Summit Marketing

SOW xx004 for agreement to perform consulting services to Oakwood

DATE	SERVICES PERFORMED BY:	SERVICES PERFORMED FOR:
Sept 19th 2025	DKB Innovate 321 Sycamore Ave. Frisco, TX 76543	Summit Marketing 123 South Street Manhattan, NY 54321

Index

- Engagement Resources
- Executive Summary
- Current Environment
- Project Goals & Scope
- Proposed Solution
  - PS.1 Server Platform
    - PS.2 Network Modernization
      - PS.3 Backup & Disaster Recovery
        - PS.4 Management & Security
- Implementation Plan
- Deliverables and Benefits
- Assumptions & Exclusions
- Licensing & Subscriptions
- Decommission and Degassing
- Solutions Diagram
- Out Of Pocket / Invoice
- Completion criteria
- Project change control procedure
- Sign Off

Engagement Resources

Name	Role	Contact
Zachary Gafford	Solutions Engineer	Xxx-xxxx xxx.xxxx@xxxx.com

Executive Summary

Summit Marketing has rapidly adopted numerous cloud-based (SaaS) applications, leading to significant credential sprawl. Employees maintain 10 or more separate usernames and passwords, making offboarding and access management difficult and creating security risks. This proposal presents a comprehensive plan to leverage Microsoft 365 and Azure Active Directory (Azure AD) as a central Identity Provider (IdP) to consolidate and secure user logins.

Current Environment

Microsoft 365	E3 licenses with Azure AD for M365 logins.
non-synced accounts	Users maintain separate, non-synced accounts for key applications
Core Apps	- Salesforce - Slack - Zoom - Dropbox - Custom marketing analytics platform supporting SAML 2.0

Project Goals & Scope

- Configure Azure AD Single Sign-On (SSO) for Salesforce, Slack, Zoom, Dropbox, and the custom marketing analytics platform.
- Centralize user provisioning and de-provisioning for these applications.
- Create a migration and implementation plan that minimizes disruption to end users.

Proposed Solution

PS.1 Azure AD SSO Configuration

- Integrate Salesforce, Slack, Zoom, Dropbox, and the custom analytics platform with Azure AD using SAML 2.0 and/or OAuth.
- Configure Azure AD as the single Identity Provider (IdP) for all listed applications.
- Ensure secure SSO login experiences via modern authentication protocols and MFA.

SSO Deliverables

Deliverable	Description
Configured Azure AD Enterprise Applications	All required SaaS platforms (Salesforce, Slack, Zoom, Dropbox, custom analytics) integrated with Azure AD using SAML 2.0 and/or OAuth.
End-to-End SSO Testing Report	Verified SSO logins with MFA enforcement and documented pass/fail outcomes.
Conditional Access & MFA Policies	Final, documented policies ensuring secure access and risk-based controls.
SSO Architecture Diagram	Visual diagram showing Azure AD as the central IdP, application connections, and authentication flows.
Deployment Checklist & Runbook	Step-by-step guide for future maintenance, rollback, and additional integrations.

PS.2 User Provisioning & Lifecycle Management

- Implement Azure AD automatic user provisioning (SCIM) for supported applications.
- Enable automated de-provisioning to revoke access upon employee off-boarding.
- Define group-based access policies to streamline application assignment.

Provisioning & Lifecycle Management Deliverables

Deliverable	Description
SCIM Auto-Provisioning Setup	Automatic user provisioning enabled and tested for all supported SaaS applications.
Automated De-Provisioning Workflows	Verified processes to instantly revoke access upon employee offboarding.
Group-Based Access Policies	Role- and group-based application assignment configured and documented.

Provisioning & Lifecycle Management Runbook	Detailed guide covering SCIM mappings, troubleshooting, and policy updates.
Access Review Schedule	Documented schedule and process for periodic access reviews and compliance checks.

PS.3 Security & Access Control

- Enforce conditional access policies requiring MFA for sensitive or high-risk applications.
- Apply least-privilege principles and role-based access controls (RBAC).
- Establish an access review schedule to maintain accurate permissions.
- At least one emergency “break-glass” admin account is maintained, stored securely, and exempt from Conditional Access
- Add Integrate sign-in and audit logs with Microsoft Sentinel for long-term compliance reporting.”

