# TimeControl®
# On Premise
# Security Architecture

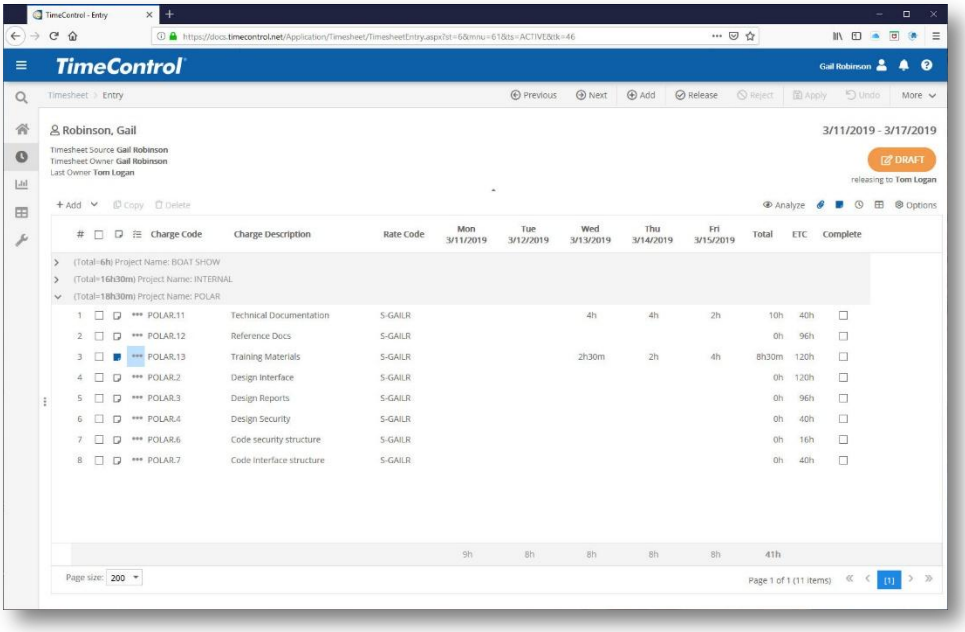
For more information contact:
**HMS Software**
189 Hymus, Suite 402
Pointe-Claire, Quebec H9R 1E9
Tel: 514-695-8122
Fax: 514-695-8121
Email: info@hmssoftware.ca
Web: www.hms.ca

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.




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 TimeControl and TimeControl Industrial for an on-premise installation and considers the design of TimeControl version 7 and higher. If you are interested in the security architecture of the TimeControl Online Software as a Service environment, then we recommend you read the white paper “TimeControl Online 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 access to,
b) protect TimeControl data from unauthorized tampering or corruption and;

c) 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.

# Database Access

TimeControl is fundamentally a database product. 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 the TCSECURE gateway database was designed to defeat this. The TCSECURE database contains a single username and password used to gain complete access to the TIMECONTROL main database where all the TimeControl data is contained. The TCSECURE data is encrypted with a method hard-coded into the TimeControl applications. This allows us to give out a username and password on machines which may require access without compromising the main database security.

When starting, the TimeControl middleware; the TimeControl Transaction Server (TTS) looks in its configuration file for the location of the TCSECURE database. It is given a username and password to access this database. Any administrator who has been given access to the TimeControl installation directories on this server will be able to read this username and password. Once the ATS or TTS has reached the TCSECURE database, it decrypts the username and password contained there to determine how to make a connection to the TIMECONTROL database. This username and password are not revealed to anyone. The only person who needs access to this data is the database administrator themselves. The TTS then establishes a connection to the database and stands by for requests from the web server via .Net communications to make a data request. All data is brokered through the middleware. End-users components are not given any knowledge of the database location and end-users never make a direct connection to the database.

