



*build*  
**smart**

*your total hr solution...*

***Technology and  
Architecture Overview***

[www.psiberworks.com/buildsmart](http://www.psiberworks.com/buildsmart)

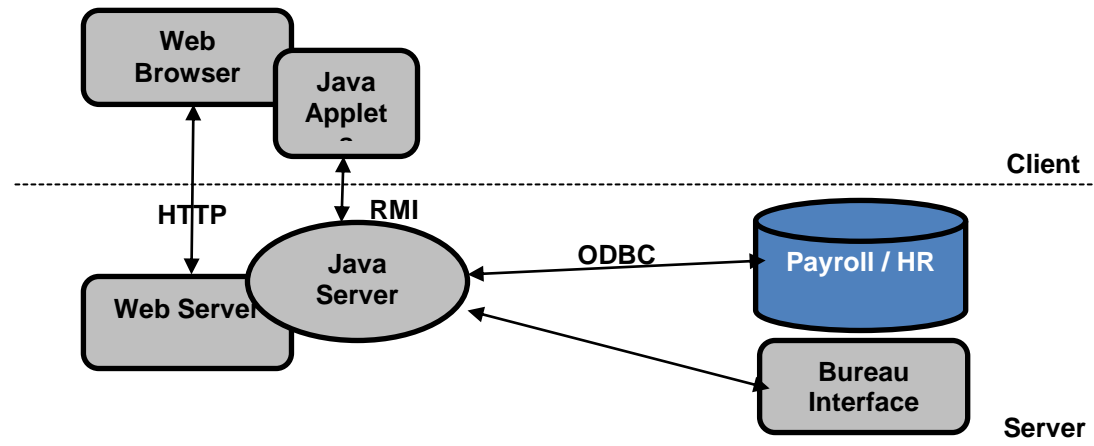
## Index

1.	PSIber Technology and System Architecture .....	3
1.1.	Server.....	3
1.2.	Data Transfer .....	4
1.2.1.	Client - Server .....	4
1.2.2.	Database - Server .....	4
2.	Security.....	5
2.1.	Outsourced Firewalls.....	5
2.2.	Code Signing.....	5
2.3.	Product Content Encryption.....	5
2.4.	Website Security .....	5
2.5.	Passwords.....	5
3.	Secure Backups .....	6
3.1.	PSIber Internet & PSIber Hosted.....	6
3.2.	Intranet/Standalone Versions .....	7
4.	Technical Specification .....	7
4.1.	Hardware and Software Specification .....	7
4.2.	Software Requirements .....	7
4.3.	Web Server .....	8
5.	Setup / Implementation Considerations .....	8
5.1.	Ports.....	8
5.2.	Firewalls & Proxy Servers .....	8
5.3.	Connection Method .....	8
5.4.	Bandwidth Considerations.....	9
5.4.1.	Line Speed .....	9
5.4.2.	Capped vs Uncapped.....	9
5.4.3.	Shaped vs Unshaped .....	10
6.	Email and SMS Notification Setup .....	10
6.1.	SMS Notification Setup.....	10
6.2.	Email Notification Settings.....	11
7.	Other.....	13
7.1.	Payslip and Report Logos .....	13
7.2.	Images .....	13
7.3.	Application Program Interfaces (API) .....	13
7.4.	Branding.....	13
8.	Performance Benchmarking .....	14
9.	Properties and Configuration Files.....	16

## 1. Technology and System Architecture

The system is a three-tier Internet enabled software package written in Java (Version 1.6). The software's Client-side consists of several Java Applets embedded and viewed in a Web Browser such as Microsoft Internet Explorer 7+ and Firefox. These Applets collectively constitute the Client application.

The software's Server is a standalone application that resides and executes as a service on an application Server. The Server service hosts most of the business logic, coordinates Client actions and interfaces with the relational database.



