**Introduction**

The objective of this initiative is to develop a fully configured Azue AD environment with multiple integrations that are in high demand by our customers and cover identity and access management scenarios that challenge our clients. A key goal is to develop a scripted and pre-built methodology for configuration that would reduce human errors and accelerate adoption.

**Actors**

The integration has capabilities for different types of users (or personas):

**End Users** will use Azure AD to perform self-service tasks like request access, reset password etc. and use Azure AD’s strong authentication capabilities to securely access enterprise applications.

**Identity Administrators** will use Azure AD to manage access across many systems, including Active Directory and other on-premises applications, Azure Cloud and other SaaS applications.

**Security Administrators** will use Azure Sentinel to monitor Azure and on-premises systems for security related events.

**Identity and Access Management (IAM) Processes**

The integrated solution will support the following capabilities:

1. Authoritative Source Integration (Workday
2. Complex Joiner, Mover and Leaver scenarios, including birthright access is utilized to provide the End User with access to applications, such as ServiceNow, which are needed the first day the end user is employed. Birthright access by departments will vary and will be automated. For example, an end user on the sales team would be provisioned to Salesforce as part of birthright access.
3. Request and Approval Processes
4. Self-Service – First Time User Login and Registration and Password Management
5. Device Management
6. Compliance Reports
7. Identity Administrator Dashboards - KPIs and Metrics
8. Azure Privileged Identity Management (PIM) will be enabled to allow further security for high value assets within an organization. PIM allows for management, control, and monitoring to resources in Azure AD, Azure, Office 365 and other Microsoft online services. This reduces the chance of malicious actors accessing sensitive data. To further lock down data Just in Time (JIT) provisioning will be utilized for Azure VMs. JIT forces users to request and only access services when needed.
9. Multifactor authentication will be set up to prompt the end user during the sign-in process for an additional form of identification. Azure AD allows for various options to allow the second form of authentication. This will include a text message, OATH hardware token, phone call, or utilizing the Microsoft mobile authenticator application. The type of authentication used will be defined by administrators.
10. Conditional access will be used for cloud applications to specify that when specific conditions are met access will be allowed or blocked. The decision to allow or block access based on the defined policy. This will include setting controls around conditions such as sign-in risk, location, device, or to enforce multifactor authentication.

**Integrated Systems**

SaaS Applications

**ServiceNow(SNOW):** SNOW is a leading SaaS solution for technical management support, including helpdesk and IT service management. Many of our clients prefer SNOW for their IT support staff to manage service tickets. Microsoft Azure AD will showcase that wherever required, identity management related service tickets will be automatically created based on approved access needs of users. Additionally, Azure AD will provide user management and SSO capabilities to SNOW

**Salesforce:** Salesforce is a leading cloud based customer relationship management (CRM) technology. Integration with Azure AD simplifies user management workload for IT administrators and provides SSO capability for users.

**Microsoft O365:** Microsoft’s enterprise software are ubiquitous across our clients and Azure AD is the standard for managing user’s access to enterprise licenses and SSO.

On-premises Applications

**Active Directory:** Integration with Azure AD will simplify user management on Active Directory. Due to regulatory commitments, business risks and strategic decisions like M&A, many organizations employ and complex AD infrastructure with a variety of requirements for different domains. For example, separate identity governance procedures for different countries, integration with acquired business entities, password management etc. A key goal of this initiative is to develop a strong configuration recommendation on how complex Active Directory setups will be integrated with Azure AD and develop leading recommendations around a variety of real world scenarios. Additionally, many organizations are exploring options to move from Active Directory Federation Service based SSO to cloud. This initiative will develop recommendations how this will be achieved using Azure AD.

**Legacy Applications:** Many of our clients continue to rely on legacy custom built applications for their business and are exploring options to protect their legacy applications via SSO and automate user management to such applications. This initiative will demonstrate a proven design pattern to facilitate this requirement.

**Mobile Applications:** Many of our clients continue to rely on Android/iOs applications for their business and are exploring options to protect their mobile applications via Oauth and automate user management to such applications. This initiative will demonstrate a proven design pattern to facilitate this requirement.

APIs

**Securing APIs:** Securing API integrations is a key ask from our clients. In this initiative we will develop proven design patterns on how APIs will be secured through Azure AD. This would include management of API keys and using end user context. The demonstration would include capabilities to integrate these APIs in modern web and mobile applications.

**Azure Sentinel**

Security Administrators will utilize Azure Sentinel to review alerts, reports, dashboards, and threat detection. Sentinel centralizes information from users, devices, applications, on-premise infrastructure, and Azure AD. Sentinel will be used to configure security rules and incident response playbooks. Utilizing Azure Sentinel allows Security Administrators to gain an understanding of the threat landscape across the enterprise.