MYOB EXO EMPLOYER SERVICES

MyStaffInfo System Overview

September 2012

EXO EMPLOYER SERVICES

MYOB ENTERPRISE SOLUTIONS

Contents

Introduction

MYOB MyStaffInfo Overview

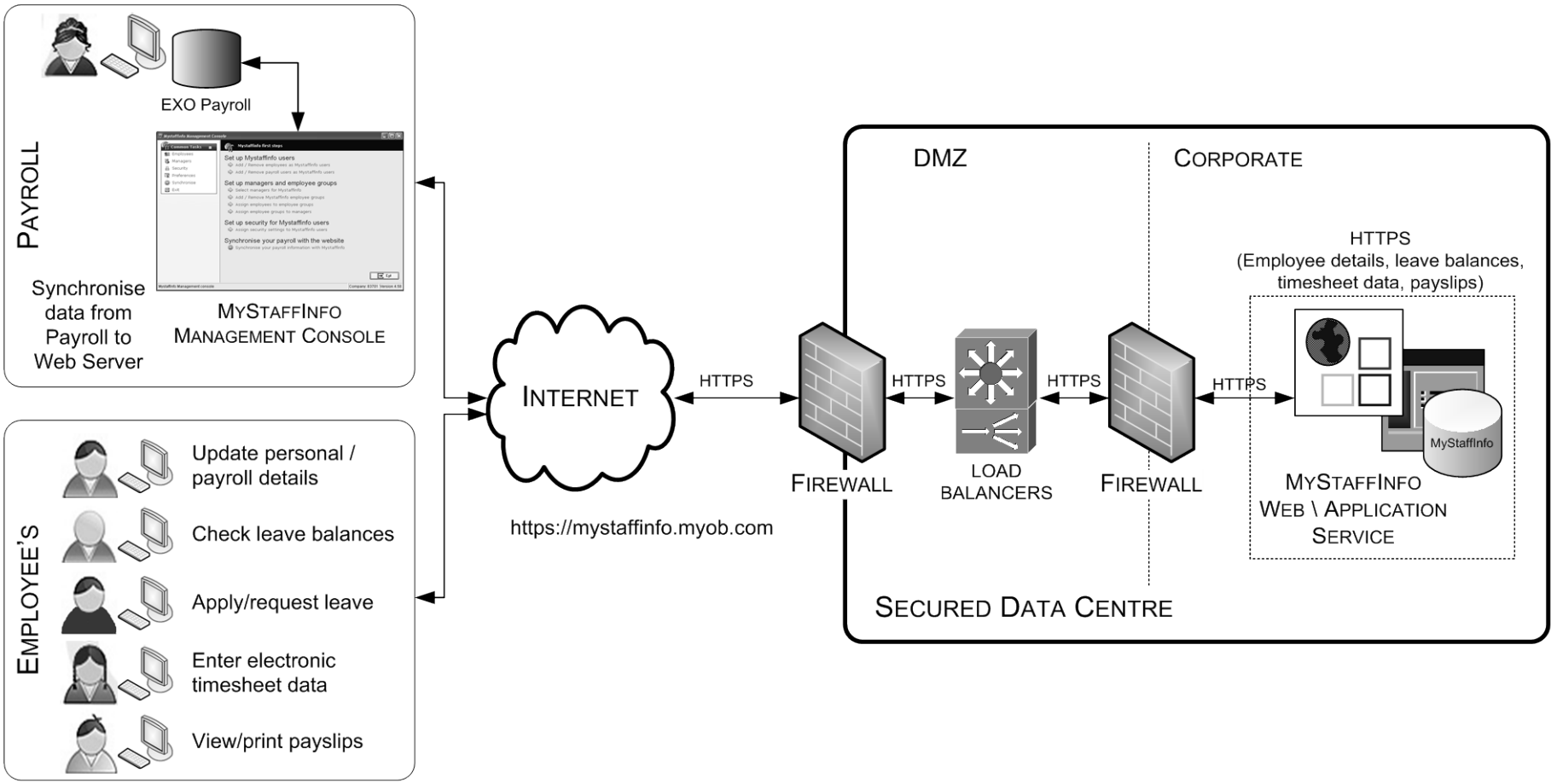
MYOB MyStaffInfo is a commercial web-based employee self-service that is developed, maintained and supported by MYOB. MYOB MyStaffInfo is a Software as a Service (SaaS) application, with data held in a multi-tenanted configuration. MYOB MyStaffInfo web servers are hosted at MYOB's secure Australian-based data centre.

