

TimeControl Security Architecture

An HMS Technical White Paper

Our Mission:

Heuristic Management Systems
is a leading-edge provider of
high-quality, enterprise-wide
solutions for project-oriented
environments

For more information contact:

HMS Software

1000 St-Jean, Suite 200

Pointe-Claire, Quebec H9R 5P1

Tel: 514-695-8122

Fax: 514-695-8121

Email: info@hmssoftware.ca

Web: www.hmssoftware.ca



TABLE OF CONTENTS

Overview	1
Database Access	2
Web Access and SSL	3
Password encryption	4
Middleware n-tier Architecture.....	5
Proxy Servers and Firewalls.....	8
LDAP and Windows Active Directory	10
User Profiles.....	12
About HMS Software.....	15

HMS has been designing corporate timesheet systems since its first project in 1983. Our clientele has always been corporate-based project-oriented clients, usually from Fortune 1000-type companies and in these environments, security is a critical concern. Many of our clients are financial firms such as the Credit Suisse/First Boston Bank or Defense/Aerospace clients such as Canadair or Rolls Royce. For these firms, managing the security of sensitive corporate data is always a serious concern.

Of any data for which the security is important, timesheet data is often considered the most sensitive. If used for payroll, timesheet data contains the salary costs per employee. If used for project management, timesheet data reveals the true actual costs of accomplishing elements of work. In the wrong hands, this data has the potential to cause heartache for management of the organization.

This paper will outline the various aspects of security of TimeControl data. We will look at different perspectives here including database architecture, data encryption, TimeControl communication layer architecture, TimeControl functionality architecture, working across the Internet and discuss related topics of interest such as firewalls, proxy servers, integrating with other access services such as LDAP and Active Directory.

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

Over this paper, we will be discussing different aspects of security in TimeControl Express, Professional and Enterprise. For more complete information on the differences between these three editions of TimeControl, consult the TimeControl Differences white paper on the TimeControl website at www.timecontrol.com.

The fundamental driving force behind 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 other corporate resources.

DATABASE ACCESS

When all is said and done, TimeControl is fundamentally a database product. It has few calculations and is mostly 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 comprimizing the main database security.

When starting, the TimeControl middleware; the Administration Transaction Server (ATS) and/or the Java Transaction Server (JTS) starts up and looks in its startup definition 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 ATS or JTS directories on this server will be able to read this username and password. Once the ATS or JTS 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 ATS and/or JTS then establish a persistent connection to the database and stand-by for requests from the client-access controls such as a TimeControl applet or ActiveX component to make a data request. All data is brokered through the middleware. End-users components are not given any knowledge of the database location. 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. The database administrator is not concerned that there is data access to the TimeControl data aside from regular TimeControl traffic that is not authorized. 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.

TimeControl has 3 different interfaces available: A Windows interface client which does not require a web browser, a Windows-based Web interface and a Java-based Web interface for other hardware client environments such as UNIX and Macintosh. We'll be discussing the 2 web-based interfaces here.

The architecture of a web interface is such that a web-server such as Internet Information Services (IIS) or Apache contain 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 `timecontrol.mycompany.com`, a user name and a password. The user enters the URL into a browser such as Internet Explorer and is presented with a login page. The user name and password are entered and the page then connects to the TimeControl middleware to determine if a login should be allowed.

We'll discuss the communications and control of TimeControl itself later in this paper. It's important to remember, however, that access to this first TimeControl login page itself can be controlled through standard-types of Web security.

First of all, Network security or web security such as `.htaccess` can control access to a page to make it available with certain restrictions. Each web server is a little different and TimeControl Enterprise supports several. TimeControl Express, Professional and Enterprise all support Microsoft's IIS web server. Whatever the version of TimeControl you are installing and whatever the web server you are using, the security controls within a web site allow at a minimum to allow or deny different IPs or different Subnet masks to a given web site. This security could be used to ensure that company users who are on the corporate network only are given access to the TimeControl front page. This security can be extended to the entire Internet so that anyone who tries to get access to the corporate TimeControl site itself will be denied even seeing the log in screen until they enter the right user name and password to do so.