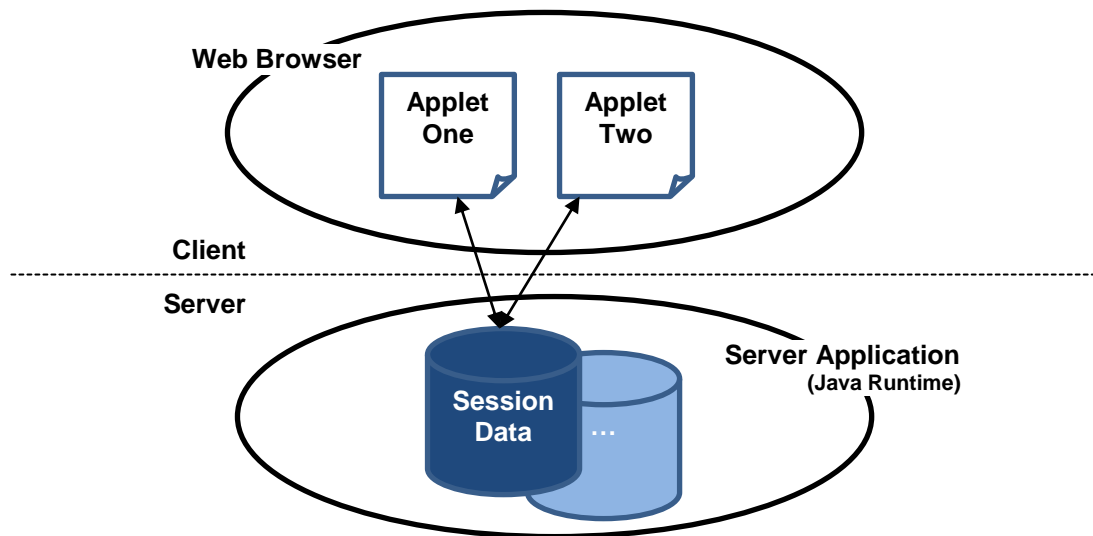
### 1.1. Server

The Server application acts as a cache for the shared data. This is more easily explained by describing and explaining the events that occur when a User makes use of the software:

A User logging in to the application will provide his or her User name and password to gain access to the system. At this point the Applet that provides the login facility establishes a session for the active User on the Server application. This session exists until the User discontinues using the software by logging out or until such time as the client disconnects from the Server. When the User navigates to another web page within the Client application the Applet on that page re-establishes connectivity to the active User's session on the Server application. This effectively provides a mechanism where any data can be shared among all the Applets within the application via the Server.

Thus, a 'Server session' is established for the IP Address from which the User accesses the system. As the User navigates through the various Client interfaces, the Client processing communicates with the Server to reconnect with the session initially established and in this way the data is shared between the Client interfaces. The establishing of a Server session also allows for the implementation 'time-outs'. If the User is not active for a User defined period e.g. 10 minutes (this is a user customizable property), the Server session will be timed-out and the User will be forced to logon to re-establish the session before continuing.

The diagram below illustrates this concept. Within the Web Browser Applet One and Applet Two have access to the same, shared session data. All Clients actively using the software have their own private session allocated to them within the Server application.



## 1.2. Data Transfer

### 1.2.1. Client - Server

The ports handling incoming connection requests are configurable. All data is transferred via RMI between the Client and the Server. The RMI hosting port is configurable.

NB: Although the system is able to tunnel through firewalls with the help of a proxy Server by wrapping the RMI protocol in an additional HTTP layer, it is preferable that any firewall be configured to allow traffic to the service on the ports specified.

Data transfer is encrypted using a proprietary encryption technique. This technique involves encrypting the data stream being transferred by randomly generating a 'key' and scrambling the data in the stream. The 'key', together with the scrambled data stream is passed to the recipient. The recipient descrambles the data stream using the 'key'.

Optionally, industry standard SSLv3/TLSv1 encryption is also supported.

*Note: PSiberWORKS (Pty) Ltd is the holder of a VeriSign Code Signing certificate for the Buildsmart HR Product Suite.*

### 1.2.2. Database - Server

The application communicates with the SQL Server Database using standard JDBC (Java Database Connection) libraries. Any JDBC MS-SQL driver should suffice, although we recommend the JTDS JDBC (3) type 4 driver for maximum performance.

Currently only Microsoft™ SQL Server is supported.

## **2. Security**

### **2.1. Outsourced Firewalls**

The IS Outsourced Firewall enables us to access 'best of breed' firewalls within one of IS' secure Internet Data Centres. The solution is "outsourced" in that Internet Solutions take full responsibility for the hardware, software and infrastructure components of our solution. We however retain full control over the firewall rule base, which can be modified to suit our individual security policy requirements as and when our needs change.

IS Outsourced Firewall solutions are geared to provide low latency, high throughput security solutions, which examine traffic in both inbound and outbound directions. Whether it is the only firewall or an additional layer to an onsite firewall, IS' Outsourced Firewall provides high levels of security based on Fortinets award winning Fortigate Firewall Appliance and is built with high levels of infrastructure redundancy to provide a robust offsite perimeter protection solution.

### **2.2. Code Signing**

PSiber Group (Pty) LTD holds a Digital Certificate that is used to sign all redistributables and binaries. This ensures that the executable code has not been tampered with and that the binaries were issued by the PSiber Group (Pty) LTD.

### **2.3. Product Content Encryption**

Data passed between the Client and the Server is encrypted. The system supports SSLv3/TLSv1 encryption if a valid certificate is supplied. A self-signed certificate may also be used, should this be preferred.

Encryption prevents interception and tampering of data in transit. Should the data stream be compromised the User will be logged off immediately and any pending actions cancelled to ensure that the integrity and security of the system is maintained.

### **2.4. Website Security**

The PSiber Group (PTY) Ltd. is the holder of an industry standard SLL certificate which is used to secure sensitive information.

