Enterprise Cloud IAM w/ Microsoft Entra ID Lab

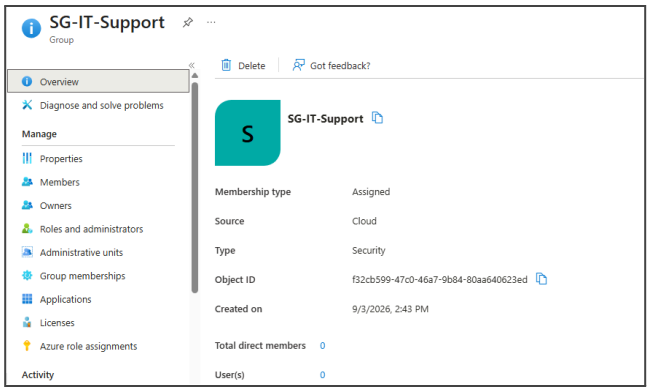
Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Microsoft Entra Admin Center (Entra ID P2) |
PORTFOLIO WEBSITE: https://www.saintmaiden.site/

EXECUTIVE SUMMARY:

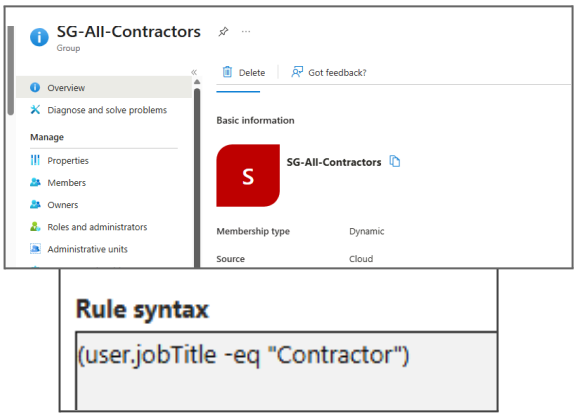
PROBLEM:	SOLUTION:	IMPACT:
Manual onboarding requests and password reset requests create Help Desk bottlenecks, while unmonitored privileges lead to the creation of "Privilege Creeps".	**Configured Microsoft Entra ID P2 for identity lifecycle management automation, enforce RBAC (Role-Based Access Controls) with PoLP (Principle Of Least Privilege), implement zero trust access controls with the deployment of SSPR (Self-Service Password Reset).**	**Eliminated manual group provisioning, reduced password reset ticket overhead exponentially using SSPR, and secured identity endpoints with mandatory MFA.**

PHASE 1: DYNAMIC GROUP ARCHITECTURE AND RBAC (ROLE-BASED ACCESS CONTROLS)

Established Role-Based Access Controls to automate group membership. This prevents "Privilege Creep" and human error by automatically granting or revoking access instantly based on the employee's role in the company.