In addition, this can be combined with storing the TimeControl login areas in an SSL (Secure Socket Layer) area of your website. This technology is virtually universally supported by web servers and results in all traffic to and from the page being encrypted by the web server. This is only important within TimeControl for the movement of the login page itself and the user name and password during log in. Once a user is logged into the system, internal security takes over and all data is encrypted.

PASSWORD ENCRYPTION

Okay, so you've got access to the TimeControl login page and now TimeControl would like to determine if you should be granted access to the application at all.

Depending on which edition of TimeControl you've installed, communications is now passed either to the ATS or to the JTS either directly or the web server. TimeControl determines through its User profiles what menu items you should have access to and presents a menu with only those items.

Each user is given access to TimeControl based on a user name and a password. Within the TimeControl database a table is maintained of these values. The password values are encrypted within the database so that even if someone is given casual access to that table, they could not easily determine the password value for a user.

User name / password combinations are stored as temporary "session variables" by the web server for as long as the browser session is active. Once logged in, the user name and password are only transmitted back and forth in an encrypted form.

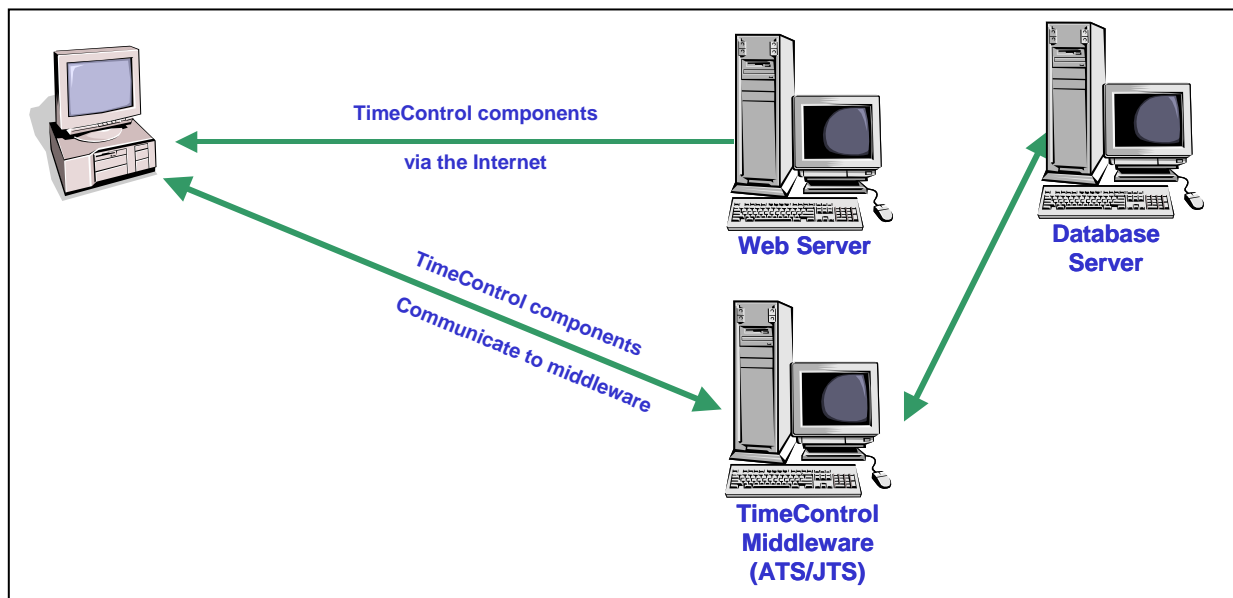
When each TimeControl component is accessed by the user, TimeControl determines if the session variable user name / password is still appropriate for this component. If so, it displays the component to the user. This prevents end users from trapping a full component URL then trying to access it later with a user name and password which should no longer deliver the component to the end-user.