### **2.5. Passwords**

The system has a robust password management facility which allows the User to customize the security of the log-in process to fit their needs. Passwords can be set to expire automatically after a certain amount of incorrect login attempts, a specified period of time, or a specified period of inactivity. Furthermore, passwords can be comprehensively customized to have a compulsory amount of characters, whether numeric, alphanumerical either upper or lowercase, as well as special characters. The login system also contains a secure facility to retrieve a forgotten password, which is then mailed by the system to the specific e-mail address stored against the User account.

### 3. Secure Backups

#### 3.1. Internet & Hosted

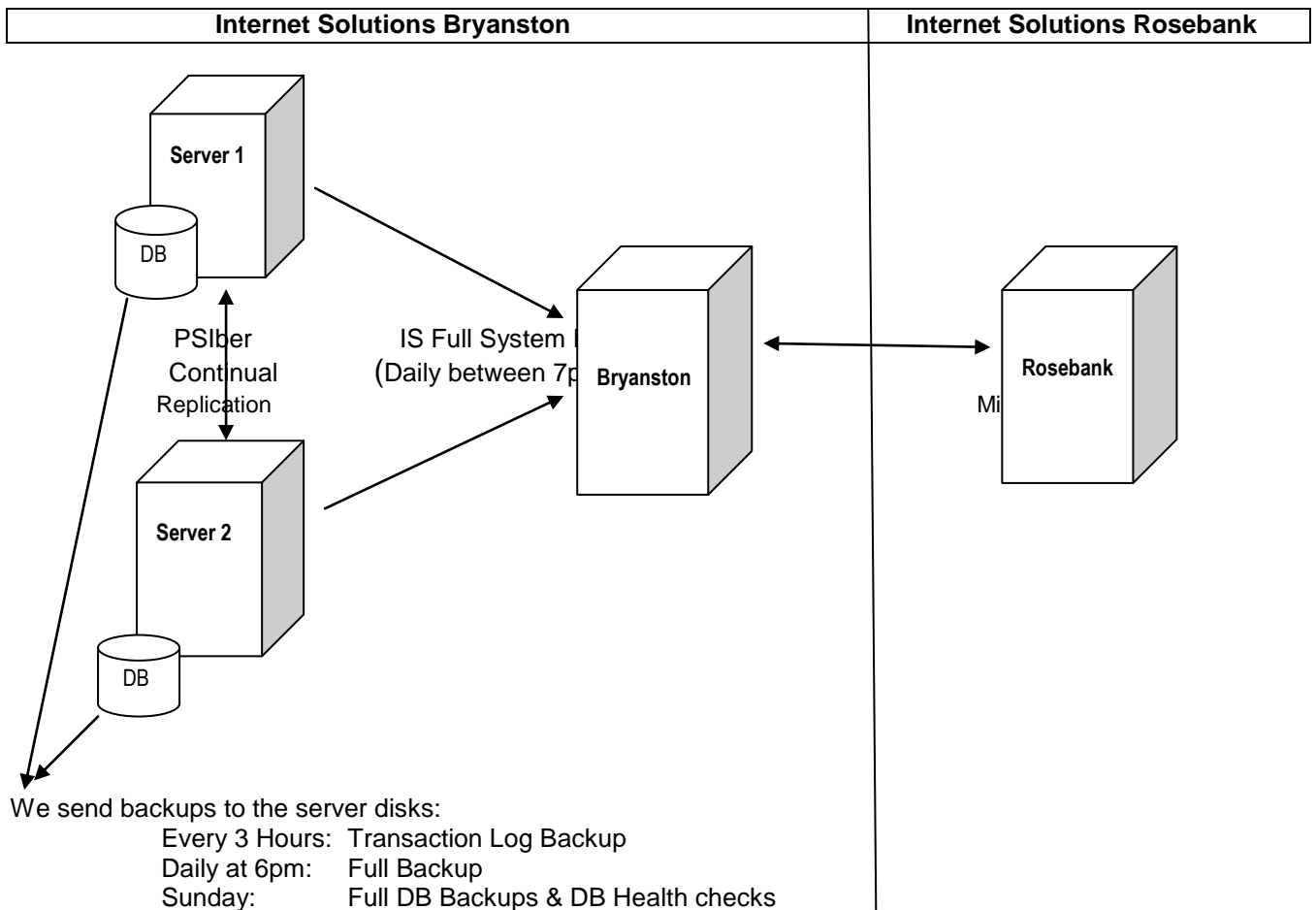
Where Clients are using the Internet version or are hosted by us, all backups are done using the Attix5 digital backup technology. Although the backups are scheduled for various specific times during the day, the technology also allows for customised backups (user controlled) at any time. This technology also facilitates mirror imaging of data etc in the IS Rosebank environment which ensures local, as well as offsite digital backups are always available. Schedules backups are as follows:

**IS Backups:**

- Attix5 Digital Backups at IS : Daily between 8pm and 8am (full system and Data Base backups)
- Attix5 backup servers at IS Bryanston Data Centre are mirrored at IS Rosebank Data Centre

**PSIber Backups:**

- Daily backups at 3 hourly intervals : Transaction Logs
- Daily Backups at 6pm : Full Backups
- Continual replication between the two servers
- Weekly Backups on Sundays :
  - Full Backups
  - Weekly data base history
  - Data Base health checks





### 3.2. Intranet/Standalone Versions

Clients running the system in their own environments are responsible for their own backups.

