**Active Directory Integration for a mobile management solution**

**By**

**Mark McDaniels**

**Student ID: 008094156**

**D342 Task 3**

**Western Governors University**

**Table of Contents**

1. AD Integration Summary ….................................................................. 3
2. Service Interactions …........................................................................... 5
3. Disaster Recovery and Security Improvements …................................ 6
4. Financial Budget …............................................................................... 7
5. Project Methodology …......................................................................... 8
6. Solution Evaluation …......................................................................... 10
7. Postmortem and Continued Support …................................................ 11

References ….............................................................................................. 13

1. **AD Integration Summary**

When the Covid Pandemic hit the Southeastern United States during the Spring of 2020, many businesses were forced to adapt. Paper Pusher, LLC had to take on a work-from-home strategy quickly. Their willingness to adopt new technology was light years ahead of its IT (Information Technology) department's maturity level. This forced Paper Pusher to adopt an ad hoc mobile strategy. One of the biggest challenges was to keep consistency, both in authentication and ensuring everyone had access to the required tools. It was impossible to purchase, deploy, and manage mobile standard devices within a reasonable time. They adopted a strategy that involved Bring Your Own Devices (BYOD) for speed, and financial necessity. In 2020, the company was using local servers running Office 2013 on their Windows based network. They knew Office 2013 would not be supported in Microsoft 365 after April 11th, 2023 (Microsoft, n.d.). This will force Paper Pusher to move to Microsoft 365 exclusively to continue security and support updates.

Users are supposed to only access their email through the company’s portal. However, people intermittently use their default mail client that came with their phone email because it is more convenient. Employees can do this because proper authentication and authorization has not been implemented. The current setup does not include best practices or ease of use in mind. It is even affecting internal department correspondence. The inconsistency is creating confusion across the organization. Paper Pusher is moving to Microsoft 365 because Office 2013 is no longer being supported. This project is designed to make the transition as smooth as possible. Outlook did not add functionality for Gmail until April of 2023. The April update did not fix the security concerns. Outlook app does not give you the opportunity to have two-factor authentication (Zac Bowden, 2023). It is not possible to maintain security and functionality.

Paper Pusher needs a consistent authentication solution that allows Single Sign On with Azure Active Directory. Azure AD Connect will be a solution that works with on-premises Active Directory to allow the local version’s log-in credentials for Azure AD (Microsoft, 2023 May).

Once that integration is successful, a second service is necessary for mobile devices. There is no efficient way to manage authentication and authorization for Paper Pushers mobile devices in this current state. Microsoft Intune is a cloud-based solution for managing mobile devices (Microsoft, 2023 April). It gives the administrator a way to manage users and devices from Microsoft’s Intune administrator center. This will allow policy and compliance in a simpler, more effective way. It gives developers a way to automate certain aspects of mobile management that would be time and cost consuming beyond the company’s internal programming capacity. This will, with Microsoft Intune, allow for an integrated solution that makes it easier for users to maintain a consistent mode of communication.

**B. Service Interactions**

There will be three main services integrated within Paper Pusher’s infrastructure, Microsoft 365, Microsoft Intune, and Azure AD Connect. The company is currently running an on-premises Active Directory. The employees use Paper Pusher’s employee portal for access to their company email or their Windows machine. Other Office products are locally installed on their main devices. There is no current strategy for users to access their applications or files securely from remote devices other than the portal. To address this, the company is going to deploy Azure Active Directory Connect (ADC) to avoid on-premises user information duplication, Microsoft Intune (Intune) for mobile devices, and Microsoft 365 for Office applications. ADC is a cloud-computing solution that will integrate Paper Pusher’s current Active Directory users and rules with Azure Active Directory (Microsoft, May 4). Microsoft 365 will be connected to ADC so that current users associated with on-premises accounts can log-in seamlessly (Microsoft, March 15). Intune will manage all the devices associated with the new Azure Active Directory.

