data by enabling data-at-rest encryption in the database. It protects the privacy of information, prevents data breaches and helps meet regulatory requirements including:

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- California Consumer Protection Act (CCPA)



Data at Rest Encryption

MySQL Enterprise TDE enables data-at-rest encryption by encrypting the physical files of the database. Data is encrypted automatically, in real time, prior to writing to storage and decrypted when read from storage. As a result, hackers and malicious users are unable to read sensitive data from tablespace files, database backups or disks. MySQL Enterprise TDE uses industry standard AES algorithms.

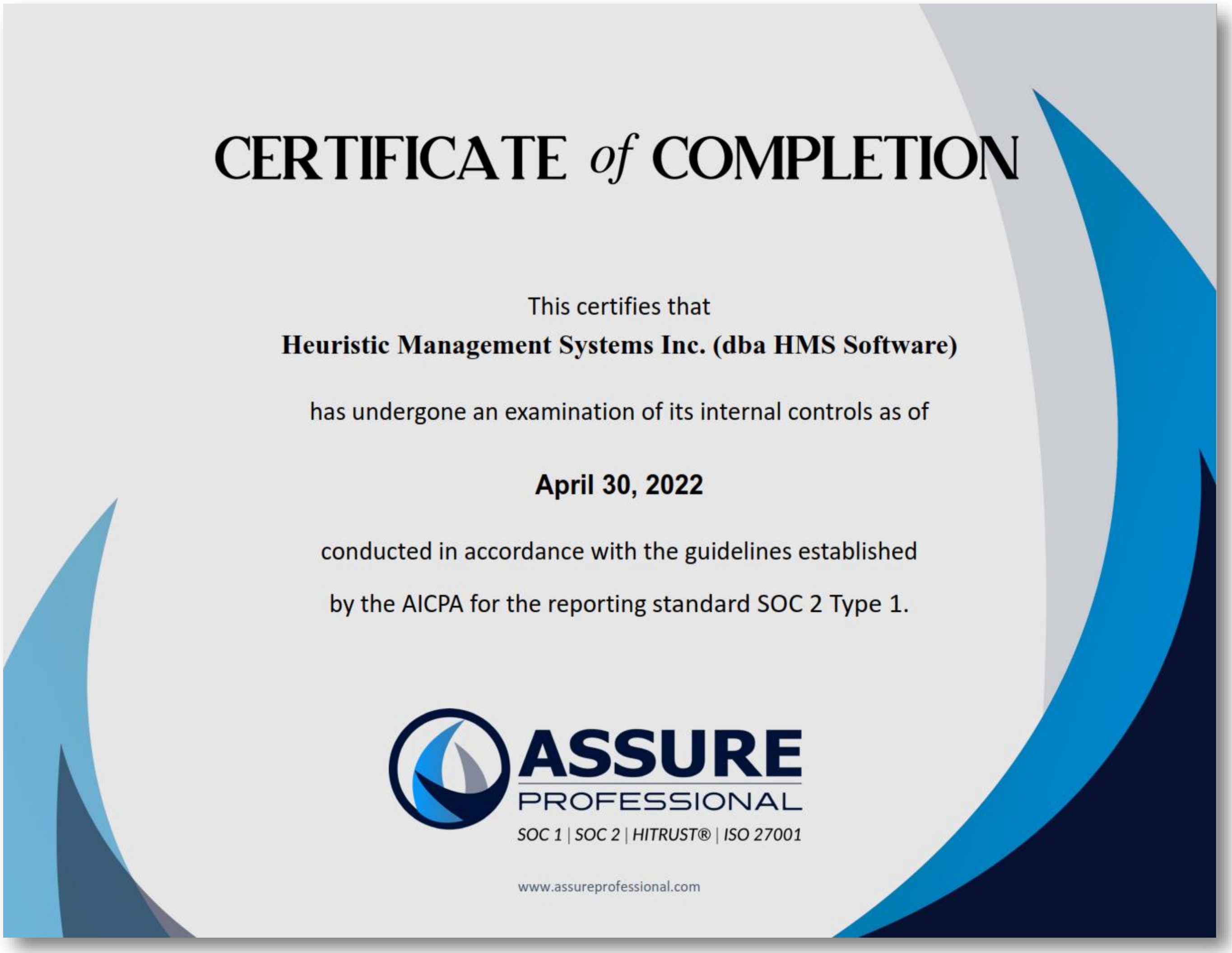
Encryption Key Management and Rotation

MySQL Enterprise TDE uses a two-tier encryption key architecture, consisting of a master encryption key and tablespace keys providing easy key management and rotation. Tablespace keys are managed automatically over secure protocols while the master encryption key is stored in the AWS Key Management Service (KMS) centralized key management solution.