Session variables 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 Web Properties file of the TimeControl server components

MIDDLEWARE N-TIER 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.

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 Enterprise 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 Administration Transaction Server (ATS) middleware 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

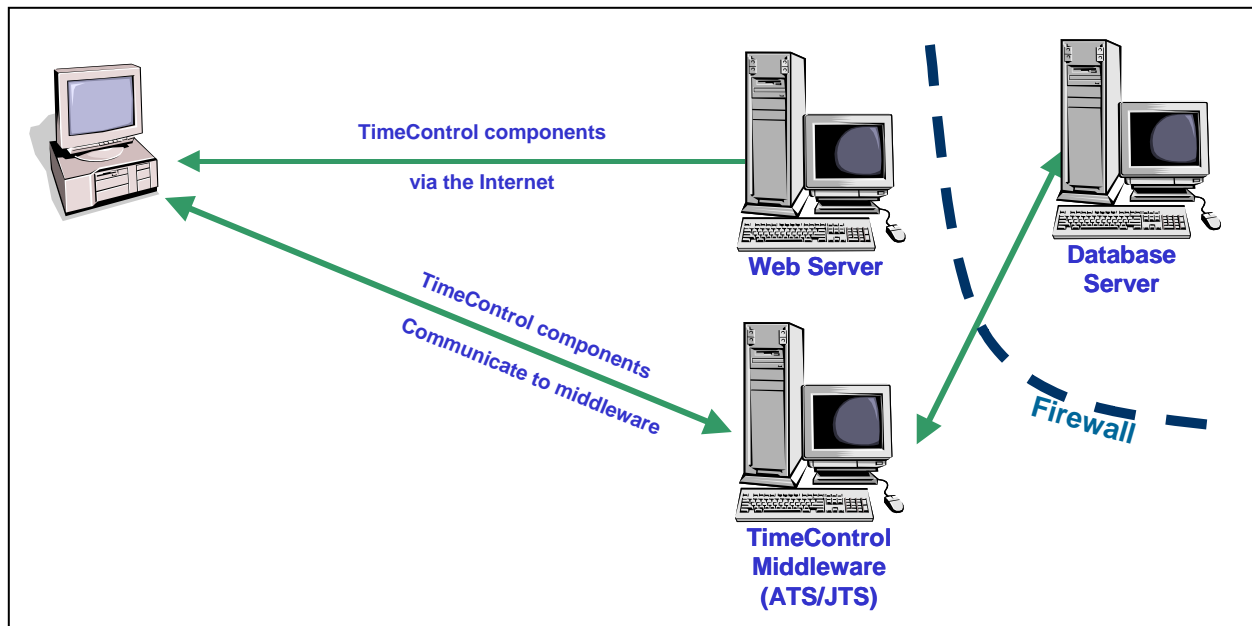
4. The TimeControl components are activated by the end user by selecting a menu item
5. The selected TimeControl component then communicates directly with the middleware. This communications layer is completely encrypted.
6. The TimeControl middleware brokers any traffic and makes the appropriate interaction with the database server.

At no time does the end user machine communicate directly with the database server unless either the web server computer or the middleware computer are also hosting the database.

If a firewall is in use, a port on the middleware machine must be exposed in this scenario for the TimeControl components to be able to communicate with the middleware.