They work in concert like this:

Microsoft 365 includes Azure Active Directory as its identity and management account (IAM) service. This will allow Azure AD to synchronize with the local Active Directory. The identity model we will be using is called the Password hash synchronization method. The local Active Directory Domain Service (AD DS) will use ADC to communicate with Microsoft 365's built in Azure Active Directory. Once a connection is created between AD DS and Azure AD, AD DS will send password hashes to Azure AD. This allows Azure AD to authenticate users. It is called Password Hash Synchronization because the password hashes are used by Azure AD instead of having the AD DS do the authentication. Then Microsoft Intune will work with Azure AD for user and device management.

Azure Active Directory Connect is a way for businesses to allow their local AD DS to work with Cloud services without having to recreate users, groups, and policies. There are two identity models to choose from. The Password hash method as previously described, and Pass-through method. The Pass-through method has Azure AD redirect the request to a local software agent that then talks to AD DS to authenticate (Microsoft, March). The Pass-through method allows administrators to immediately enforce password policies, and login times. This is not a priority and would be a more complicated project.

Microsoft Intune makes the process of managing users and devices simpler. It allows administrators to apply policies, configuration, and conditional access. It is designed to integrate directly into Microsoft 365 Active Directory. Intune has self-service password reset that reduces some administrative needs (Microsoft, April).

**C. Disaster Recovery and Security Improvements**

Availability of data is paramount for any business to successfully operate. An important part of this solution is to take away that risk as much as possible. Cloud solutions are designed to be reliable and available without the need for intervention. Azure is built with NIST’s cloud-computing standards in mind (NIST SP 800-145, 2011). This is resolved in Azure by logically and physically creating separation to contain dependencies only where appropriate. Without proper data replication and resource access the business will suffer. It is unlikely for the whole Southeastern Region of the United States to have no availability zones functioning (AZ AG, n.d.). Putting two virtual machines in your availability set gives the company a 99.95% SLA (Service Level Agreement) of uptime (AZ AS, n.d.). As we move to Microsoft 365, we are moving away from an on-premises solution that involves physical tape copies of data. Implementing these solutions for device management allows users to access and generate new data that will now be part of a cloud solution. As part of the security maturity this takes one step towards fulfilling our commitment to the CIA Triad (Washington University in St. Louis, n.d.).

One of the most important parts of this change is the inherent security capabilities of these services. Microsoft is more committed to cyber security and data protection than anyone in the industry. They built Azure’s services with security in mind from the beginning (Azure, 2022). By using Microsoft solutions our cyber security posture matures significantly. This solution closes holes that currently exist. It was a main priority to improve security. Integration using Microsoft Solutions designed for interoperability helps close many areas present in running a separate portal.

**D. Financial Budget**

The cost of the entire solution is quite reasonable. An upgrade from Microsoft 365 (365) Standard Business to the Premium version will cover both software solutions. 365 has Azure Active Directory included as part of the service, and with Premium 365, the Azure AD subscription will increase as an extra benefit. The upgrade to 365 Premium is necessary for Azure Intune. Azure Intune is an add-on that is only available in Premium 365 plans and up. The Premium upgrade of Microsoft 365 will increase the cost per user by $10.50 (Microsoft 365, n.d.). As part of this upgrade, there are some added benefits that justify the increase beyond the mobile security management capabilities. All users will gain the ability to have desktop versions of the 365 suite. It will allow users to use an environment that they are already familiar with. The security increases associated with this upgrade will advance our security posture beyond what is internally achievable. It includes Enterprise-grade endpoint security, Data loss prevention capabilities, and conditional access security for employee access (Microsoft 365, n.d.).

**E. Project Methodology**

We have chosen to use the Project Management Life Cycle (PMLC) for this endeavor (Flynn, T.A., 2007). It is a clear and useful method that is widely used throughout most industries. It consists of five phases to achieve project success. The phases are:

Initiation: The Project Sponsor and Project manager begin to organize the objectives of the project. They decide who are the main stakeholders that must be considered. They figure out the scope of the project and identify constraints.

Planning: The path to success is decided in this phase. This is the phase where we set a budget. We decide who is responsible for various aspects of the project. Who oversees what. We will decide the milestones, times, and project tasks. We will design teams associated with specific duties.