This architecture allows a database administrator to allow more extensive access to the database for integration purposes without having to leave the data completely open to any user. The database administrator is assured that regular TimeControl traffic through the application is authorized and they can then grant other rights as they require. This would allow, for example, a scenario where 3rd party reporting tools could be used to create reports from TimeControl data where the end-users are given read-only direct access to only certain elements of the TimeControl data.

The TimeControl installation does not encrypt data by default. All data tables are in normalized rows and columns and accessible through SQL if the database administrator grants access to them. However, TimeControl does support the data being encrypted by internal tools to the database such as the Transparent Data Encryption offered by Oracle and Microsoft. This protects the data from unauthorized access from outside the database application through compromising the physical storage.

## Communications: .Net

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

## Web Access and SSL

The architecture of a web interface application is such that a web-server such as Internet Information Services (IIS) contains web pages (either static or database-driven) which deliver a web-page to a web-browser that requests it.

This makes life very simple for the end-user. A user is given a URL such as https://timecontrol.mycompany.com or https://timecontrol, a user name and a password. The user enters the URL into a browser such as Firefox, Safari, Edge or Chrome and is presented with the login page. The user name and password are entered and the page then connects to the TimeControl middleware to determine if access should be allowed.

One of the first security decisions to make in an on-premise installation of TimeControl is whether to make the system accessible only within the corporate firewall or make it also available outside the corporate through the Internet. A website or web application like TimeControl that is accessible through the Internet from outside the building is called "outward-facing". If TimeControl is to be used only from within the corporate firewall then the security already built into that infrastructure becomes a level of protection to the system. The security features available to outward facing sites can still be effective. If TimeControl is to be available through the Internet, then some elements of the web security design of the system are even more important.

If TimeControl is to be an outward-facing system then locating the TimeControl web server and middle ware into a protected area of the network referred to as the DMZ is critical. DMZ is a reference to "De-Militarized Zone" and in networking terms refers to an area that is connected to the corporate network but distinct to it and is referenced from the Internet in a separate area of the firewall. There are many references to how to make a secure web environment with a DMZ available.

Network and web security such as management of the .htaccess file can control access to a website or webpage to make it available with highly configurable restrictions. The security controls within IIS can also be configured to allow or deny different IPs or different Subnet masks to a given web site. This type of security can be used to ensure that only recognized machines or networks are given access to TimeControl. This configuration can be extended to deny any access to any site in the world that is not already listed in the web server's configuration.

If TimeControl is outward-facing then HMS recommends configuring the TimeControl website with a Secure Socket Layer (SSL). When this is done, all networking traffic from the outside to the TimeControl webserver is highly encrypted as it travels across the Internet. Users can identify that the TimeControl website is protected by a small lock icon that typically appears in

the browser near the URL and by the URL starting with https:// rather than http://.  In order to secure the TimeControl website, you will need to acquire a website certificate which is sold through registered and recognized suppliers.  HMS does not provide such certificates.

# Authentication: TimeControl Passwords

TimeControl includes several methods of authentication to access the system and then to determine for each action if the user has sufficient authority to perform that action.

When using the internal TimeControl password system each user is given 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 is given inadvertent access to that table, they will not be able to read the password entry for a user. You can set your own policies for passwords in the system preferences including length, requirements for numbers, special characters and upper and lower case characters.

Once the login is complete, control of TimeControl communications is now passed to the TTS. 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.

TimeControl supports extensive password policies for its internal password architecture. Configuration of the password policies are done in the TimeControl configuration files on the server and include the ability to determine password length and complexity.

# Authentication: LDAP and Windows Active Directory

Some clients will wish to control authentication to TimeControl from Active Directory or a Lightweight Directory Access Protocol (LDAP) instead of the internal TimeControl password system. TimeControl supports all of these authentication methods as well as its own security model simultaneously. This allows each user's authentication method to be defined distinctly. For example, this would allow internal corporate users to be authenticated using Active Directory and external users to have logins that are defined in the TimeControl password system.