PS.4 User Experience & Change Management

- Provide single-portal access via the My Apps portal or Microsoft 365 portal.
- Offer user training sessions and quick-reference guides.
- Implement a phased rollout to minimize disruptions and support user adoption.
- Enable Azure AD SSPR to improve user convenience.

Implementation Plan

Man-Hours

Phase	Implementation	Details	Time-Frame

Phase1	Assessment & Planning	Inventory all SaaS applications (Salesforce, Slack, Zoom, Dropbox, custom analytics platform). Confirm each app's SAML/OAuth and SCIM provisioning capabilities. Review current identity policies and group structures in Microsoft 365. Produce a detailed SSO architecture and migration plan, including rollback and cutover strategy.	1 Week
Phase2	Azure AD Configuration & Testing	Deploy and configure Azure AD Enterprise Applications for each SaaS platform. Create Conditional Access and MFA policies tailored to sensitive apps. Configure and test automated provisioning (SCIM) and group-based access assignments. Validate single sign-on end-to-end for each app in a lab environment.	1 Week
Phase3	Pilot Rollout	Migrate a small pilot group to Azure AD SSO. Collect user feedback and monitor sign-in logs for issues. Refine provisioning rules, MFA prompts, and access reviews based on pilot results. Finalize user communications, training materials, and support procedures.	3.5 days
Phase4	Organization-wide Deployment & Legacy Decommission	Roll out SSO and automated provisioning to all employees. Conduct live user training sessions and distribute quick-reference guides. Decommission redundant or legacy credentials and disable direct logins to integrated apps. Deliver final documentation and formally hand off to internal IT for ongoing maintenance.	3.5 days
Phase5	Post-Deployment Troubleshooting & Tuning	Provide focused support for individual signon issues and edge cases. Adjust Conditional Access rules, group memberships, or SCIM mappings as needed. Validate long-term monitoring and reporting within Azure AD and Microsoft Sentinel.	1 Week

Supporting documents and checklist

Document	Description	Link

SSO Deployment Checklist & Runbook	Step-by-step guide covering Azure AD setup, SAML/ OAuth configuration for each SaaS app, and verification steps for cutover.	Xxxx
Identity Architecture & Access Diagram	Visual diagram showing Azure AD, application connections, Conditional Access flows, and MFA enforcement.	Xxxx
Provisioning & offboard Guide	Explains SCIM auto-provisioning, group-based assignments, and offboarding steps for IT staff.	Xxxx
User Training & QuickReference Guides	Employee-facing instructions for signing in via Azure AD SSO, setting up MFA/security keys, and accessing the My Apps portal.	Xxxx
Security & Compliance Documentation	Details on Conditional Access, RBAC, auditing schedules, and integration with Microsoft Sentinel for ongoing monitoring.	Xxxx
Post-Deployment Support & Troubleshooting Log	Checklist and issue tracker for Phase 5, recording resolutions to any individual sign-on issues.	Xxxx

Total estimated project duration: ~3 weeks.

Deliverables and Benefits

Deliverables

Deliverable	Summary
SSO Integrations	Fully operational SSO integrations for Salesforce, Slack, Zoom, Dropbox, and the custom analytics platform.
Centralized Provisioning	Centralized provisioning and de-provisioning system.
IAM Policies & Procedures	Documented policies and procedures for identity and access management.
User Training & Adoption	User training materials and adoption support.

Benefits

Benefit	Solution	Problem
Simplified user access	Implement Azure AD SSO so users sign in once to access Salesforce, Slack, Zoom, Dropbox, and the custom analytics platform.	Employees manage multiple usernames and passwords.

Improved security	Apply Conditional Access and MFA policies via Azure AD to all integrated applications.	Disparate logins make enforcing MFA and security policies inconsistent, increasing the risk of unauthorized access and credential compromise.
Faster onboarding and offboarding	Use Azure AD SCIM autoprovisioning and automated de-provisioning tied to HR/ user lifecycle events.	Manual account creation and delayed deactivation lead to onboarding delays and lingering access for departed employees.
Reduced IT overhead	Provide centralized monitoring and auditing through Azure AD and Microsoft Sentinel.	IT spends excessive time on password resets, access audits, and tracking application usage across multiple disconnected systems.

Assumptions & Exclusions

- Requires continued Microsoft 365 E3 licensing with Azure AD Premium P1 or P2 if advanced features are needed.
- Integration of applications outside the listed scope will require additional scoping and resources.