- **Static Group (SG-IT-Support): Configured membership for all IT roles.**

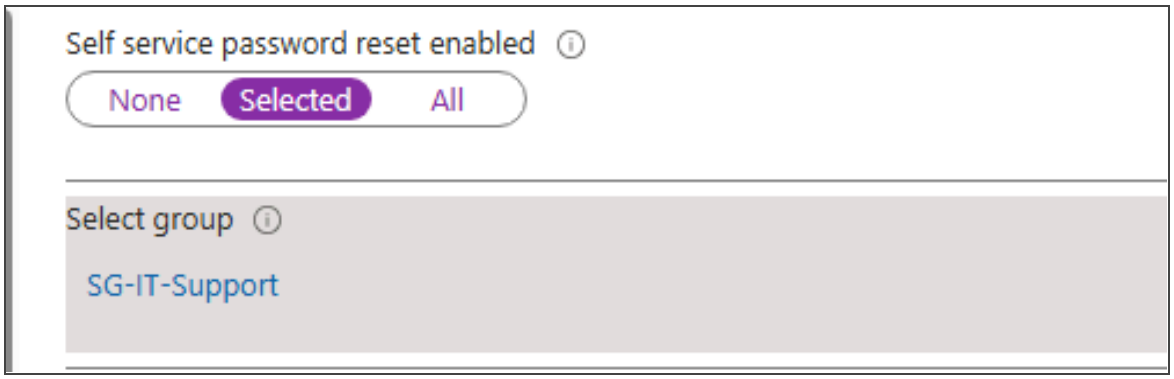


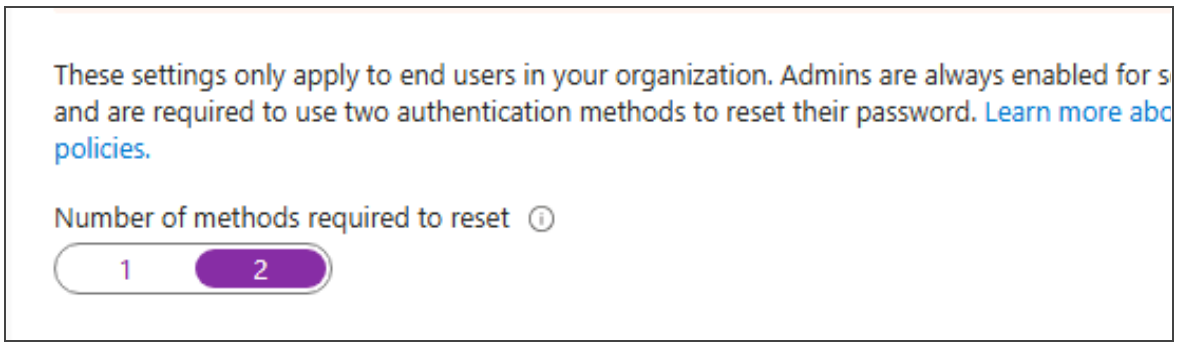
- **Dynamic Group (SG-All-Contractors): Implemented dynamic syntax (user.JobTitle -eq "Contractor") to instantly grant/revoke permissions based on attributes, eliminating "Privilege creep during onboarding and offboarding.**

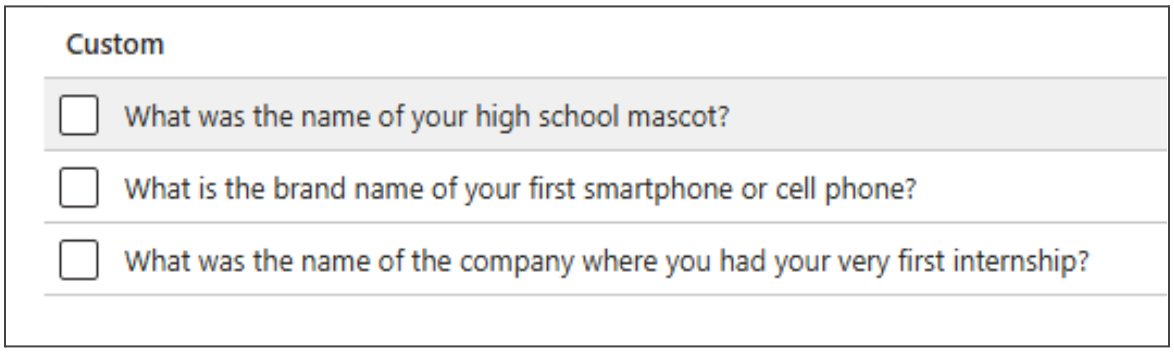
PHASE 2: SELF SERVICE PASSWORD RESET

ACTION: **Activated SSPR targeting SG-IT-Support, enforcing a requirement of two authentication methods and custom security questions.**

WHY?: **<u>This enables users to securely reset their own password without intervention, cutting down high-volume Helpdesk tickets, reducing support overhead, and maintaining productivity across the board.</u>**