Obviously the most secure implementation of TimeControl Express, Professional or Enterprise 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 Professional or Enterprise without using a proxy server is the following:

1. Have the database server not be the same machine as the middleware server
2. Have a firewall installed in which only a single port to the middleware machine is opened for TimeControl access.
3. Aside from TimeControl middleware and web server services, run no other internet services on this machine
4. Masquerade the database server so that it is not visible outside the firewall



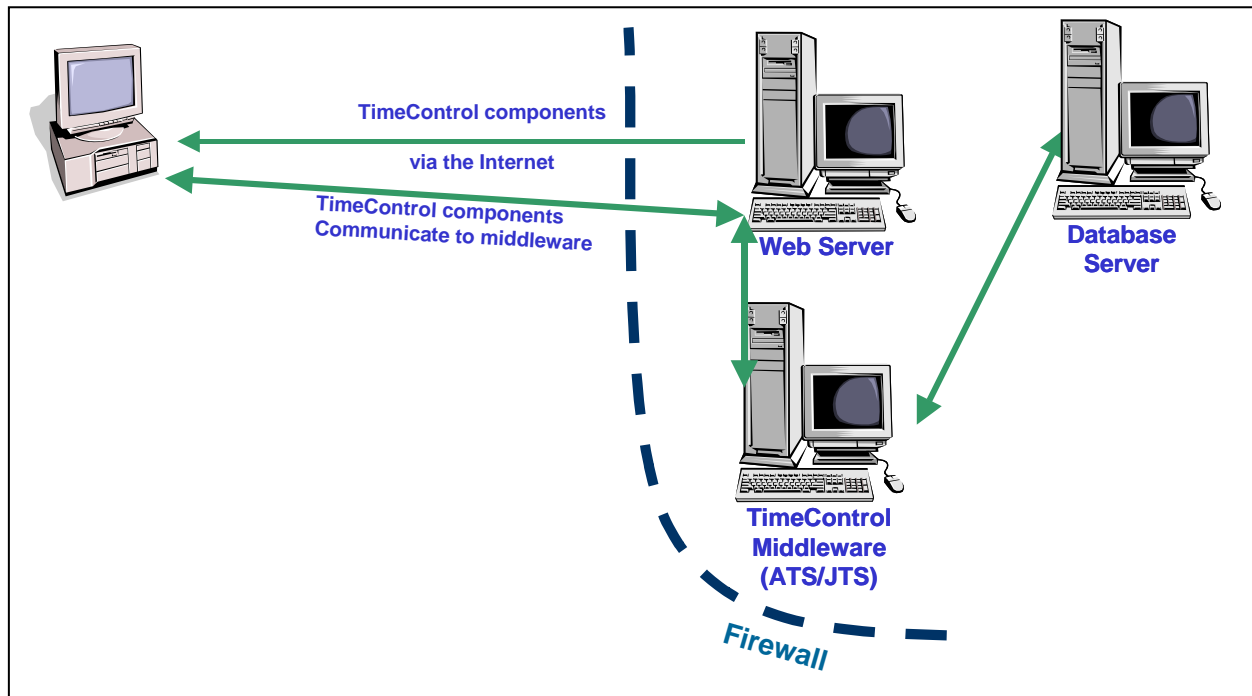
This is a very secure environment. The only area which is even vulnerable to attack is traffic on its way from the web browser client outside the network to the middleware machine inside the network. A worst-case scenario is that traffic to or from the middleware would be corrupted through malicious intent and this traffic is encrypted with a 128bit algorithm. Since the middleware only accepts data that meets the proper business rules anyway, this type of attack would, at worst, cause an erroneous transaction, which would be rejected by the transaction server.

With an open port at the middle-ware transaction server one could argue that this machine is vulnerable to a hacker attack. If so, there is no data stored on this machine and, if masquerading and a firewall is in place, nowhere to connect to past that machine. The worst-case scenario should a skilled hacker be able to penetrate the server through the single firewall port would be a reinstallation of the middleware on the transaction server. This has never happened to a TimeControl client.

Should an environment require even more stringent security, TimeControl Enterprise supports the use of a proxy server. This is discussed in the next section.

PROXY SERVERS AND FIREWALLS

TimeControl Enterprise includes the capability of implementing the ultimate in security architecture using a proxy server. Using a proxy server essentially redirects traffic through your web server's open port to an internal machine that is not otherwise available outside the network.