## 4. Technical Specification

### 4.1. Hardware and Software Specification

Please ensure that the correct environment specifications are used. The various environment types are as follows:

- **Internet:** online version i.e. accessible directly via the public internet
- **Standalone:** where product has been installed on an individual workstation / PC / laptop
- **Intranet:** where product has been installed on an in-house server, where the Client accesses through their own network

Please note that the following requirements are a guideline only as the following will have an impact on these requirements:

- Number of Users (CPU cores and RAM)
  - Number of Payrolls and Employees
  - Amount of history & Product usage
- Note: if performance is not in line with provided guidelines (please see the Benchmarking Section of the document), the hardware specifications should be revisited.

HARDWARE REQUIREMENTS (environment specific)			
Environment	Hardware	Recommended (Small to Medium)	Recommended (Large)
CLIENT	RAM (Memory)	2 GB	4 GB
	Processor	2.33 GHz Core 2 Duo	2.33 GHz Core 2 Quad
	Free Disk Space	20 GB	20 GB
INTERNET / INTRANET	RAM (Memory)	4 GB +	16 GB – 32 GB
	Processor	2.33 GHz Quad Core +	2.8 GHz Xeon (Multi Core)
	Free Disk Space	50 GB (depending on size of database)	200 GB
STANDALONE	RAM (Memory)	2 GB	Not recommended
	Processor	2.33 GHz Core 2 Duo	
	Free Disk Space	50 GB	

### 4.2. Software Requirements

SOFTWARE REQUIREMENTS (for ALL environments)			
Environment	Software	Minimum Requirement	Recommended Requirement
INTERNET, STANDALONE & INTRANET	Operating System	Microsoft Windows XP / Vista / 7 / 2003 / 2008	Microsoft Windows XP / Vista / 7 / 2003 / 2008
	Adobe Acrobat	Any	Any
	SUN JAVA VM	1.6.0_07	1.6.0_22
	Web Browser	For best viewing, we highly recommend the latest versions of web browsers available.	

**Important Notes:**

- Memory requirements are a guideline only and requirements of other applications must be factored in.

- Free Disk Space is an estimate only, and is dependent on product / module usage, size of company and amount of historical data.
- For the up-to-date requirements page go to: <http://www.psiberworks.com/TechnicalSpecifications.aspx>
- Internet Explorer 7+ (8 preferred), Google Chrome and Firefox are all supported.

### 4.3. Web Server

A Web Server, such as Microsoft Internet Information Server, is required to serve the application to Client Browsers.

## 5. Setup / Implementation Considerations

### 5.1. Ports

At present, the live environment has a number of opened IP addresses and ports, which need to be connectable from the Client's network. This is only applicable if the Client is utilising one of our specific hosted services (e.g. [www.psiberworks.com](http://www.psiberworks.com) or [www.psiberworks.com/clientname](http://www.psiberworks.com/clientname)). The network address and ports are as follows:

Network Address: 196.35.164.88/29  
Subnet Mask: 255.255.255.248  
Port Range: 2030 – 2092  
Connection Type: TCP, Outbound.

### 5.2. Firewalls & Proxy Servers

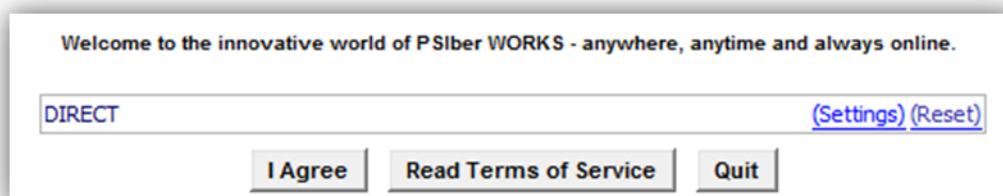
In order to ensure that Users can connect to the service, it is imperative that Firewalls & Proxy Servers etc, allow Users on the network, to connect to the addresses and Ports as specified above. Although the system can connect via a Proxy Server, this can have an adverse effect on system performance ie the application data needs to be wrapped in http, which adds an additional protocol layer, forces the system to compile an entire message before sending it to the server and vice versa. Therefore we recommend that the firewall allows individual clients direct access as per 4.1 above.