The solution allows the exchange of information, pay and leave details between employees and an organisation's payroll administration team. MYOB MyStaffInfo saves payroll staff hours of time of double entry by allowing employees to access functions where they can undertake tasks themselves, including viewing payslips and leave balances, applying for leave and entering timesheet information. MYOB MyStaffInfo works in conjunction with the MYOB EXO Payroll (on-premise) solution, as data is synchronised between the two systems.

There are two software components:

1. the MyStaffInfo Management Console application, which runs inside the MYOB EXO Payroll system; and
2. the MyStaffInfo Server application that it communicates directly with. Communication is via standard HTTPS Internet protocols and standards.

MYOB MyStaffInfo Logical Topology



MYOB MyStaffInfo Hosting

MYOB Data Facility

MYOB MyStaffInfo is hosted in the MYOB data facility based in Victoria, Australia. The facility offers the following protection:

- Uninterruptible Power Supply (UPS) systems;
- Auto-start generator backup;
- Facility is monitored 24x7x365 days per year;
- Equipment stored in a secured area of the building, with full protection and intrusion alarms;
- MYOB IP core is a dual redundant symmetrical network core, based on switching and routing equipment from Cisco Systems.

The facility conforms to Payment Card Industry Data Security Standard (PCI-DSS). Also the facility follows ISO27001 certification guidelines but as yet has not completed formal certification within this area.

All direct access to the servers is through a specific named list of staff only. MYOB has a tailored, managed security solution that covers areas such as access control, alerts and escalation procedures.

MYOB MyStaffInfo Web Servers

The MYOB MyStaffInfo web servers are all high-end server machines utilising fail-over drive arrays and redundant power supplies. The web servers utilise Microsoft Windows Server 2003 RS SP2 operating systems and are using IIS 6.0.

Disaster Recovery, Management and Administration

Backups are completed regularly to provide protection against data loss and to meet regulatory requirements. The following backup schedule automatically undertaken:

- Incremental backups performed daily;
- A full backup undertaken every week;
- Weekly backups are held for five weeks;
- Monthly backups are held for twelve months; and
- Yearly backups are held for seven years.

Backups are stored on-site with data being sent off-site on a daily basis as part of the MYOB Disaster Recovery Plan. MYOB MyStaffInfo is configured in a highly available environment. Connectivity to the end user is via redundant firewalls and load balancers, while the servers are protected using VMWare technologies. Disaster recovery is provided through the use of offsite tape. MYOB does not disclose the provider of our offsite storage.

MYOB IT Services have access for viewing recent backups, and the restoration of data can be undertaken if required. The MyStaffInfo system is constantly monitored and alerts are responded to by an experienced IT team with escalation processes in place to minimise downtime as well as to deliver optimum performance and uptime.

MyStaffInfo Communication

Securing Electronic Communication

Personal information that is submitted to MyStaffInfo is protected through the use of the Hypertext Transfer Protocol Security (HTTPS) protocol.

MYOB MyStaffInfo also utilises a verified SSL certificate allowing the use of a high-grade encrypted (RC4 128 bit) channel when transmitting information over the internet, increasing data security and user confidence when using this solution.

This allows transmitted data to be encrypted and then sent via the Internet to the server, where once received, the data is decrypted. This is also works in reverse, with data being sent from the server to the client where data is encrypted as it travels across the Internet.

MYOB enforces HTTPS for all MyStaffInfo clients by re-directing all access through to this secure protocol.

You can confirm that any MyStaffInfo webpage is secure by checking that:

- the page address in the Web browser's tool bar or status bar begins with https://, or
- the padlock icon in the web browser's tool bar or status bar is locked.

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. MyStaffInfo is verified by the GeoTrust® SSL digital certificate.

SSL Digital Certificate

The MyStaffInfo web site has a digital certificate issued by GeoTrust®. GeoTrust® is a leading Secure Sockets Layer (SSL) certificate authority enabling secure e-commerce, communications, and interactions for Web sites.

With booming Internet trends and fraud, most website providers will not submit their private details on the web unless they know that the information they provide is securely transmitted and not accessible for anyone to view.