This allows the standard web security that is part of every web server to intercept and evaluate traffic. It also allows the internal middleware server to be completely hidden from access from outside the network at all. A proxy server is accomplished by registering a redirector with the web server that knows how to interpret TimeControl traffic that arrives from the end user browser. TimeControl Enterprise includes a redirector for the TimeControl multi-platform timesheet interface written as a Java servlet. This redirector is also written in Java and supports multiple web server environments.

Setting up a proxy server environment is technically more complicated to install than any of the other TimeControl installations. There is also the possibility of a slight performance decrease by directing all traffic through the web server.

TimeControl Enterprise also supports multiple instances of both the web server and the middleware transaction servers. This allows, in the largest of TimeControl implementations the capability of a web-farm architecture and load balancing. By using such a structure a TimeControl implementation could be created that would support a

virtually unlimited number of users. TimeControl has been architected for up to 100,000 users within a single system.

LDAP AND WINDOWS ACTIVE DIRECTORY

Some clients will wish to control all application access from Active Directory, LDAP or NT Authentication. TimeControl supports all of these authentication methods as well as it's own security model.

In the TimeControl User Table, select TimeControl Security, NT Authentication, or Active Directory / LDAP as the authentication type. You may be asked for the location of the LDAP or Active Directory Server. A password need be entered into TimeControl only if the TimeControl Security type is selected.

TimeControl will take the User name and Password combination that were 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 the NT Authentication module, pass the User Name and Password to it and wait until NT returns a pass or fail reply. If the method was Active Directory or LDAP, TimeControl will send the User name and Password to the AD or LDAP server and wait for a pass or fail.

This is sometimes desirable in very large organizations when the management of new users, security for various applications and security on servers etc, is a huge undertaking. TimeControl, as an application that is often distributed to virtually every employee means that it is one more application that requires user entry when the employee is added.

At this time, TimeControl does not include direct support for full-time integration with either of these environments. An import of information from the LDAP directory or from Windows authentication can be used, however, 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, contain data that is considered among the most sensitive in the entire organization. This is not like ensuring that someone can start a word processing package so they can write a memo

Also, 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.