In the TimeControl User Table, select TimeControl Security, or Active Directory / LDAP as the authentication type. You may be asked for the location of the LDAP or Active Directory Server. In addition, while now less common, Windows NT Authentication can be selected. A password needs be entered into TimeControl only if the TimeControl Security type is selected.

TimeControl will take the User name and Password combination that are used during the login and validate them according to the method selected. If the method was TimeControl Security, TimeControl will search the TimeControl User database for the encrypted password. If the method was NT Authentication, TimeControl will call check the server machine itself using the NT Authentication module, pass the User Name and Password to it and wait until the server returns a pass or fail reply. If the method was Active Directory or LDAP, TimeControl will send the User name and Password to the Active Directory or LDAP server and wait for a pass or fail.

In these scenarios, the storage, management and maintenance of the password is outside of TimeControl. This can be desirable in large organizations when the management of new users, security for various applications and security on servers etc., is a huge undertaking. TimeControl is an application that is often distributed to virtually every employee so managing authentication of TimeControl Active Directory or LDAP means one less password for employees to remember.

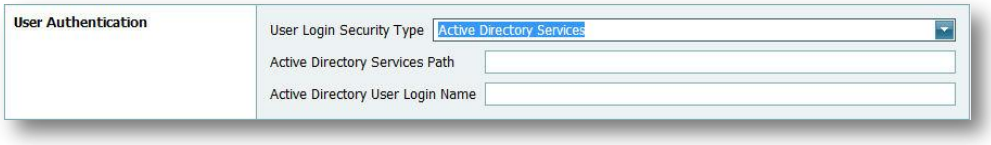
An import of information from LDAP or Active Directory can be used to populate user names for the first time when TimeControl is implemented.

Access to TimeControl is something that should be rigorously managed. Timesheets, while they take up a minimal part of one's week, can contain data that is considered among the most sensitive in the entire organization.

Entering information for a new employee in TimeControl involves more than just the user name and password. Depending on the configuration of a given implementation, numerous fields and entries might need to be populated to define a wide range of properties of that employee for reporting and analysis purposes with any timesheet data entered. Also, rate information is often entered on an employee-by-employee basis which is why functional or role-based management of TimeControl functions is controlled from within TimeControl not Active Directory.

TimeControl supports Microsoft's single sign-on authentication, otherwise known as Windows Authentication.

To activate Windows Authentication, Windows Authentication must be enabled within Internet Information Services on the Web Server. Anonymous Authentication must be turned off. The WINDOWS_AUTHENTICATION parameter in the TimeControlWeb.ini file must be turned on.




Within the TimeControl User Table users must have their authentication type set to "Active Directory Services", and their "Active Directory User Login Name" must be filled out to either DOMAIN\USERNAME, or USERNAME, or their USR_CODE must match their windows authentication username.

When Single Sign-on is enabled, users will not be presented with the TimeControl login screen. TimeControl will authenticate them automatically and move them directly into TimeControl or, if they have been designated as an alternate user for someone else, to the Alternate User screen.