Licensing & Subscriptions

License / Subscription	Notes	Fees & Release Notes
Microsoft 365 E3 (Required / Already in place)	Core productivity suite providing Exchange Online, Microsoft 365 services, and Azure AD Premium P1 for SSO, Conditional Access, MFA, and user provisioning.	Foundation license required for all users.
Microsoft Entra ID (Azure AD) Premium P2 (Optional / Recommended)	Adds advanced Privileged Identity Management (PIM), risk-based Conditional Access, and automated access reviews.	Without P2: Standard SSO and Conditional Access remain, but no just-in-time admin rights or automated access review workflows.

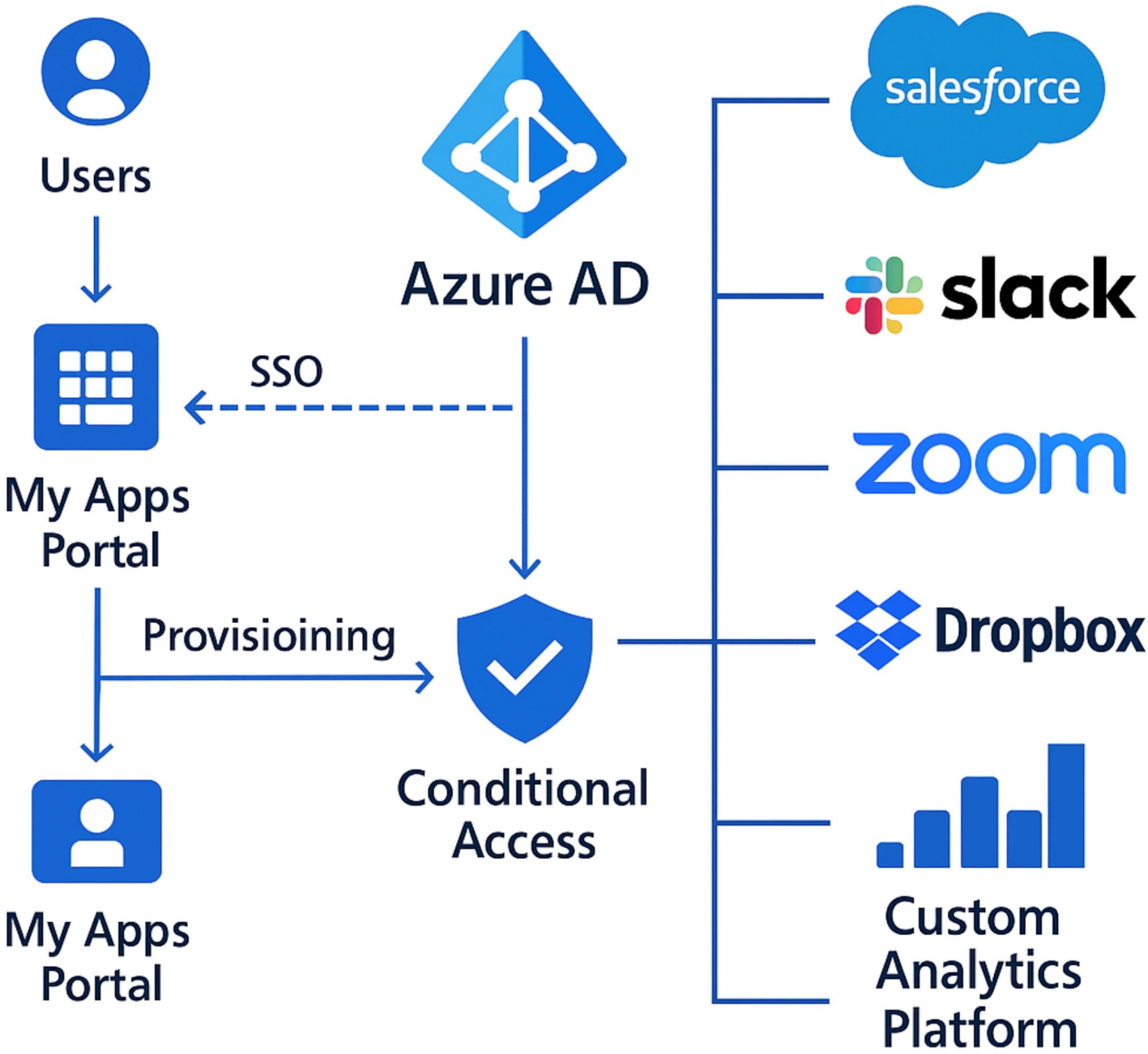
Microsoft 365 or Azure AD User CALs for Integrated Apps (Included)	Covers SSO and autoprovisioning for integrated SaaS apps (Salesforce, Slack, Zoom, Dropbox).	No extra Microsoft license is required beyond each app's own subscription.
Application Vendor Licenses (Salesforce, Slack, Zoom, Dropbox) (Already in place / Required)	SaaS subscriptions supporting SAML 2.0 or SCIM for SSO and user provisioning.	Ensure each vendor plan includes SSO capability.
Microsoft Intune (Included with Microsoft 365 E3)	Provides optional device compliance enforcement for Conditional Access, such as BitLocker and OS health checks.	No separate license required.
Microsoft Sentinel (Optional / Usage-based)	Cloud-native SIEM/SOAR for centralized log collection, correlation, and automated incident response.	Without Sentinel: Security events remain in native Azure AD logs without unified, automated response.