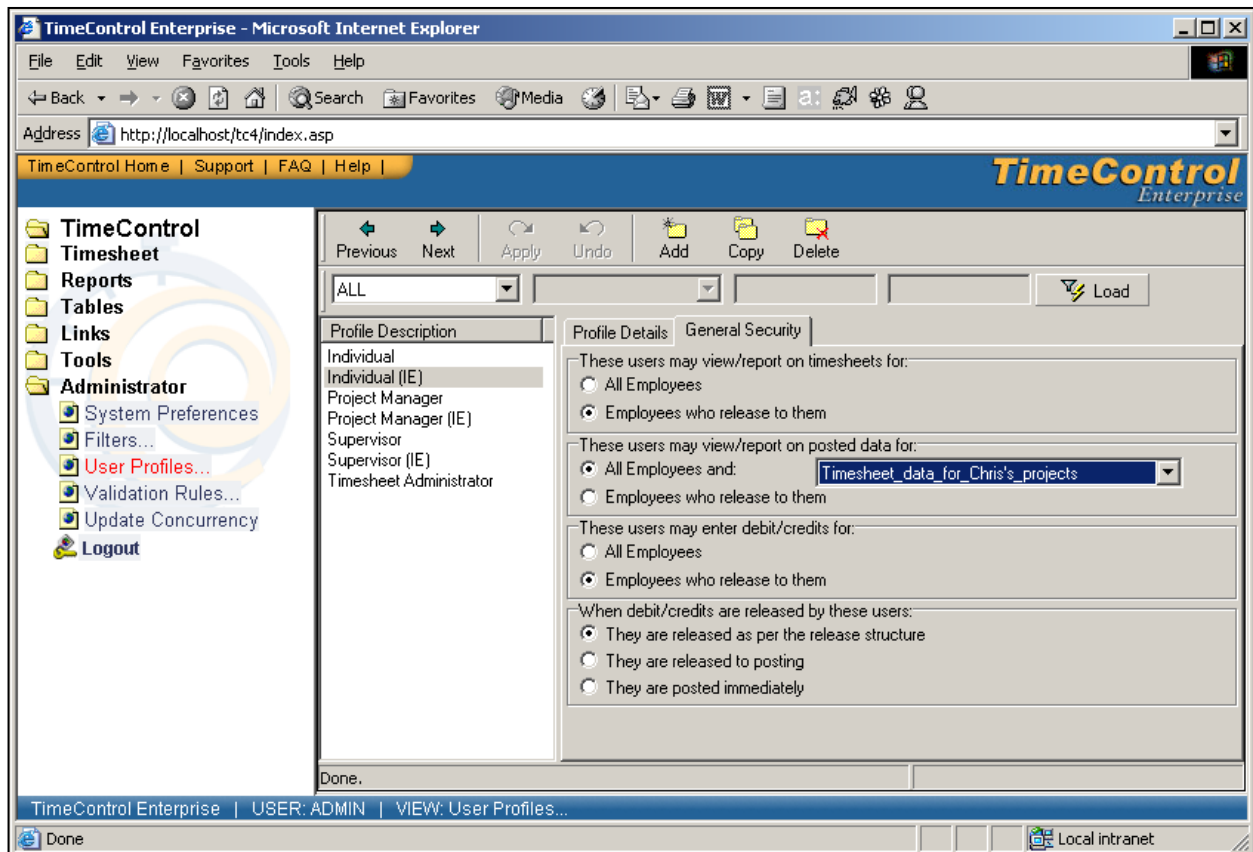
This is why access for new users is more often keyed off the human resources system. In some TimeControl implementations, direct links have been established to trigger an

direct entry of TimeControl by the database itself. Database triggers can be established to move all the pertinent data from the HR or payroll system to TimeControl in order to properly enter all data required by the system to get the employee started with TimeControl.