### 5.3. Connection Method

The system supports the following connection methods:

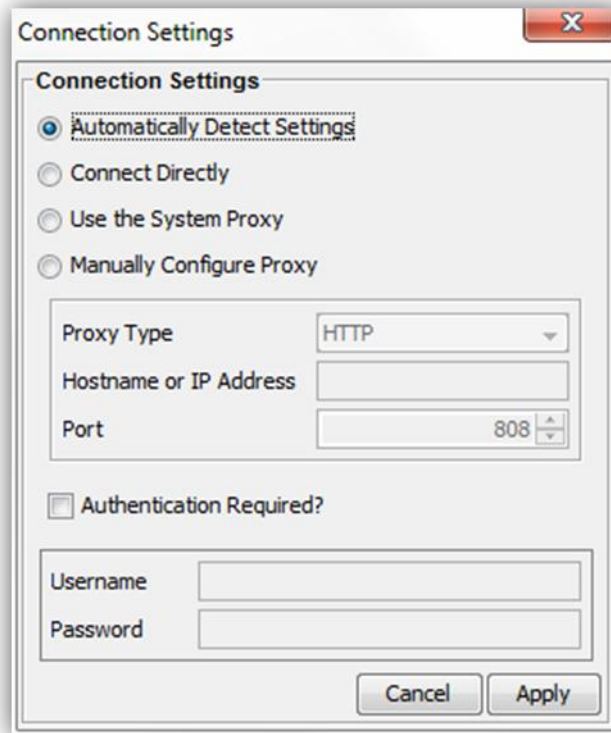
- i. Direct Connection
- ii. Direct Connection wrapped in HTTP.
- iii. HTTP Masquerade through a Proxy Server.

The system will try connecting in the order of the above ie the best connection type first. The 'Connection Status Bar' on the login screen will reflect the type of connection that has been made, please see below:





The login screen allows the User to override the automatic detection. Clicking the 'Settings' option on the connection status bar will present the User with the following popup:



- Automatically Detect Setting: This option attempts each connection method, to determine the best available option.
- Connect Directly: This option forces a direct connection to the application ports, if it is possible.
- Use the System Proxy: Forces the system to connect via the Administrator defined Proxy setting ie Windows.
- Manually configure Proxy : Forces the system to use the User definable Proxy settings as per the following:
  - Proxy Type
  - Hostname or IP address
  - Port

## 5.4. Bandwidth Considerations

### 5.4.1. Line Speed

Broadband internet connection is required. The required line speed varies dependant on the following factors:

- Number of concurrent Users
- Line utilization (by all other applications/services)

### 5.4.2. Capped vs. Uncapped

It is very difficult to calculate beforehand how much bandwidth will be required in a given month. We recommend therefore, that where a capped account is used, bandwidth utilization is monitored, to determine whether an uncapped account would be more cost effective.

### 5.4.3. Shaped vs. Unshaped

An unshaped internet connection is highly recommended for performance reasons. Shaped connections assign a much lower priority to application traffic that is not travelling through certain standard ports e.g. HTTP/S is usually unshaped. Because the Buildsmart HR product suite uses application specific ports, it is highly susceptible to shaping, depending on your service provider's, and possibly the Client's own IT departments, shaping policy. This results in an extremely slow and unresponsive system, which may appear to be hung, each time the system needs to communicate with the server.

## 6. Email and SMS Notification Setup

### 6.1. SMS Notification Setup

The system currently supports sending of SMS notifications through one of two gateway services:

- [www.clickatel.com](http://www.clickatel.com)
- [www.smscity.co.za](http://www.smscity.co.za).

In order to enable SMS notifications, an account must be opened with one of these Service Providers and the necessary information captured in the 'Email Room Setup' facility, after which the notification system can be configured to send SMS's for all currently supported notification types.

Client specific SMS gateway preferences should be addressed directly with the Technical / Support department to establish interface availability and what changes are required to facilitate the SMS functionality.

SMS Notifications can be configured from the 'Mail Room Settings' facility. The various providers have different account information requirements for sending SMSs. The fields that are required will be enabled according to the Service Provider selected.

The following information may be required:

- Username : The username provided by the gateway service
- Password : The password provided by the gateway service
- API\_ID : The api\_id provided by the gateway service (Clickatel only)
- Sender ID: From where the SMS originated.

SMS Settings

Gateway: Clickatel

Username: psiber

Password: ●●●●●●

Api\_id: 3231957

Sender ID: 27824252035

Send Test SMS

To test the SMS facility:

- SMS Credits must be available/purchased ie should insufficient credits be available, the SMS will not be sent.
- Click on the 'Send Test SMS' button on the 'Mail Room Settings' Screen
- Provide a cell phone number:
  - This service requires the international format for numbers eg 27 72 123 4567.
  - No '+' is required before the number. Credits are purchased in advance
- Note:
  - Messages can be a maximum of 462 characters
  - Messages that exceed 160 characters will consume multiple credits.