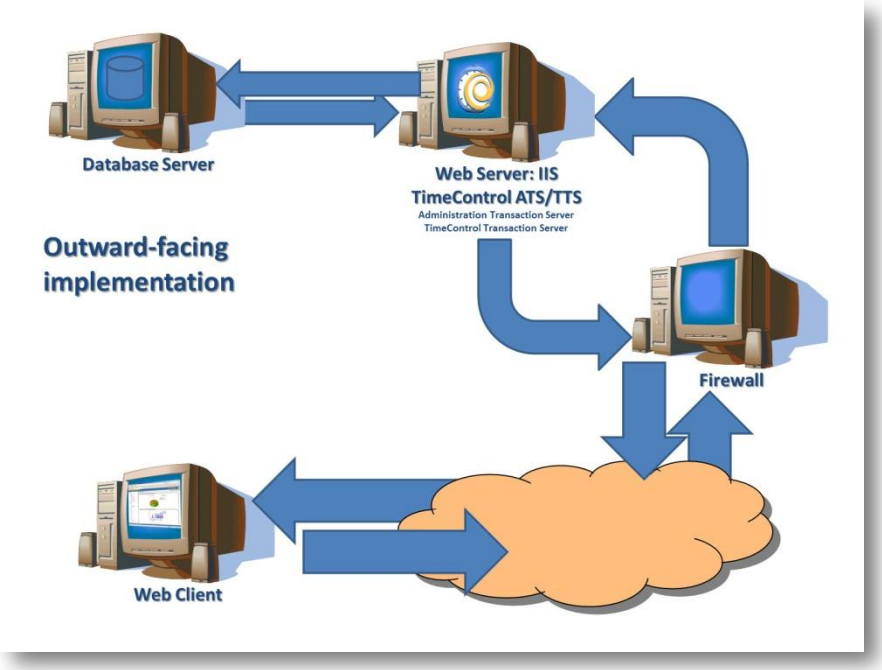
## SAML support

TimeControl supports SAML 2.0

# Middleware N-tier Architecture

Modern web-based interfaces like TimeControl have multiple levels. Each level is referred to as a 'tier'. TimeControl is an N-tier application meaning that it can have many tiers.

N-Tier design is important when we talk about security as it allows us to locate different parts of the system in different areas and restrict access to corporate data. Regardless of whether or not a firewall is implemented, end users are connected only to the internal TimeControl application website and that site is connected on to the TimeControl middle tier. Neither the users themselves nor the website is ever directly connected to the database server which allows protection of the database server to be much more stringent.




The sequence of events in accessing TimeControl is as follows:

1. The end-user web browser accesses the TimeControl login web page on the web server. Using one of the authentication methods we've already described, the user name or user name and password are entered. This information goes to the TimeControl 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 a randomized secure token session variable and 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. TimeControl uses the secure token to determine for each action if the user still has the appropriate rights to perform that function.
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.

If TimeControl has been implemented to be outward-facing, a firewall should be in use and it will filter and protect the traffic to and from TimeControl and the TimeControl webserver against intrusion.

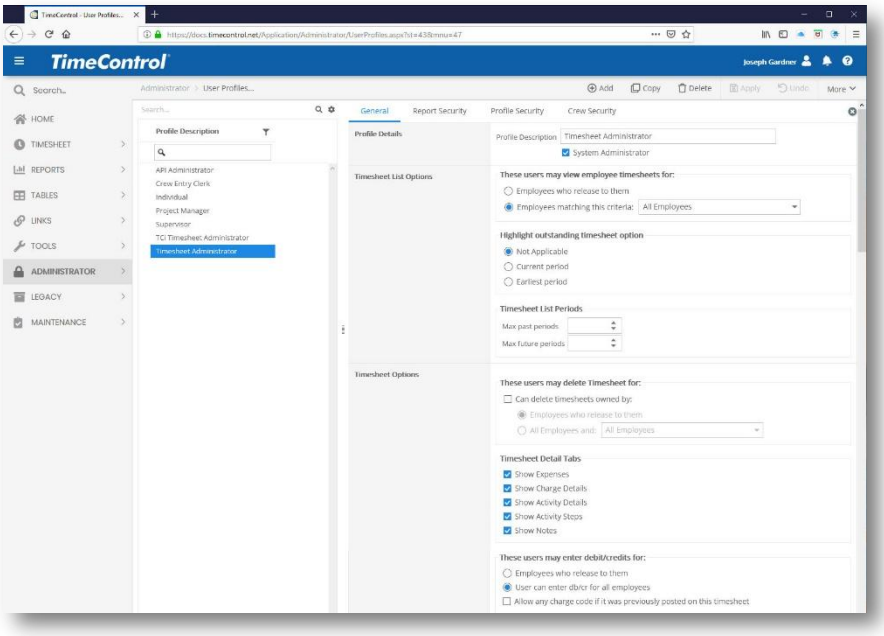
Obviously the most secure implementation of TimeControl is to disallow access to any part of TimeControl from outside the network. This can be accomplished with network and web security and blocks all access to the servers in question. If, however, you wish to allow traffic from outside the network, then the most secure implementation of TimeControl is accomplished by:

1. Having the database server not be the same machine as the middleware server
2. Have a firewall installed
3. Install the TimeControl middleware and web server into a DMZ
4. Use SSL to encrypt TimeControl web traffic
5. Aside from TimeControl middleware and web server services, run no other internet services on this machine
6. Ensure the database server access is behind the firewall and that the database server's IP is masqueraded

This creates a highly secure environment.

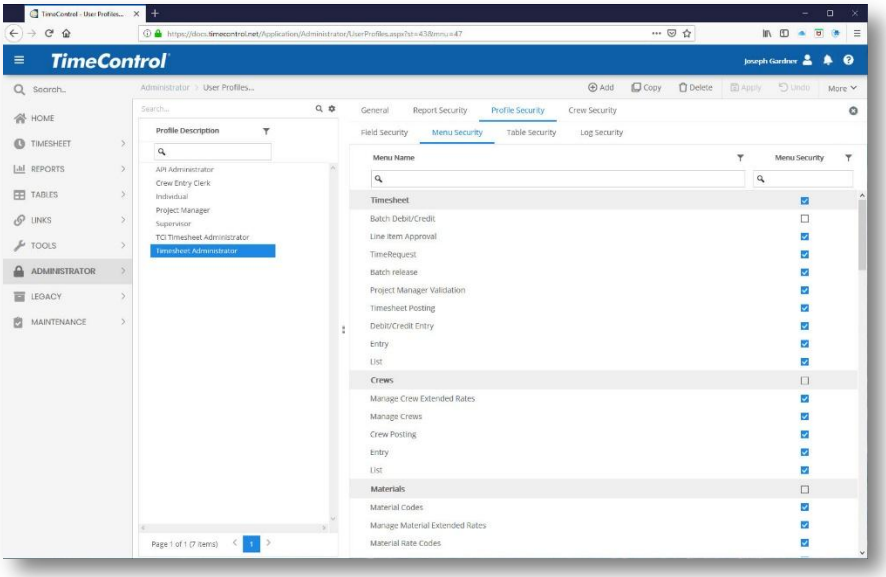
- ✓ Access to the database is insulated from the users, the web server and is highly restricted even to the middleware
- ✓ Traffic to and from the TimeControl web server is encrypted

Once in TimeControl, 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. This architecture ensures that users are not confronted with menu selections that are of no interest to them. 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.

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.