USER PROFILES

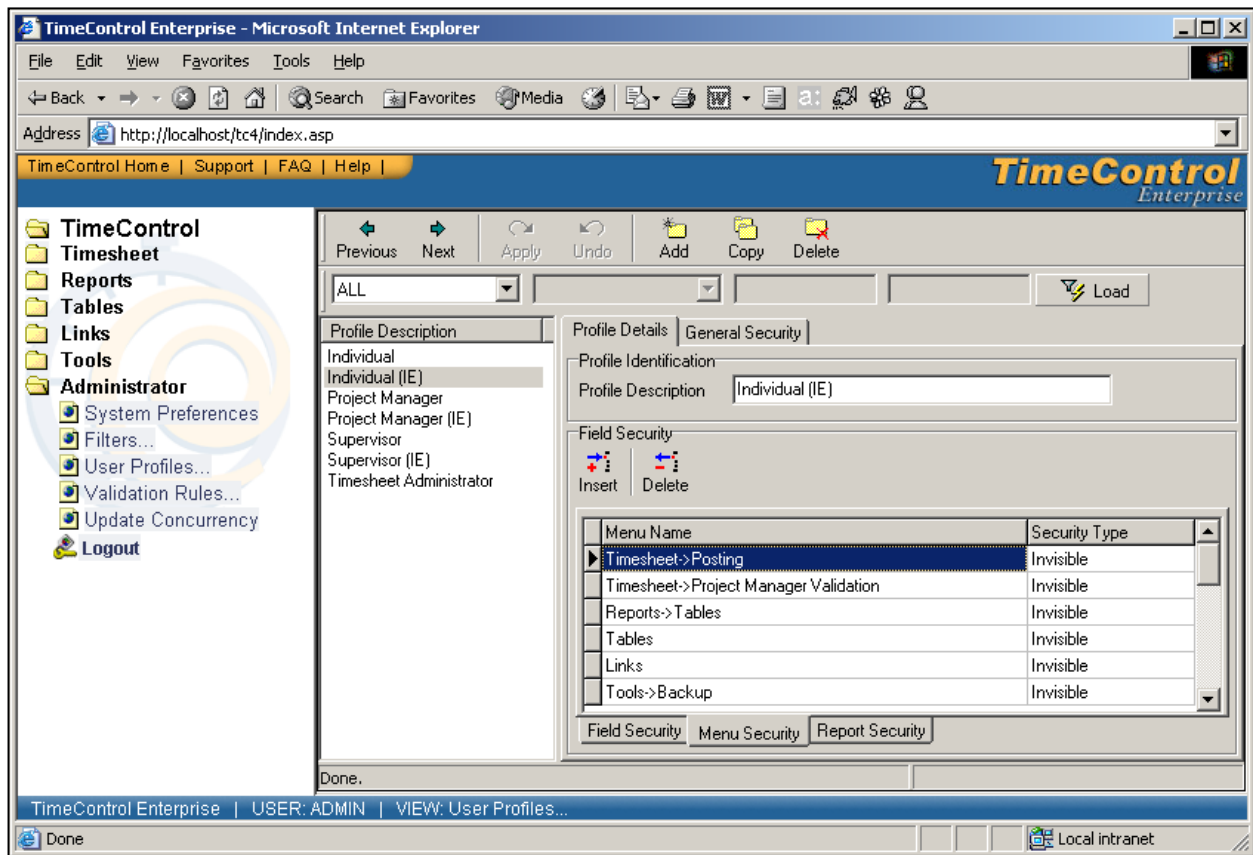
Once in TimeControl itself, there are extensive security structures in place to ensure that users are presented only with the functionality and data they require. The most significant of these is managed through the User Profile area. User Profiles is part of each of the TimeControl editions. This architecture 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 that users such a supervisor 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.