## 6.2. Email Notification Settings

In order to utilise the Email Notification facility effectively, it is important that the following be noted. Default email notification settings are defined in the **mail.properties** file for each instance. By default, emails are sent through a Relay which may result in Emails being identified as spam and thus being rejected by the mail marshal. In order to prevent this, a 'Mail Room Setup' facility is available which allows for the User to set their own exchange or smart host, which will then be used to relay Emails. The 'Email Room Setup' facility allows the User to:

- Override the system default settings (as defined in the **mail.properties** file) for sending email notifications;
- Authenticate email; and
- Specify their own SMTP Server for sending emails as well as the sender address.

The benefits of setting up the mail room settings are as follows:

- Emails will be sent from your own mail Server;
- Emails will no longer be blocked i.e. marked as spam; and
- A specific 'From Address' can be defined



Mail Room Settings	
Host	<input type="text"/>
Port	25
Require Authentication	<input checked="" type="checkbox"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Enable TLS	<input type="checkbox"/>
Enable SSL	<input type="checkbox"/>
Check server ID	<input type="checkbox"/>
From Address	<input type="text"/>

Field Name	Description
Host	The SMTP Server's FQDN or I.P. address. This address should be available from the Buildsmart HR Server i.e. the Server on which Buildsmart HR is running must be able to connect to this address on the specified port.
Port	The port on which to connect to the SMTP Server.
Require Authentication	Tick this if the SMTP Server requires authentication before sending email. If this is not ticked then Buildsmart HR will attempt to connect to the mail anonymously which may fail if the Server requires authentication and result in the mail not being sent.
User Name & Password	The credentials of the specified User from who emails will be sent i.e. the 'From Address'. This is required to send emails on behalf of the specified User.
Enable TLS	Tick this to enable TLS connection security; however this can only be done if the SMTP Server supports TLS. (If using a self-signed certificate, this needs to be added to the product's certificate store).
Enable SSL	See Enable TLS. (SSL and TLS are mutually exclusive i.e. only one of these may be enabled at any one time).
Check Server ID	Tick to perform additional identity checks. This helps to prevent third parties intercepting emails. (This option is only available when using SSL / TLS).
From Address	This is the address from which emails will be sent and to which any 'replies' will be sent. (The address must exist and must be valid on the SMTP domain).

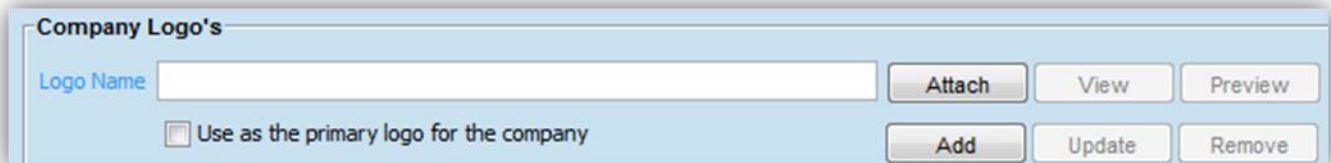
**Please Note:**

- These settings should match your SMTP Server settings and ideally be setup by a network administrator or IT Manager.
- Only basic authentication is supported by Java Mail API (not windows integrated authentication / LDAP)
- When authentication is required, the specified User must have 'Send As' permissions on the specified Sender mailbox.
- If the 'Mail Room' settings are not defined, then the setting will default to the **mail.properties** settings.

## 7. Other

### 7.1. Payslip and Report Logos

Users are able to print Company Logo's on Payslips and reports. For the best quality Logos, the required dimensions are: 87 pixels wide by 4 pixels high. The Logos are attached from within the product ie:



### 7.2. Images

The Digital Images function within PSiber allows Users to attach and view a number of Digital Images for an Employee. This facility allows for Employee related Digital Images, such as Employee's photo, Employee Take-on form, ID Book, Proof of residence etc.

Please note the following requirements:

- Digital Images can only be saved in the following formats: **jpeg, gif, png or bmp**; and
- The maximum file size of each Digital Image can be customized in the Properties file, the default maximum size being **256KB**.
  
- We recommend the use of scanned documents / Digital Images or digital camera images.
- If emailing of images it to be used, please request your IT department to setup/check the following:
  - Set up an SMTP relay - one is provided with IIS (Internet Information Services) and can usually be installed off the Windows CDROM;
  - Edit the mail.properties file in the Buildsmart(HR)\server\lib file;
  - Set the various 'xxx.smtp=hostname' accordingly; and
  - Set the 'xxx.mail=email\_address' to the required 'From' address.

### 7.3. Application Program Interfaces (API)

Buildsmart HR caters for the import of Mass data via API. APIs are available for all Employee information as well as Company information such as Cost Centres, Departments, Job Grades etc.

The import facility is available from the 'System Administration & Utilities / Imports & Exports' option and uses Excel Spreadsheets.

### 7.4. Branding

Buildsmart HR does offer Client Branding of the Product ie all HTML can be client branded according the Client requirements.

## 8. Performance Benchmarking

As so many factors can impact the response times, this benchmark serves purely as a guideline.