As MyStaffInfo utilises a verified GeoTrust® SSL certificate, it allwos MyStaffInfo to use a high-grade encrypted channel when transmitting information over the Internet, increasing user confidence when using this application.

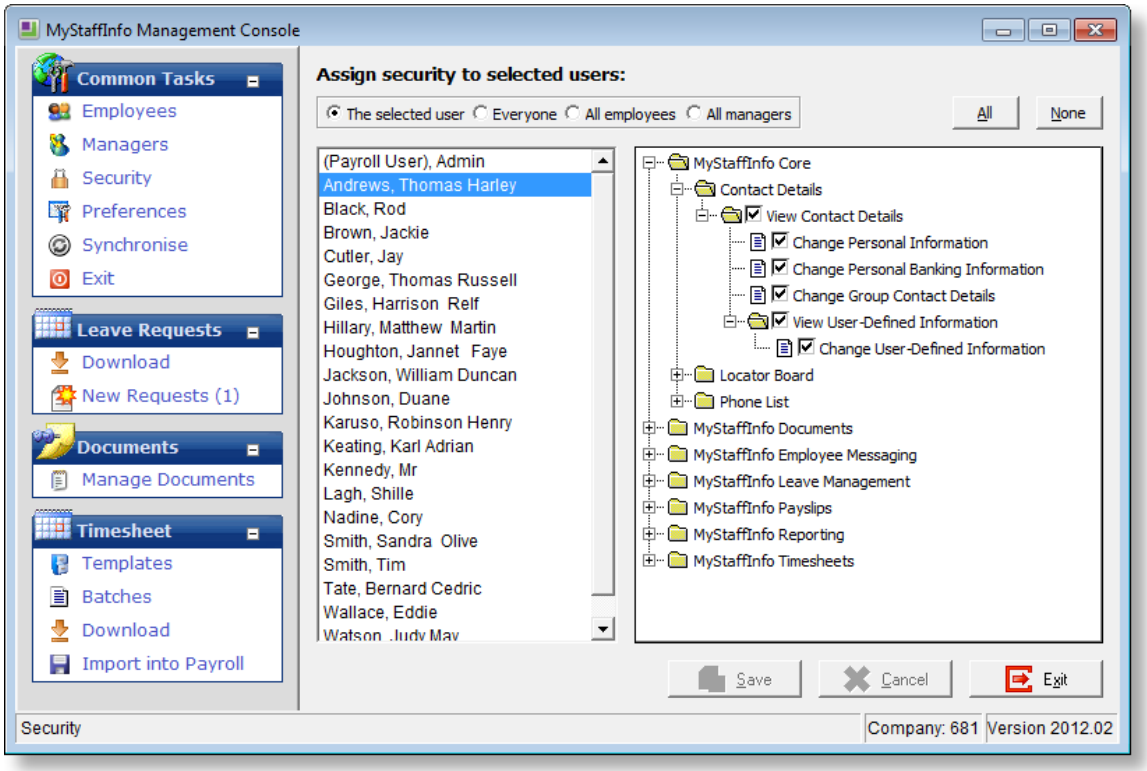
MyStaffInfo Employee Access

Employee Access Rights

MyStaffInfo Management Console provides extensive controls over what the employee is permitted and is not permitted to see. Simply check or uncheck boxes in the tree view to grant or prevent the viewing of components on the website.

The assignment of security options is task-driven. The recommended course of action is to:

1. Grant access to commonly used components, to all users at once, taking special care to ensure that restricted items are not selected;
2. Tailor specific access requirements to individual users as necessary, refining the lists of previously-ticked components from step 1, one employee at a time;
3. If you want to define access rights for users of the system who are not payroll employees of the payroll company in question, you can also elect options either globally or individually, for user-based logins, without altering the access rights for employee-based logins.



MYOB MyStaffInfo Web Login Security Controls

MyStaffInfo provides for organisations to enforce to specific employee password complexity. The system can be implemented to enforce the following password complexity settings:

- Minimum / maximum character length of password;
- Minimum numbers, alpha and non-alphanumeric characters used within password;
- Ability to enforce mixed case alpha characters within passwords;
- Ability for an employee to change their password.

MYOB MyStaffInfo also manages multiple failed login attempts by users. This feature enforces best practice across all organisations, that where a user fails six attempts to login, the user will be locked out for up to thirty minutes. Successful/failed login attempts are logged.