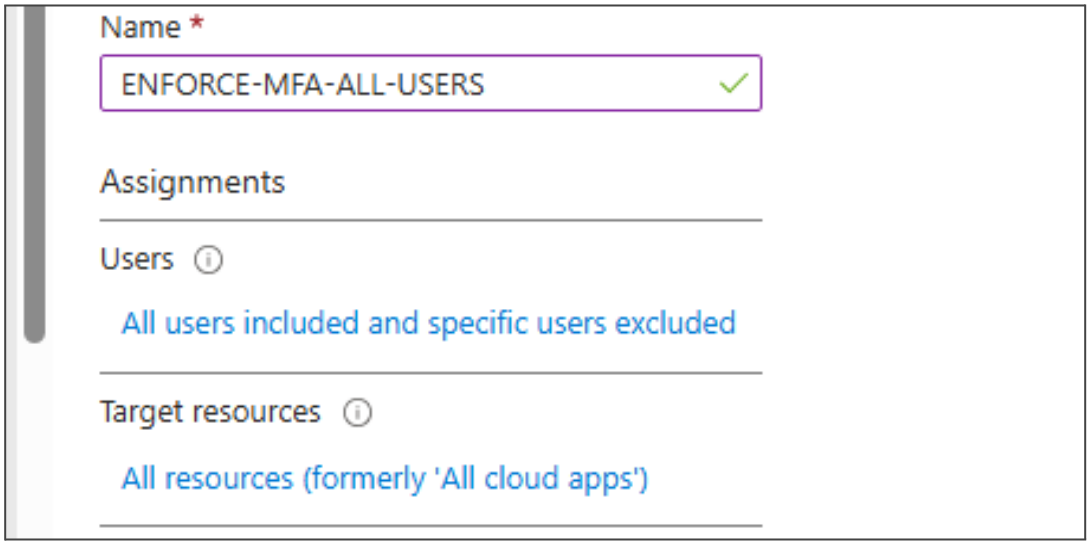


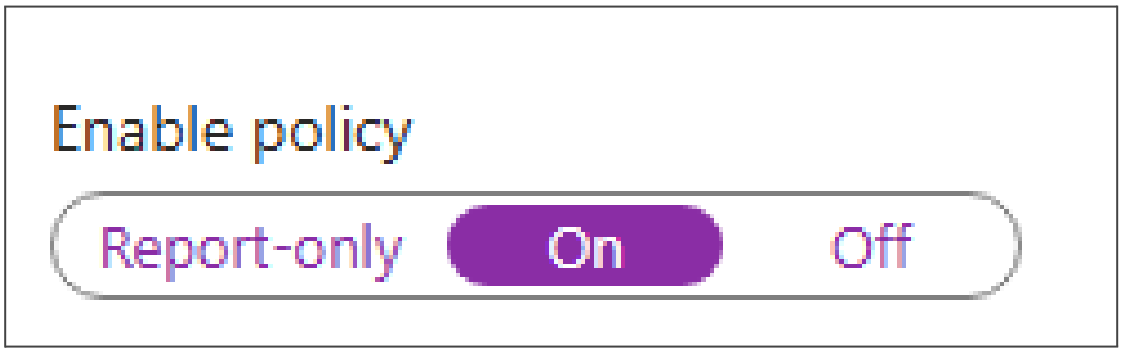


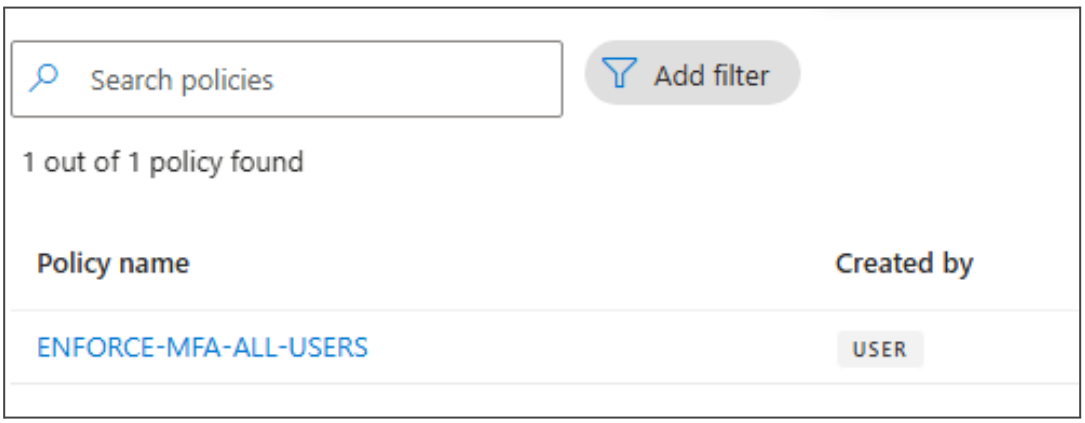
PHASE 3: ZERO TRUST CONDITIONAL ACCESS & MFA (MULTI-FACTOR AUTHENTICATION)

ACTION: **Created a conditional access policy ENFORCE-MFA-ALL-USERS applying to all cloud applications (excluding emergency break-glass accounts) and granting access conditionally on MFA completion.**

WHY?: **Enforces the Zero-Trust principle ("Never Trust, Always Verify") to block unauthorized access, close Single Sign-On exploits, and stop compromise if passwords are stolen.**