Execution: At this phase we do the work. Workflows are organized. Tasks and duties are delegated to the proper people and teams. Project resources are allocated and managed during this phase as well.

Closure: Now that the majority of the work has been done, the other administrative duties are handled in this phase. The project manager begins releasing resources. This may include people, equipment, removing access, and closing budgets. Now the project manager will ask important questions about the project. Have the project goals been achieved? How did the team perform overall?

Closing down: This section of the PMLC is not always given proper attention. It is important to make sure all aspects of the project are over. Doing a post-mortem for future success is paramount for continued success. This allows the organization to end the process with a finality that gives everyone involved a sense of accomplishment. People deserve to be thanked, and to take a win.

Using the PMLC will help us meet our deliverables and stay within budget. Our first milestone is to create the connection between our on-premises Active Directory Domain Services, Azure AD Connect, and Microsoft 365 AD. This will result in a fully functioning AD DS synchronization with Microsoft 365 AD. The second milestone will be the integration of Microsoft Intune for mobile management. The final milestone will be a successful rollout of this solution to production.

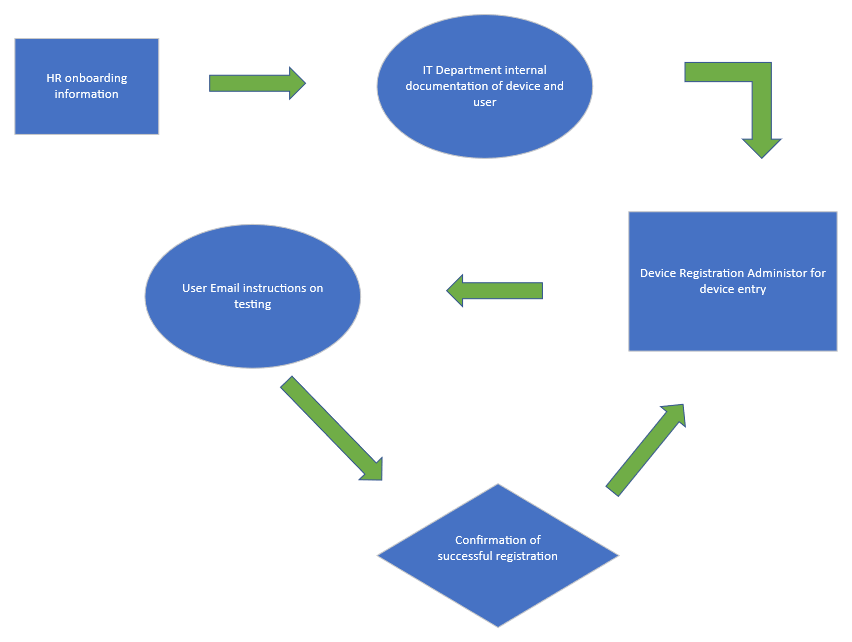
**F. Solution Evaluation**

There are integration of the three services AD DS, ACS, and 365. Proper testing of solutions is necessary. At each stage we will thoroughly investigate what has been implemented. The Active AD Connect will interact with our local Active Directory to make it possible for on-premises users to be synchronized with Microsoft 365 Azure AD. We will test ADC installation by making sure that Microsoft Server 2019 has a green circle visible. This denotes success. For ADC to connect to Azure AD, there are two ways to make sure the service is working properly. If a synchronization attempt failed. an email would have been sent to the designated administrator. The second way is to look at the Azure portal. If it has been successful, you will see a green check mark. If there is an issue, it will be an orange triangle alerting an error (Microsoft Exchange Online, n.d.).

To check if Microsoft Intune is operable, you would use Intune’s Dashboard. Navigate to “Devices,” and then “All Devices” for a list of registered devices. If the device you are looking for is present, then it was a successful integration of Microsoft Intune (Crystal-MSFT, 2020). If all these tests prove successful, you are ready to start entering data.

**G. Postmortem and Continued Support**

Tests have passed, and we are ready to begin using/supporting the solution. The first thing to be done is to delegate device registration responsibilities. Each device’s information should be available to this administrator. The administrator will be designated as the point person for early transition, adoption, and onboarding. It will be reviewed in two months to ascertain workloads and general duties for improvement. A process for confirming device registration must be followed. See diagram:



In review, we will lean heavily on a designated administrator for building long term strategies for onboarding, offboarding, and general device management procedures.