Decommission and Degassing

Phase	Action	Notes
Assessment & Inventory	Identify all legacy logins, direct SaaS credentials, and any outdated identity connectors (per-app admin accounts, old SAML configs) slated for removal.	Confirm that all user accounts are synchronized with Azure AD and no production roles depend on legacy credentials.
Data & Access Verification	Verify that all Salesforce, Slack, Zoom, Dropbox, and custom analytics accounts are functioning exclusively via Azure AD SSO.	Ensure that provisioning (SCIM) and de-provisioning are fully tested and documented before cutover.
Legacy Credential Disablement	Disable and/or delete redundant user/password stores within each SaaS app.	Include disabling direct logins, old admin accounts, and any stored API keys no longer required.
Conditional Access & MFA Enforcement Check	Validate that MFA and Conditional Access policies are active and enforced for every integrated application.	Double-check that fallback logins are closed and emergency break-glass accounts are documented.

Audit & Documentation	Capture pre- and postdecommission access logs, and archive SSO architecture and runbook.	Provide evidence for compliance and future audits (e.g., Microsoft Sentinel or native Azure AD reports).
Drive / Key Material Sanitization	Securely remove or reset any shared secrets, certificates, and encryption keys used in previous SAML/OAuth configurations.	Store certificates of destruction or revocation where required by compliance.
Final Decommission & Disposal	Decommission obsolete identity connectors, scripts, or servers (if any) that previously handled authentication.	Remove any on-premises servers or virtual appliances solely used for old authentication methods.
User & Admin Confirmation	Conduct final confirmation with application owners and IT admins to ensure all staff are logging in only through Azure AD SSO.	Document sign-offs for each application owner.
Post-Deployment Monitoring	Monitor Azure AD sign-in logs and Microsoft Sentinel (if used) for anomalies during the first 30 days.	Rapidly address any lingering direct login attempts or provisioning errors.

Solutions Diagram



Out Of Pocket / Invoice

Client will be invoiced all costs associated with out-of-pocket expenses (including, without limitation, costs and expenses associated with patching, cables termination, local transportation and any other applicable business expenses) listed on the invoice as a separate line item.

Reimbursement for out-of-pocket expenses in connection with performance of this SOW, when authorized and up to the limits set forth in this SOW, shall be in accordance with client's thencurrent published policies governing travel and associated business expenses.

Completion criteria

Contractor shall have fulfilled its obligations when any one of the following first occurs: Contractor accomplishes the contractor activities described within this SOW, including delivery to client of the materials listed in the section entitled "deliverable materials," and client accepts such activities and materials without unreasonable objections. No response from client within 2business days of deliverables being delivered by contractor is deemed acceptance. Contractor and/or client has the right to cancel services or deliverables not yet provided with 20 business days advance written notice to the other party.

Project change control procedure

A project change request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect of the change. The designated project manager of the requesting party (contractor or client) will review the proposed change and determine whether to submit the request to the other party. Both project managers will review the proposed change and approve it for further investigation or reject it. contractor and client will mutually agree upon any charges for such investigation, if any. If the investigation is authorized, the client project managers will sign the PCR, which will constitute approval for the investigation charges. Contractor will invoice client for any such charges. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the agreement. Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a change authorization will be executed. A written change authorization and/or PCR must be signed by both parties to authorize implementation of the investigated changes.

Sign Off

Summit Marketing	DKB
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____