The AWS Key Management Service (KMS) (AWS KMS) is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

Third Party SOC Certification

HMS successfully completed a SOC II, Type 1 audit as of April 30th, 2022. The Auditors were Assure Professional (assureprofessional.com) who worked on the audit between December 2021 and April 2022. A copy of the successful audit letter from Assure Professional can be provided to prospective or existing clients who complete a Non-Disclosure agreement with HMS.



CERTIFICATE *of* COMPLETION

This certifies that

Heuristic Management Systems Inc. (dba HMS Software)

has undergone an examination of its internal controls as of

April 30, 2022

conducted in accordance with the guidelines established

by the AICPA for the reporting standard SOC 2 Type 1.

ASSURE PROFESSIONAL

SOC 1 | SOC 2 | HITRUST® | ISO 27001

www.assureprofessional.com

Common Security Questions and Answers

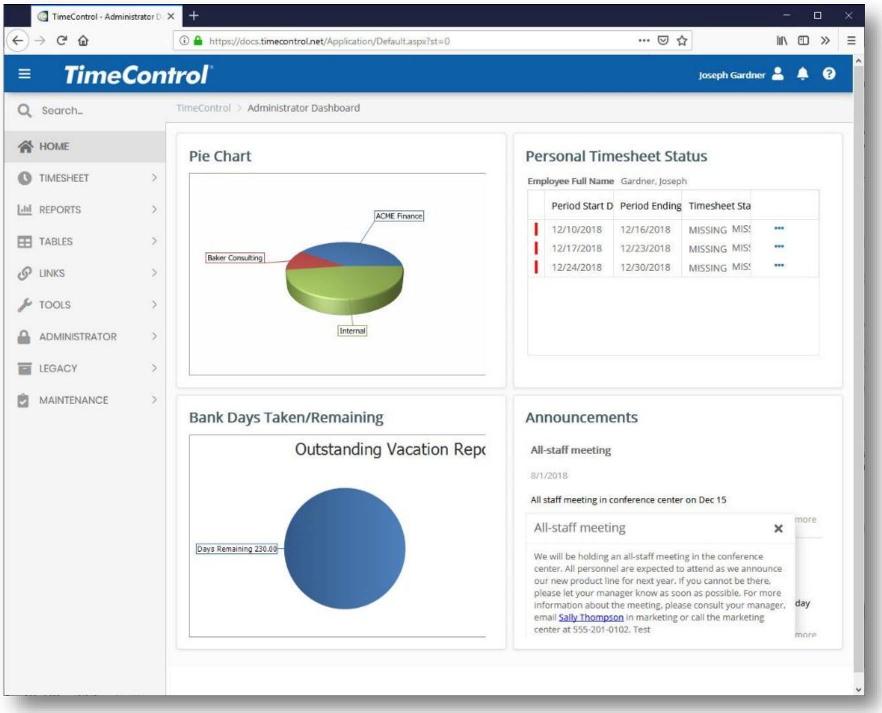
HMS responds regularly to security questionnaires from existing and prospective clients. Here are some of the most common questions and our answers.

