MYOB Exo Employer Services

Security and Disaster Recovery

Last modified: 4 March 2021

Contents

Introduction

What’s covered in this white paper?

Software applications have an increasingly crucial role in our lives, yet they are also a real security threat, with hackers always finding new ways to bypass security defences. This white paper looks at how to keep Exo Employer Services secure in your operating environment.

The purpose of this document is to provide essential information and best practices for installing and using Exo Employer Services.

- The **Protect Your Data** section provides an overview of securely installing Exo Employer Services in a standalone environment and network environment.
- The **Disaster Recovery Plan** section describes how to plan for disaster discovery during unplanned incidents.

Need assistance? If you have any questions or you need assistance with any of the topics in this document, please contact your MYOB Accredited Business Partner or MYOB Support.

Note: An active support plan is required when contacting MYOB Support.

Protect Your Data

Considerations for standalone Windows PCs

The following points should be considered to make Exo Employer Services secure in a standalone windows environment.

- Set up your Windows environment to automatically install the latest patches for your PC.
- If your Windows version comes with Bitlocker encryption, make sure to use the Bitlocker encryption for your local hard drives.
- Use a Windows Local Account with a strong, secure password.
- Make sure the System Restore option is enabled and your Windows system is configured to revert to an old configuration after any undesired changes happen in your system.
- Use Antivirus software and enable Windows Firewall. Note: Having firewall and antivirus software in place can slow down the product. MYOB generally recommends you set up an exclusion zone for payroll software.
- If any other users use the same PC and you do not want them to access your Payroll data, make sure that the payroll folder is not shared and no-one has any access to it except the actual user.

Search the Windows Help on the Microsoft support website for information on setting up the Windows security features mentioned above.

Considerations for networked environments

The following points should be considered to make MYOB Exo Employer Services secure in a networked Windows environment.

- Create separate Windows logins for all users and do not allow administrator access to everyone. Do not used shared accounts—separate logins provide a clearer audit trail.
- Clients with proxy should have proxy ports open for MSI syncing.
- Exo Employer Services should be installed on a secure server, and only restricted payroll/HR users should be given folder permissions for the payroll software and data folder.
- Create separate Exo Employer Services logins for all users and do not allow administrator access to everyone.
- Set up a strong password for the Exo Employer Services admin login. By default, the admin password is not strong in the AU edition, and in NZ edition there is no password on the default admin account.
- Do not allow any users to download random utility programs from internet. The data files for Exo Employer Services can be viewed easily using third-party programs if users get access to the payroll data folder.
- Restrict access to forms of removable media or file transfer:
    - Disable unnecessary access to removable media storage.
    - Disable unnecessary access to wireless devices/unknown SSIDs.
    - Segregate the server from other parts of the wired/wireless network that could contain file shareable folders.
    - Restrict access to internet-based file sharing technology.
    - Third-party server additions can be used to monitor file or folder usage or uploads.
- If you are using Windows Terminal Server, MYOB recommends that the Exo Employer Services installation folder be on the Terminal Server's local drive. This avoids many potential network-related issues.
- Employees will come and go in any organisation, so it helps to have an **employee exit IT security checklist** to make sure that there are no gaps in your defences after they leave. If an employee leaves, you should:
    - Revoke email access
    - Revoke windows access
    - Revoke access to Exo Employer Services
    - Change any password shared with multiple members of staff when an employee leaves.
- Consider a folder-level audit policy for the Exo Employer Services application folder and data folder, normally C:\PAYROLLV and all subfolders. The following documents from Microsoft will help you to enable a folder-level audit policy on your Windows machines:
    - Plan for File Access Auditing
    - Apply a basic audit policy on a file or folder

See the Education Centre websites for information on setting up login accounts in Exo Employer Services:

- MYOB Exo Employer Services Education Centre (Australia)
- MYOB Exo Employer Services Education Centre (New Zealand)

Disaster Recovery Plan

It is vital to have payroll disaster recovery plan in case an Exo Employer Services server or workstation goes down.

Disaster recovery and business continuity planning are integral parts of the overall risk management for an organization. In the event of a disaster, the continued operations of your company depend on the ability to replicate your IT systems and data.

Exo Employer Services is a desktop applicationby default, the data is stored in a local Windows folder or a networked Windows folder, depending on the configuration.

It is possible to use Exo Employer Services on a Windows Terminal Server hosted in the cloud. This could be one of the best possible ways to plan for disaster recovery and business continuity.

Other options available are regularly taking backups of the payroll folder (including software and data) using network storage devices or portable hard disks. It is always a best practice to keep multiple copies of the backup in each location if your business is in multiple regions. Backups should be kept onsite and offsite.

It is possible to use network cloud drives like OneDrive or Google Drive for your Exo Employer Services backups.