The following factors need to be considered as they all have an impact on the response time ie:

- Server specifications
- Client machine specifications
- Line speed and utilisation
- Number of payrolls, size and complexity of payrolls
- Proxy servers
- Shaped vs. Unshaped internet
- Traffic Shaping

The response type benchmark example below was carried out in the following environment:

- ADSL line 1 mbps
- Accessing the internet system
- Firewall
- Three computers with different specifications were utilised for this test
- Server hosted at Internet Solutions
- Server spec:
  - O/S – Server 2008
  - 4 CPU Hex Core with hyper threading
  - 32 Gb RAM
- Unshaped internet with Buildsmart HR high priority allocation
- Payroll size +/- 50 – 500 employees, +/- 10 payrolls and high complexity



Function	PC 1	PC 2	PC 3
	Windows 7	Windows Vista	Windows XP
	Pentium Dual-Core 2.10 GHz	Intel Core 2 Duo 2.80 GHz	Celeron D 3.46 GHz
	4.00 GB RAM	2.00 GB RAM	448 MB RAM
Time measured in <b>seconds</b>			
Loading of "Login" screen	4 - 8	9 - 12	10 - 15
Physically logging in to the "Product Menu"	1 - 4	4 - 9	12 - 16
Accessing a payroll (click "Go" button)	1 - 6	3 - 6	3 - 12
"Leave Calendar" popup	0.1 - 0.5	0.1 - 0.5	0.5 - 0.9
Accessing "Payslip Adjustments" screen on employee	2 - 7	3 - 7	3 - 11
"View Payslip" on screen	0.2 - 1.1	0.5 - 1.1	0.5 - 1.1
Loading "Run Payroll" Screen	2 - 4	2 - 4	4 - 8
Accessing the 'Reports' from menu click to pop-up	2 - 3	2 - 3	4 - 5
Run the "Detailed Payroll Summary" report (select all Allowances, Normal and Occasional Earnings)	7 - 11	7 - 15	7 - 22
Run the "EMP201" report	4 - 7	4 - 7	5 - 9
Run the "Staff Movement (incl. Headcount)" report	1 - 4	1 - 4	3 - 4

## 9. Properties and Configuration Files

Users need to be aware that the system includes various 'Properties' and 'Configuration' files, which include settings which may impact the system setup in Standalone and Intranet environments. These are as follows:

- **Mail Room Properties:** this includes the parameters as per the 'Email Notification Rules' screen. The Mail Room properties have the following default settings, which are overridden by the User defined settings in the aforementioned Email Notification Rules screen:
  - **Host:** The SMTP Server / Smart Host which is responsible for delivering the email to its destination.
  - **Port:** The TCP port that the Host is accepting connections on. Default SMTP Port is 25.
  - **User Name:** The username used to authenticate on the SMTP server.
  - **Password:** The password for the above username.
  - **Enable TLS:** Enables Transport Layer Security if required by the SMTP Server.
  - **Enable SSL:** Enables Secure Sockets Layer if required by the SMTP Server.
  - **Check Server ID:** This will enforce an additional check that the server is who it claims to be. (Only applicable if TLS is enabled.)
  - **From Address:** The Sender Address. i.e. the email address that the systems emails will come from.

**Persistence Properties:** It is imperative that these settings are correct and incorrect setting could result in not being able to connect to the system:

```
#
# SQL
#
sql.syntax.type.long=DECIMAL
works.implementation=sql
#
# jtds
#
works.protocol=jdbc:jtds:sqlserver:
works.url=jdbc:jtds:sqlserver://psiber-
db/works;user=psiberworks;password=psiberworks;instance=mssqlserver;
works.sql.driver=net.sourceforge.jtds.jdbc.Driver
```

### PSiberWORKS Properties:

PSiberWorks Client:	
HideSouthAfricanLinks=false #	<b>this hides everything South African in the GUI. This is for non SA clients</b>
client.debug=N/A #	<b>only.</b>
client.ShowTermsOfService=true #	this won't do anything noticeable, but might degrade performance.
<b>screen.</b>	<b>this enables the Terms Of Service on the current login</b>
client.AllowRegisterOnLogin=true #	This allows the user to register a new company etc. In any event this can be
	reached from the branding and so is not important.
client.Compression=false #	No impact
seifsa=1 #	Impacts client using SEIFSA
ImagePath=c:/PSiberWORKS/res/ #	No longer used. Originally for the location on the client PC of Payslip Logos
ReportWizardLink=http://psi-qa/reportwizard/ #	Only necessary where there is a Report Writer instance set up
CompanyRegNoLength=4 #	don't change this!!!
EmployeeNumberLength=16 #	don't change this!!!
UserRevokeThreshold=4 #	No longer used.
ProductExpiryFirstWarningThreshold=40 #	<b>this is the number of days before the license file expires that the system will</b>
	<b>start warning the User.</b>
ProductTrialPeriod=40 #	No longer used.
ProductTrialRegPrefix=X #	No longer used.

