EAPconnect Account Security

August 8, 2019

In today's world, everyone needs to be focused on security and protecting their data. We all have heard about data breaches where millions of people's personal data has been leaked. Many of those leaks have even included passwords which is hard to imagine still happening today. In RIAA, all passwords are stored with a one-way encryption so that there is no way for anyone to determine the password value. All we can do is compare the password entered by the user to the encrypted version in the database.

However, just having passwords is not sufficient today. Any software system that has privileged information is a likely target for attack. One of the primary means of attack is to compromise a user and access the system as that user. To address this, systems need to have a means to do authentication that ensures the user is who they claim to be.

One way this is addressed today is to use an authentication provider that has advanced capabilities. We have implemented Microsoft Accounts to handle the authentication for EAPconnect. This allows our system to rely on Microsoft to do the authentication of users which is a great advantage because they have made huge investments into their authentication systems ensuring significant security. Microsoft Accounts allow for advanced authentication such as Multifactor Authentication which require a user to have more than just a password to prove their identity (text message, phone call, authenticator app, etc.).

Microsoft Accounts come in two forms: Organization accounts and Personal accounts.

Organization accounts are linked to your organizations Active Directory. This means that you use the same username and password to login as you do on your computer at work. This has some great advantages for your organization such as:

- User accounts are controlled by your IT department.
- Your organization can control password policies.
- Your organization can choose to enable Multifactor Authentication based on the user's location (disabled inside the office and required outside the office).
- When a user leaves your organization, the IT department disables their account.
- You can track application usage by user.

Organization accounts can be obtained through various Microsoft products. The most common is through an Office 365 subscription which is how most companies get started. If your organization has an Office 365 subscription for some of your staff, then you have the ability to use organization accounts even if not everyone has an Office 365 subscription. Microsoft offers special pricing to Nonprofit organizations that is very low cost and includes the Microsoft Office applications (Word, Excel, Outlook, etc.). If you would like information on this, please let us know.

If you already have Office 365, then your IT staff should already have the synchronization for Active Directory setup, and you are ready to go.

Personal accounts are free accounts that individuals setup. These are accounts with an email address of @outlook.com, @hotmail.com, or @live.com. Personal accounts do not let your organization manage the user's authentication, but you still control what the user can do within EAPconnect. While personal accounts don't have the advantages of an Organization account, they are still a step up from standard 'built in' types of authentication.

To setup a personal account, a user can go to www.outlook.com and click the 'Create Free Account'.

2433 South Ninth Street
Lafayette, IN 47909
765-474-5402 Phone
765-474-4485 FAX

#2 Chase Park
Logansport, IN 46947
574-753-0411 Phone
574-722-3894 FAX

www.roeing.com

We have a training video that will walk you through setting up users in EAPconnect. This video is available from a link inside EAPconnect and will walk you through the steps of getting your users access with either type of account.

2433 South Ninth Street
Lafayette, IN 47909
765-474-5402 Phone
765-474-4485 FAX

#2 Chase Park
Logansport, IN 46947
574-753-0411 Phone
574-722-3894 FAX

www.roeing.com