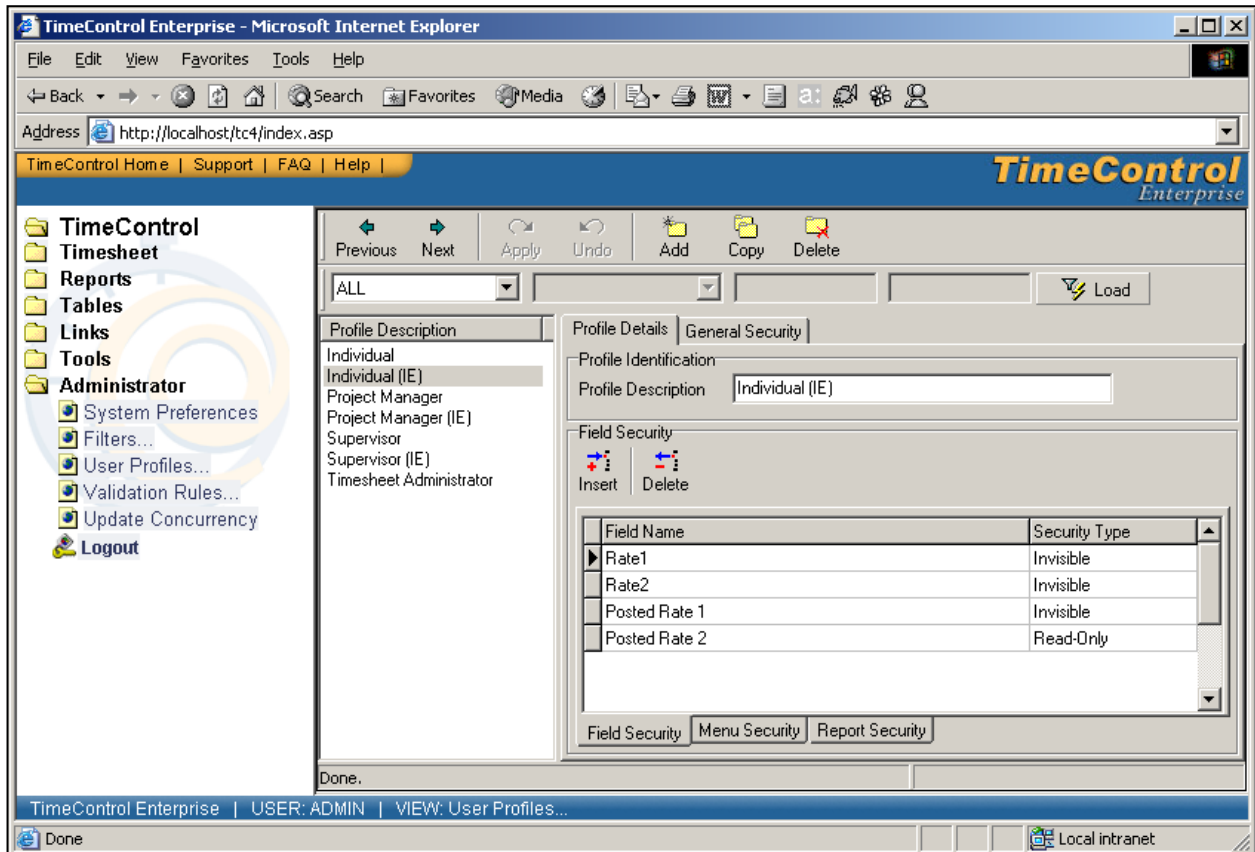


The Menu Security area can be defined at any level of the menu. Top level entries result in that entire tree of the menu structure to be made invisible. If a particular user requires use of a menu item somewhere in the tree (for example just one of the tables), each other item in that area must be made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

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 but 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 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.

ABOUT HMS SOFTWARE

HMS Software, a division of Montreal, Canada-based Heuristic Management Systems Inc., is a leading provider of enterprise timekeeping systems for project environments.

Founded in 1984, HMS Software's expertise in implementing enterprise project-oriented and activity-based-costing systems is recognized worldwide by some of the world's largest organizations. Project oriented products and services from HMS have been used to plan some of Canada's most recognizable projects including the Hibernia Oil Platform, Hydro Quebec's James Bay development, Ontario Hydro's nuclear station refurbishing and InterProvincial Pipeline's cross-country pipeline network.

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.

TimeControl provides organizations with accurate financial reporting and timely project information. TimeControl operates across almost all hardware platforms, integrates seamlessly with many project management systems and with virtually all finance systems.

HMS Software's client list includes some of the world's leading corporations in the telecommunications, IT, finance, engineering, defence/aerospace and government sectors including such organizations as Bombardier, Canadair, Credit Suisse/First Boston Bank, Ericsson, First Trust Financial, Mercury Marine, Motorola, Positron, and the American Red Cross

HMS maintains offices in Montreal, Quebec and Toronto, Ontario.

TimeControl

First published by HMS in 1994, TimeControl has been adopted as an enterprise-wide timekeeping system by clients around the world. TimeControl is designed specifically as an activity-based-costing application and includes such features as hierarchical user structures to allow for multiple levels of timesheet authorisation and an open data architecture which makes the product ideally suited for integration with existing data systems in any organisation. TimeControl is a true client/server system supporting Oracle, Sybase, Microsoft SQL Server, InterBase and Informix. It includes both a Windows and a Web-based interface.

Strategic Services

In addition to being a publisher of enterprise timekeeping software, HMS provides a full range of support services including technical support, training and consulting tailored to meet clients' specific needs. HMS Software consultants are skilled in activity-based-costing, timekeeping methodology, project management techniques, cost management as well, of course, in the HMS-supplied products.

For more information about TimeControl, visit our website at: www.timecontrol.com.