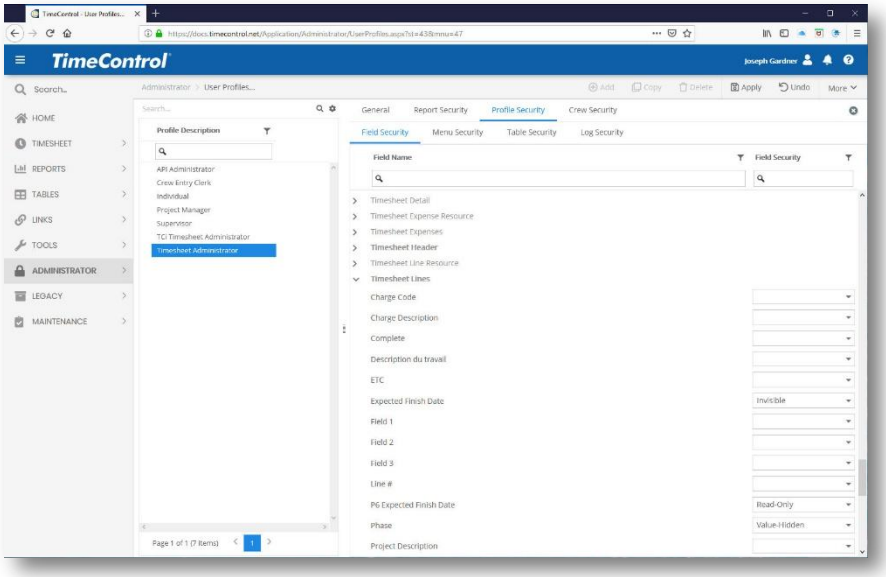

The second area of User Profiles is a lower level of detail. The Details tab controls first the functions that are available to each user. This allows an administrator to hide completely any aspect of the program including such things as table access, exporting functionality, project linking functionality,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

security is essential in such an application.

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.

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.

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.




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 an unlimited number of rate codes per employee. For each rate code by default, TimeControl maintains up to 9 values. These values are often used to track internal costs such as actual payroll costs vs. external billing 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 private pay rates of all the employees. For the project manager, the pay field values would be made invisible. Yet a human resources employee could be given access to the rates table to update the actual payroll costs. For this person, the payroll rate field would be editable but the billing rate field would be made read-only to ensure the billing value would not be updated inadvertently.

## Intrusion Detection

There are many ways that your network and website can be protected against intrusion but one of the most important things you can do for security is to identify when your site is under attack.  TimeControl logs any failed login attempts so if someone is trying to gain unauthorized access to your site through automated multiple login attempts, the log can help identify this. The failed logins are written to the TimeControl Event log in Windows and, if that log is unavailable, to the TimeControl log files.

# 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.

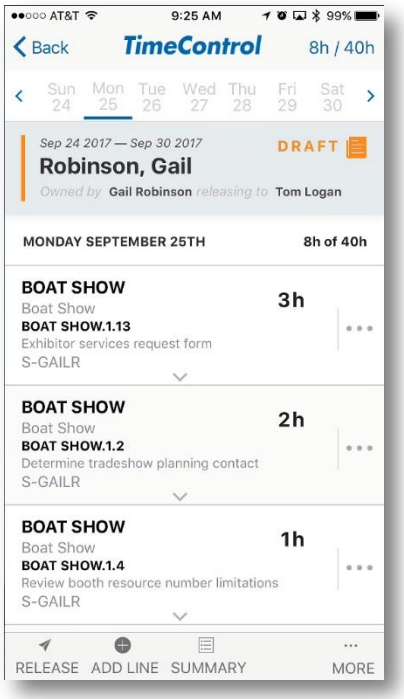
The TimeControl API can be activated or deactivated for any TimeControl Online account through the System Preferences. Then, access to the API is additionally controlled through the User Profile. This allows a client to determine if access through the API is required at all and, if so, to set up a profile 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.

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".