#	Question	HMS
Security		
1	Does your organization have a Security Incident Response Plan?	Yes
2	Does your organization have a vulnerability management process in place including regular security patches? Does it include an emergency security patch process?	Yes and Yes
3	Does your organization conduct 3rd party penetration tests on a regular basis?	Yes
4	Does your organization have a formal process in place to continuously monitor security and availability of applications and services?	Yes
5	Does your organization have a process for managing employee access to systems and data including access requests, changes and deletions?	Yes
6	When an employee leaves the company, are the employee's user accounts and passwords immediately revoked.	Yes
7	All passwords stored on network devices and systems are encrypted.	Yes
8	Employees, administrators, or third parties access the network remotely, are configured with a unique username and password and with encryption and other security features turned on.	Yes
9	Does your organization have firewall configuration policies and procedures in place to protect all types of data including sensitive and confidential? i.e. switches, wireless access points, routers etc.	Yes
10	Are your systems protected by a properly configured and maintained firewall using a default deny posture that ensures only authorized users are allowed access.	Yes
11	Is TimeControl data protected by a firewall between the internet and the	Yes

	data presentation server with another firewall between the presentation and application server?	
12	Do the firewalls log all access to all servers containing TimeControl Online data?	Yes
13	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration	Yes
Privacy		
14	Does HMS have a formal Privacy Plan?	Yes
15	Does HMS have a process for notifying TimeControl Online clients, if a privacy incident has occurred that impacts their users?	Yes
16	Is sensitive and/or confidential data securely disposed of when no longer needed?	Yes
17	Is access to sensitive or confidential data restricted for users on a need-to-know basis?	Yes
Business Continuity		
18	Does HMS have a formal Business Continuity Program?	Yes
19	Does HMS perform regular reviews of the Business Continuity program?	Yes
20	Has HMS identified critical business processes and the resources required to support the continuity and/or recovery of the organization?	Yes
21	Does HMS have a strategy and plan to maintain critical business processes and resources, if its facilities are not available?	Yes
22	Does HMS have a Pandemic Plan?	Yes
23	Does HMS maintain and review its Business Continuity Plan and Program regularly?	Yes
24	What is the Recovery Time Objectives for critical processes / technology?	Yes
25	Does HMS have a Disaster Recovery Plan?	Yes

About TimeControl, the multi-purpose timesheet

In today's economy, tracking productivity is more important than ever. It is no longer enough to know only how much time has been spent. Now management demands that you know what was done with the time. Many organizations are turning to project and task based management as a way of being more effective. One of the most difficult aspects of implementing project control is the capture and approval of labor actuals. *TimeControl* provides an electronic timesheet system designed to serve both Finance and Project Management


TimeControl - Administrator D
https://docs.timecontrol.net/Application/Default.aspx?st=0
TimeControl
Joseph Gardner
Search...
TimeControl > Administrator Dashboard
HOME
TIMESHEET
REPORTS
TABLES
LINKS
TOOLS
ADMINISTRATOR
LEGACY
MAINTENANCE
Pie Chart
ACME Finance
Baker Consulting
Internal
Personal Timesheet Status
Bank Days Taken/Remaining
Outstanding Vacation Repo
Days Remaining 230.00
Announcements
more
day
more

Employee Full Name Gardner, Joseph

	Period Start D	Period Ending	Timesheet Sta	
❙	12/10/2018	12/16/2018	MISSING MIS	•••
❙	12/17/2018	12/23/2018	MISSING MIS	•••
❙	12/24/2018	12/30/2018	MISSING MIS	•••

All-staff meeting

8/1/2018

All staff meeting in conference center on Dec 15

All-staff meeting ✕

We will be holding an all-staff meeting in the conference center. All personnel are expected to attend as we announce our new product line for next year. If you cannot be there, please let your manager know as soon as possible. For more information about the meeting, please consult your manager, email Sally Thompson in marketing or call the marketing center at 555-201-0102. Test

Subscribe in the Cloud Online or Install on-premises

TimeControl is available both as a subscription model with our Timesheet as a Service TimeControlOnline or as a purchasable license to be installed on your premises. You can find out more about our online subscription at www.timecontrol.net.