If a user has forgotten their password, they can request for their password to be sent to their nominated email address. Also, the organisation's payroll administration team can reset an employee's password if required.

The MYOB MyStaffInfo Application

The MyStaffInfo Management Console

The MyStaffInfo Management Console is an add-on to the EXO Employer Services suite. Once installed, it appears under the Pay menu in MYOB EXO Payroll.

Its primary functions are to:

- Assign groups of employees to managers, allowing managers to review activity that is specific to their assigned employees on the website
- Select employees for inclusion onto the MyStaffInfo website
- Select managers for inclusion onto the MyStaffInfo website
- Set security restrictions for each login
- Set up documents for upload to the website
- Set up Timesheet Templates and Batches for use on the website
- Retrieve timesheet transactions from the website and import them into the Current Pay
- Synchronise EXO Payroll information with the MyStaffInfo website

MyStaffInfo Management Console can only be accessed through MYOB EXO Payroll and as such is subject to all of the security requirements of the MYOB EXO Payroll application. MyStaffInfo Management Console cannot be run directly, for example from Windows Explorer, as it is fully embedded in MYOB EXO Payroll.

The MyStaffInfo Management Console communicates with the MyStaffInfo web server using common Internet protocols and standards. All defined communication ports and settings for proxy servers etc. can be fully defined from the MyStaffInfo Management Console.

By default the following ports are used for communication:

- HTTPS port 443

The following table provides an overview of the methods used for particular data transfer.

Data type	Description	Transfer Package	Encrypted
Employee data	Employee contact details including bank Account information	Compressed XML over HTTPS (Upload & Download)	Yes
Leave data	Employee leave balances and calculated year-to-date leave entitlement	Compressed XML over HTTPS (Upload & Download)	Yes
Timesheet data	Employee timesheet entry	Compressed XML over HTTPS (Upload & Download)	Yes
Payslips	PDF copy of employee payslips (also password protected by employee)	PDF over HTTPS (Upload)	Yes
Company Documents	Basic repository for Company non-sensitive documents	PDF over FTP (Upload)	No

The MyStaffInfo Server Application

MYOB MyStaffInfo is SaaS application that operates within an application pool under IIS 6.0 control. MyStaffInfo databases are held in a multi-tenanted configuration and as such, are not directly accessible from the Internet and are kept in a separate data storage area within the MYOB servers. Access to data and reports can only be made through the server application, requiring both authentication and authorisation before permission is granted to proceed.

The Server application is not customisable in any way, but the offering provides various setup configurations to allow an organisation to manage employee self-service functions.

Browser Compatibility

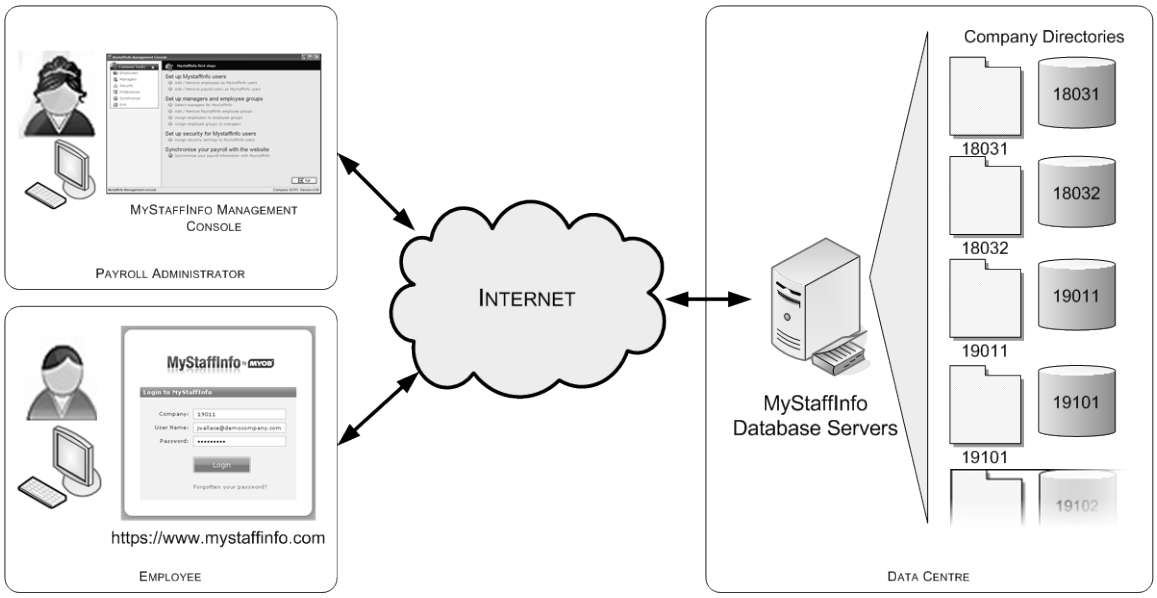
MyStaffInfo has been developed to conform to the World Wide Web Consortium (W3C) HTML standards. By complying with W3C standards, MyStaffInfo is developed to recognise the need to be compatible with other Web technologies as well to allow for any hardware and software used to access the Web, to work together.