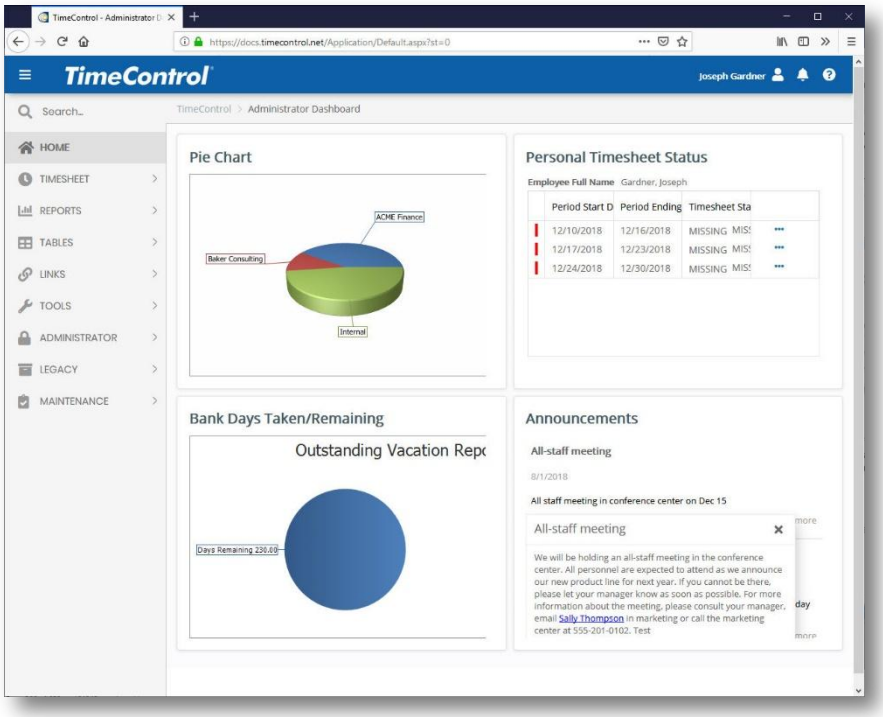



Enabling TimeControl Mobile App access to TimeControl is done by the Administrator in System Preferences. Then access for users is controlled within User Profiles. This allows configurations where some users are allowed to use the TimeControl Mobile App while others are not.

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.

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




## 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

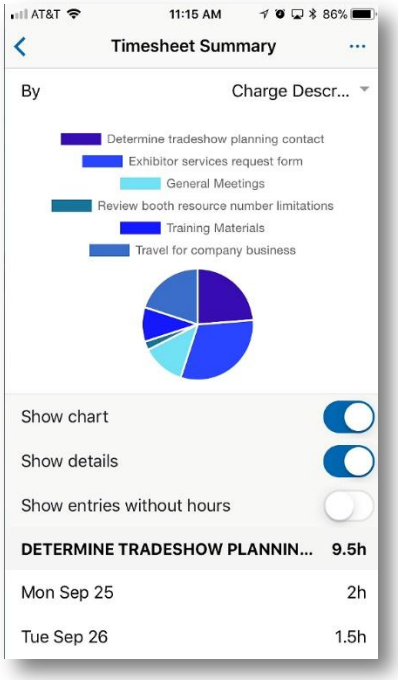
We know that not every user speaks English as their first language. TimeControl comes with a number of languages already in the system but every label and every message is open to the TimeControl Manage Languages module so you can change the existing translations or even add your own. This is a great 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.




## 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 capabilities are extensive. Reports can even be saved in Excel or HTML format.

## HMS Software

Based in Montreal, Canada, HMS Software has been a leading provider of project management and enterprise timesheet systems and services since 1984. HMS Software's first customized timesheet application was written in 1984. With the launch of TimeControl as a commercial application in 1994, HMS Software began servicing clients worldwide.

HMS Software's client list reads like a who's who of business. It includes 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. For further information about HMS Software, please visit the HMS website at: www.hms.ca or contact us at info@hms.ca.

## TimeControl

TimeControl was originally released in 1994. It was immediately successful in the project management sector and today is recognized not only as a project management solution, but also as an enterprise timesheet solution in use by companies worldwide. TimeControl is designed as a multipurpose timesheet able to serve the needs of both Finance and Project Management simultaneously. It includes features such as a multi-browser, multi-device interface, a PC and mobile interface, vacation approvals, executive dashboards, extensive approval functionality, flexible reporting and links to project management and corporate systems which makes the timesheet product ideally suited for integration with existing systems in any organization. TimeControl's flexibility allows it to be deployed for use as a time and attendance, time and billing, project tracking and flex-time system. TimeControl and TimeControl Industrial are available both as an on-line subscription in the Cloud and for purchase for an on-premises installation. TimeControl Project is a premium version of the TimeControl Online and TimeControl Industrial Online subscription service in the cloud.

For more information about TimeControl, TimeControl Industrial and TimeControl Project, monitor the TimeControl blog at blog.timecontrol.com, or the main TimeControl website at www.timecontrol.com.