After devices are registered, the security team will be given the task of configuring users and devices in Microsoft Intune. The starting permissions are set to a default that consists of only accessing Microsoft 365 products associated with their previous policies in Microsoft Office. The security team will then begin a new project on setting appropriate least privilege policies.

At completion, the project should begin to show productivity gains immediately. Users should have an easy time transitioning because the decision to upgrade to Microsoft 365 Premium to get desktop versions of Office applications was implemented. Users do not have to learn new software. Communication and collaboration are now integrated across the company. Default email phone apps will no longer be able to log in. The two-factor authentication built into Azure AD forces mobile users to use Microsoft 365 mobile applications for work-related duties (Microsoft, 2023 May). Training will begin for Human Resources on what data is needed for onboarding as part of the ongoing support for the finished project. A post-project committee will be established to check in on deliverables. They will make recommendations accordingly.

With the successful implementation of this project, security posture and maturity will increase beyond our internal capacity. End-point security, 2FA, all internal communication, and other improvements from moving to an integrated Microsoft solution will have a significant impact on the success of the business (Microsoft, 2023 April).

Azure Geographies. (AZ AG, n.d.) *Find the Azure geography that meets your needs.* <https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies/#overview>

Azure Documentation. (AZ AS, n.d.) *Availability sets overview.* <https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview>

Azure Documentation. (AZ D 1, n.d.) *Hybrid Azure AD joined devices*. <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid>

Azure. (2022, November 15). *Introduction of Azure Security*. <https://learn.microsoft.com/en-us/azure/security/fundamentals/overview>

Microsoft. (n.d.) S*upport and security updates for Office 2013 have ended*. <https://www.microsoft.com/en-us/microsoft-365/office-2013-end-of-support>

Microsoft. (2023, May 4) *Azure AD Connect and federation*. <https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-fed-whatis>

Microsoft. (2023, April 4) *Microsoft Intune securely manages identities, manages apps, and manages devices*. <https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>

Microsoft. (2023, March 15) *Determine your cloud identity model*. <https://learn.microsoft.com/en-us/microsoft-365/enterprise/deploy-identity-solution-identity-model?view=o365-worldwide>

AWS. (AWS DSP, n.d.) *AWS Directory Service Pricing*. <https://aws.amazon.com/directoryservice/pricing/>

AWS. (AWS FAQ, n.d.) *AWS Directory of Service FAQs*. <https://aws.amazon.com/directoryservice/faqs/?nc=sn&loc=5>

Bowden, Z. (2023, April 4). *The new outlook for Windows app finally gains support for Gmail accounts*. <https://www.windowscentral.com/software-apps/office-365/the-new-outlook-for-windows-app-finally-gains-support-for-gmail-accounts>

Microsoft 365. (n.d.) *Reimagine productivity with Microsoft 365 and Microsoft Teams*. <https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products>

Microsoft Exchange Online. (n.d.) *How to identify DirSync or Azure AD Connect provisioning error in Office 365*. <https://support.microsoft.com/en-us/topic/how-to-identify-dirsync-or-azure-ad-connect-provisioning-errors-in-office-365-a7f20b7c-13e2-d813-6422-c0917519cb43>

Crystal-MSFT. (2020, November 5) *Intune enrollment check*. <https://learn.microsoft.com/en-us/answers/questions/152724/intune-enrollment-check>

NIST SP 800-145. (2011, September). *The NIST Definition of Cloud Computing*. <https://csrc.nist.gov/publications/detail/sp/800-145/final>

Washington University in St. Louis. (n.d.) *Confidentiality, Integrity, and Availability: The CIA Triad*. <https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad/>

Flynn, T. A. (2007). *Integration of the project management life cycle (PMLC) and the systems development life cycle (SDLC) in accelerated project efforts: adapting project management best practices to unreasonable requests*. <https://www.pmi.org/learning/library/integration-pmlc-sdlc-7262>