Guide to Using Azure Active Directory with Ariett Cloud Purchase and Expense

Introduction to Azure Active Directory for Cloud Customers:

This document will review Azure Active Directory (AAD) capabilities, how to activate AAD for your organization, and how to transition your employees from using Forms Authentication. Ariett supports AAD as the Cloud user management system that is the equivalent of Microsoft Windows Active Directory (AD) on premise. AAD not only provides IT Admin with a central location for managing usernames and passwords but also provides Users with single sign on to Ariett, Office 365 and other Azure AD applications. Ariett's single sign-on option through AAD can either stand alone or, more commonly, integrate with your on premise AD.

Here is a link to a useful introduction video on Azure Active Directory on Microsoft Azure's website: http://azure.microsoft.com/en-us/documentation/videos/what-is-active-directory/.

How Azure Active Directory Works:

AAD makes it easy for your users to authenticate when accessing Ariett or other AAD supported applications, especially when your users are accessing the software outside of your company's internal domain. For instance, if an employee is on a personal tablet, laptop or phone, the employee can log in to Ariett by authenticating the employee's login credentials through Azure Active Directory.

When an employee logs in to Ariett, the user is seamlessly redirected to the AAD login site where the username and password are authenticated against the username and password stored in AAD. In most cases, Cloud customers pull username and password information from their on premise AD to AAD using the Azure AD Connect tool; however this is not required. AAD can be used as independent Cloud user management and authentication tool for companies using Ariett Cloud Purchase & Expense software.

Additionally, users can be added to AAD who do not exist in your AD if you need to add users who should not have access to your internal domain. In this case, Ariett identifies and matches the AAD user with the Ariett user based on the user email address.

Steps to Activate Azure Active Directory for Use with Ariett:

Your IT team is responsible for activating AAD. Please go to Microsoft Azure and create an Azure and an Azure Active Directory Account – there is no charge for the standard service. Here are the steps:

Step 1: Go to http://azure.microsoft.com/en-us/pricing/details/active-directory/ and click on "Try for free."

Step 2: Create an Azure Active Directory for your organization.
NOTE: This step is unnecessary if your organization already has an AAD by using Office 365 or another AAD supported application.

Step 3: Browse to find Ariett and authorize the Ariett product on your AAD account. Then, synchronize your users with Ariett.

How to Synchronize Azure Active Directory with Your Active Directory:

Additionally, you may sync your on premise AD with AAD, by downloading the Azure AD Connect wizard. Once you have downloaded and used this tool to sync your on premise AD users with AAD, you will be able to automatically import usernames and passwords directly from AAD when in the User Setup window in Ariett.

Having the ability to pull this information directly from AAD will save your administrators time and enhance security because when a user is disabled in AAD (e.g. when an employee leaves your organization), the user is also disabled in AD and all Azure applications. AAD also supports most AD policies already established by your organization.

Here is a link to useful information about Azure AD Connect and a link to where you download the Azure AD Connect tool from Microsoft:

- http://blogs.technet.com/b/ad/archive/2014/12/15/azure-ad-connect-one-simple-fast-lightweight-tool-to-connect-active-directory-and-azure-active-directory.aspx
- http://connect.microsoft.com/site1164/program8612

How to Transition from Using Forms Authentication to AAD:

If your organization is transitioning from using Forms Authentication to using AAD, you can continue to use Forms Authentication as well as AAD. However, we recommend that your organization eventually move to only using AAD to ensure a secure and simple login process. Your employees' email notifications can only contain one login link for Classic and Touch, so we recommend that email notifications are set to use the AAD url. Once you are ready to complete the transition to AAD, an Ariett Consultant can optionally set all users' passwords (or some users' passwords) to an unknown password for Forms Authentication to enforce use of AAD.

Azure Active Directory Pricing and Feature Options:

There is no additional Ariett cost associated with deploying Microsoft AAD for use with Ariett. All of the following features are included with Microsoft's AAD standard service:

- Directory as a Service
- User and Group Management
- Device registration
- Directory Objects 1
- End User Access Panel
- SSO for SaaS Apps
- Directory Synchronization
- User-based Access Management and Provisioning
- Basic Security Reports

Microsoft offers two additional AAD Service levels: Basic and Premium for a Fee. Basic service provides the previous features and the following additional services for a fee:

- Logon/Access Panel Branding Customization
- Group-based Access Management and Provisioning
- Self-Service Password Reset for Cloud Users
- Secure Remote Access and SSO to on-premises web applications

AAD's Premium service provides the previous features and the following additional services for a fee:

- Self-Service Password Reset for Users w/ writeback to on-premises directories
- Self-service group management for cloud users
- Multi-Factor Authentication (for cloud and on-premises applications)
- Advanced Usage and Security Reports
- Cloud App Discovery
- Microsoft Identity Manager User CAL

For additional information about AAD's features and pricing, click on this link: http://azure.microsoft.com/en-us/pricing/details/active-directory/. You will contract directly with Microsoft for these additional service levels.