Multi-lingual

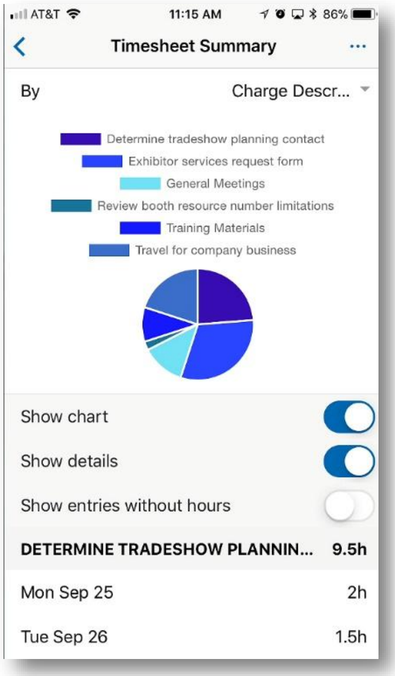
We know that not every user speaks English as their first language. TimeControl comes with a number of languages already in the system but every label and every message is open to the TimeControl Manage Languages module so you can change the existing translations or even add your own. This is a great feature for adjusting terminology in the system to match your organization's (The only word you can't change is: "TimeControl").

Easy to use web interface

TimeControl's interface is browser-based and user-intuitive. User Profiles determines what the user will be presented with and the user can define where TimeControl should start and what defaults they wish. End users can use a variety of browsers such as Internet Explorer, Firefox, Chrome, Safari, or Mozilla.

Free TimeControl Mobile App

TimeControl includes a free Mobile App available from the Apple App Store for iOS devices and Google Play for Android devices. Enter timesheet hours and expenses you can even manage approvals. When linked to TimeControl Industrial or TimeControl Industrial Online, you can also add Crew Timesheets and Material consumption.


AT&T
11:15 AM
86%
Timesheet Summary
···
Determine tradeshow planning contact
Exhibitor services request form
General Meetings
Review booth resource number limitations
Training Materials
Travel for company business

By: Charge Descr...

Show chart: on

Show details: on

Show entries without hours: off

DETERMINE TRADESHOW PLANNIN...	9.5h
Mon Sep 25	2h
Tue Sep 26	1.5h

Timesheet Approvals

TimeControl supports HMS Software's unique Matrix Approval Process for Labor Actuals which allows for quick authorization of project data. This process resolves the inherent conflict that is found when both the financial and project management hierarchies must approve timesheet data simultaneously. Automated validation of timesheet data is handled by TimeControl's remarkable Validation Rules . Additional approvals can be done manually with a simple Approve/Reject or Approve/Update process. The Project Manager Validation screen displays an easy-to-view hierarchical interface for managing project approvals.

Total Flexibility with User Profiles

TimeControl's User Profiles allows the Administrator to determine which menu choices, reports and fields are accessible by each user. The entire interface can be tailored to the user's individual needs. No other system on the market today offers this much flexibility.
Field level security ensures that only the information which is important to each user, is displayed. Fields can be made read-only or invisible, removing them from view entirely. This makes *TimeControl* at once a secure, deployable system and an easy-to-use one as well.

Links to Project Management Systems

TimeControl includes direct links to project management systems including Oracle-Primavera Pro and EPPM, Microsoft Project, Project Server, Project Online and Project for the Web, JIRA, Deltek's Open Plan and Cobra, ARES PRISM, InEight's Hard Dollar, BrightWork and SharePoint. In fact, multiple products and versions can be supported simultaneously.