Billing=true # Used for clients with billing.  
BuildsmartActive=false # **this enables the Buildsmart Interface.**  
Branding=e-Worx # this affects the product descriptions . do not change.

# This is used by the client to determine whether branch validation is active  
BranchValidationCompulsory=false # this forces branch validation.  
BranchFileName=yes # don't change this.

# remove 'host' and 'port' properties for local execution...  
host=psiber-qa # **this is the host to which the client will connect. (i.e. the server)**  
port=1585 # **this is the TCP port to which the client will connect.**  
name=works.12.03.00 #the instance name. Don't change this.

PSiberWorks Server:  
auto.billing.run.time=13 # **the hour of the day that automatic billing will run. This is only for billed instances.**  
[meagan@psiber.co.za](mailto:meagan@psiber.co.za);[sean@psiber.co.za](mailto:sean@psiber.co.za) # **the email addresses that the billing file will be sent to.**  
email.notification.manager.on=true #**This enables the Automatic Notification System. Do not disable.**  
seifsa=1 #don't change this.  
client.debug=N/A # Not important  
Compression=true # don't change this..  
IOTiming=false # don't change this.  
SQLTiming=false # don't change this.  
RemoteSessionTiming=false # don't change this

MonitorFolder=.\inspector # don't change this.  
MemoryMonitorFreq=600 # Don't change this.  
Monitor.Memory.MinLevel=30 # Don't change this.  
Monitor.Memory.SMTPServer= # don't change this.  
Monitor.Memory.NotifEmail= # don't change this.

CleanerFreq=-1 # don't change this!!!!  
CompanyCleanerFreq=-1 # don't change this!!!!  
PayrollCleanerFreq=-1 # don't change this!!!!  
PersistentSet.DefaultExpiry=600000 # don't change this!!!!

Cleaner.DoLogCleared=false # don't change this!!!!  
Cleaner.DoLogLevel=false # don't change this!!!!  
Cleaner.DoLogNotExpired=false # don't change this!!!!  
Cleaner.DoLogNotChecked=false # don't change this!!!!  
CompanyRegNoLength=4 # don't change this!!!!  
EmployeeNumberLength=16 # don't change this!!!!  
UserRevokeThreshold=4 # No longer used!  
ProductExpiryFirstWarningThreshold=40 40 # **this is the number of days before the license file expires that the system will start nagging.**  
ProductTrialPeriod=40 # No longer used.  
ProductTrialRegPrefix=X # No longer used.  
BranchValidationCompulsory=false # **this forces branch validation.**  
BranchFileName=.\lib\acb.dat # **this is the bank branch file.**  
ssl.server.enabled=false # **enables SSL/TLS communication.**  
ssl.server.keystore=./lib/psi-qa.jks # **this is the java keystore file where the SSL certificate and private key are stored.**

ssl.server.keystore.password=xxxxx # **this is the keystore password.**  
ssl.server.ciphers= # don't change this, unless you want to force a specific cipher.  
Not recommended.

ssl.server.protocols= # don't change this, unless you want to force a specific protocol. Not recommended.

ssl.server.client.auth=false # this causes client SSL certificate authentication.

auto.leave.rollover.enabled=true # **this enables automatic leave rollover for Staff Only payrolls and Leave Extract information to be updated.**

auto.leave.rollover.time=07 # **this is the hour of the day that automatic leave rollover will happen.**

auto.leave.details.enabled=true # **this enabled Leave Extract information to be updated.**  
auto.leave.details.time=07 # **the hour of the day that Leave Extract information will be updated.**

email.notification.manager.on=true # **this enabled Automatic Notifications.**

server.audit=true # **this turns on auditing. DO NOT TURN OFF!**

server.autostart=true # Don't change this

server.timeout=1800000 # **this is the Session Timeout. This is how long a client can be inactive on the server before being logged out. This is measured in milliseconds. 1800000 = 30minutes**

server.ACBUUpdateFrequency=80 # Don't change this.

server.ContractFileName=.\lib\contract.txt # Not used.

server.rds=false # **DO NOT ENABLE THIS!!!**

instance.location=http://psiber-qa/works.12.02.02 # **this is the base location that is used for notifications that contain a link back to the system.**

#  
# the following properties are used by both CLIENT and SERVER code.  
#

server.audit=true # **enabled auditing.. DO NOT DISABLE**  
server.rmiport=1586 # **this is the second TCP port.**  
# remove 'host' and 'port' properties for local execution...  
host=psiber-qa # **this is the host name or ip address of the server**  
port=1585 # **this is the first TCP port. If you change this you must change the corresponding entry in the client/lib psiberworks.properties.**

name=works.12.03.00 # **this is the instance name. If you change this you must change the corresponding entry in the client/lib psiberworks.properties.**

**END OF DOCUMENT**

**Buildsmart HR Modules**  
**Technology & Architecture Overview**

**Version 14.04.00**