MYOPB MyStaffInfo is capable of working with the following Internet browsers:

- Microsoft Internet Explorer – V7.0 and above recommended
- Mozilla Firefox – V3.0 and above recommended
- Safari – V3.0 or above
- Google Chrome – V 1.0 or above
- Opera – V9.0 and above recommended

Company Setup

The installation of MyStaffInfo is specific to a given company; there is no shared data. Each company has its own database and separate area for data and reports (multi-tenanted). Each company has its own specific user access rights only to those areas. The MyStaffInfo Management Console and Server application can only communicate for a given MYOB licence/registration. There is no way that one company can access another company's data.



Frequently Asked Questions

How is MYOB MyStaffInfo hosted?

MYOB MyStaffInfo is hosted in the MYOB data facility based in Victoria, Australia. The facility offers the following protection:

- Uninterruptible Power Supply (UPS) systems;
- Auto-start generator backup;
- Facility is monitored 24x7x365 days per year;
- Equipment stored in a secured area of the building, with full protection and intrusion alarms;
- MYOB IP core is a dual redundant symmetrical network core, based on switching and routing equipment from Cisco Systems.

How is data backed up?

Incremental backups are run daily, with a full backup once a week. Weekly backups are kept for 5 weeks, Monthly for 12 months and yearly for 7 years. Backups are stored onsite with data being sent offsite on a daily basis.

How are communications encrypted?

All communications are over SSL; no clear text is involved. Server data is multi-tenant and restricted by licence checks.

There is no encryption on data at rest in either the website or the local payroll system. Data on the website is not physically accessible except through the website interface, which is under SSL.

How does user authentication work?

Users log in with a username and password. Passwords are generated in MYOB EXO Payroll by the payroll admins. Passwords do not expire, but can be changed at any time from MYOB EXO Payroll.

The system can be implemented to enforce the following password complexity settings:

- Minimum / maximum character length of password;
- Minimum numbers, alpha and non-alphanumeric characters used within password;
- Ability to enforce mixed case alpha characters within passwords;
- Ability for an employee to change their password.

Where a user fails six attempts to login, the user will be locked out for up to thirty minutes.

Are user actions logged?

Successful/failed login attempts are logged, as are leave requests and timesheet approvals.

How does MYOB MyStaffInfo integrate with the payroll system?

There is a staged workflow. Leave requests on the website must be approved by managers. Only approved leave requests can be downloaded into MYOB EXO Payroll. Payroll admins are responsible for pulling the leave details from the website as part of their payroll process. The import is automated but must be triggered from EXO Payroll by payroll staff.

What Disaster Recovery Plan is in place for MYOB MyStaffInfo?

MSI is configured in a highly available environment. Connectivity to the end user is via redundant firewalls & load balancers while the servers are protected using VMWare technologies. Disaster recovery is provided through the use of offsite tape. Recovery of MSI to alternate location would be expected within 4 to 8 weeks in the event of a total disaster at the MYOB datacentre.

Are security/vulnerability reviews performed on MYOB MyStaffInfo?

Internal vulnerability scans are conducted on a quarterly basis. An external security review covering full penetration test and infrastructure assessment is done annually or if there is a major change to the environment. MYOB implements the Payment Card Industry Data Security Standards (PCI DSS) framework that aids in providing security processes including the prevention, detection and appropriate reaction to security incidents.