Integrating with a project management system drastically reduces timesheet errors as only valid tasks will be available in which to charge time. Hours entered in *TimeControl* are returned directly to the project management system as activity and resource progress.
TimeControl also supports customizable export formats for integration with virtually any financial or HR system.

Vacation Approvals with TimeRequest™

The TimeRequest module allows users to make a request for certain types of times to be approved for entry in future timesheets. The most common application of this module may be for requesting Vacation time off. Once approved, the time is then automatically entered by *TimeControl* into the appropriate future timesheet.

The TimeRequest module is, however, not restricted to just Vacation requests. Any category of time can be exposed to the module. This allows an infinite number of applications such as for travel time, training time, offsite or onsite time or any other type of time category where the organization wishes it to be approved in advance.

E-mail Enabled

TimeControl allows email notifications to be sent for various events such as missing timesheets, incomplete or non-approved timesheets as well as timesheets that were rejected or re-released for approval.

Expense Reports

TimeControl includes extensive expense report functionality. Users can enter an unlimited number of expense report items for each timesheet line.

Links to Payroll, HR and ERP/Finance

TimeControl is designed with a Links module that lets you define links to corporate systems and software including Payroll software or online services, Human Resources systems and ERP/Finance systems.

Using TimeControl to fulfill the requirements of not only project management but also Finance, HR and Payroll means you can eliminate the costs and inefficency of mlutiple timesheets.

Reporting

TimeControl's reporting engine looks just like Excel™. Reports can even be saved in Excel or HTML format.
TimeControl's Reporting Wizards make report generation easy. *TimeControl's* field-level security is always active so only the fields which a user has permission for will be shown. Predefined reports are available in a variety of formats which include posted timesheet data, table lists, printouts of the timesheets themselves and missing timesheet reports.

For more information

For a more complete description of TimeControl and its features, visit TimeControl.com. To try the timesheet system for free, visit freetrial.timecontrol.com.

About HMS Software

HMS Software, a division of Montreal, Canada-based Heuristic Management Systems Inc., is a leading provider of enterprise timesheet and project management systems.

Founded in 1984, HMS Software's expertise in implementing enterprise project-management and enterprise timesheet systems is recognized worldwide by some of the world's best-known organizations. HMS's signature product, TimeControl, an enterprise timekeeping system designed to serve the needs of both Finance and Project Management, is distributed worldwide through an extensive list of distributors and dealers located on every continent with representatives in the US, the UK, Australia, Mexico, Europe, Asia, South Africa and the Middle East.

HMS Software's client list includes some of the world's leading corporations in the telecommunications, IT, finance, engineering, defense/aerospace and government sectors including such organizations as AMD, Azuria Water Solutions, CANAM, CAE, EXFO, Foster Wheeler, Interpol, Kelly Services, the Government of Quebec, Pontoon Solutions, Progress Rail, Reebok-CCM, Rolls Royce, Sandoz, SEFA, Volvo Novabus, Zoetis and hundreds of others. HMS is headquartered in Montreal, Quebec, Canada.
For more information about HMS, please visit www.hms.ca.

TimeControl

First published by HMS in 1994, TimeControl has been adopted hundreds of clients and over 150,000 users around the world. TimeControl is designed to serve the needs of both project and finance simultaneously. It allows an organization to use a single timesheet for project tracking, time and attendance, time and billing, HR tracking, R&D Tax Credits, DCAA and project costing instead of having to deploy many timesheets to serve these needs. TimeControl is available for purchase for an on-premises implementation or as a subscription as service. TimeControl's architecture is flexible and extensive supporting numerous databases such as Oracle, Microsoft SQL Server and MySQL, multiple browsers such as Internet Explorer, Firefox, Safari and Chrome and even includes a free Mobile App available on Google Play for Android devices and the Apple Store for iOS devices.
For more information about TimeControl please visit: Timecontrol.com.