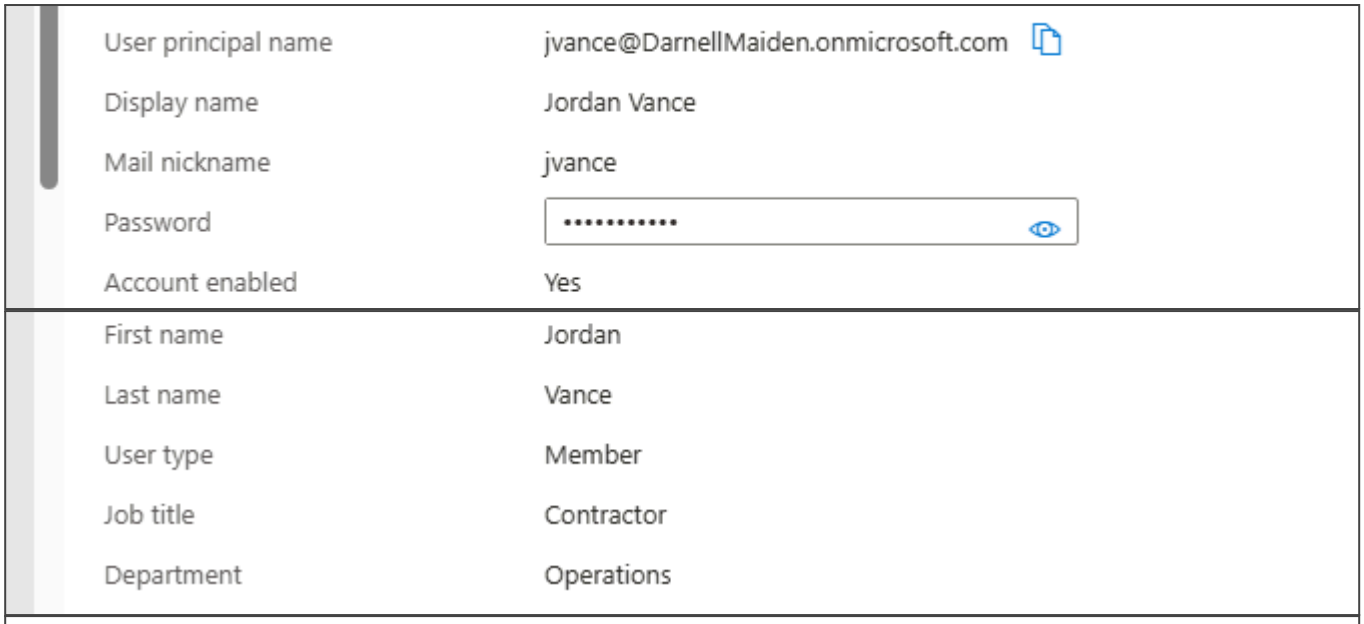


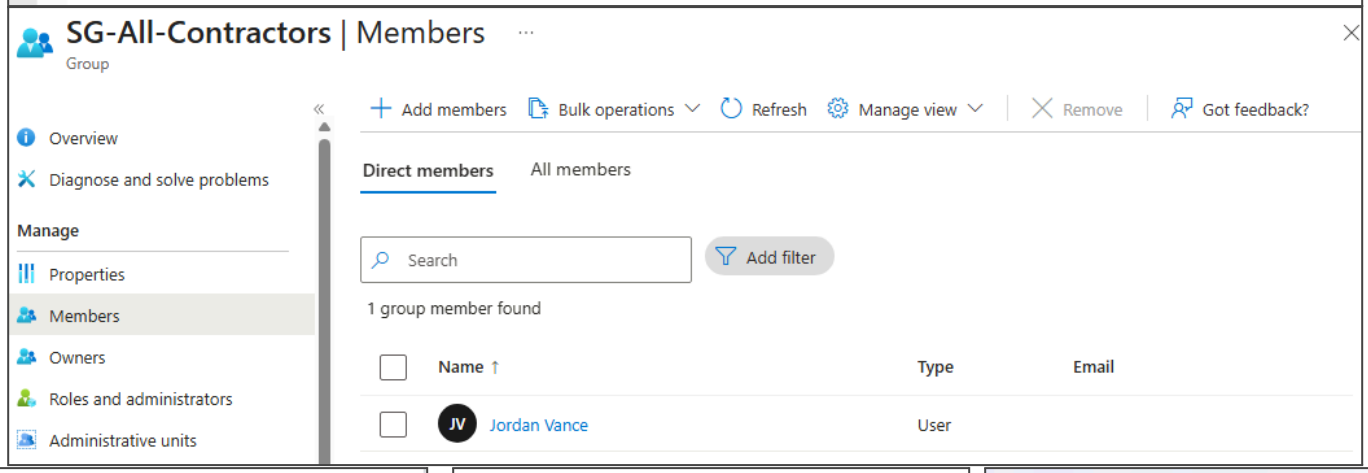


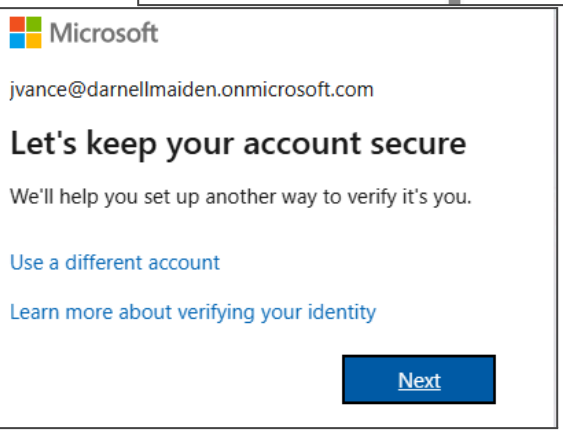
PHASE 4: IDENTITY PROVISION & WORKFLOW AUTOMATION

ACTION: Created test identity "Jordan Vance" (Job Title: Contractor) with a temporary password to test dynamic evaluation and policy enforcement.

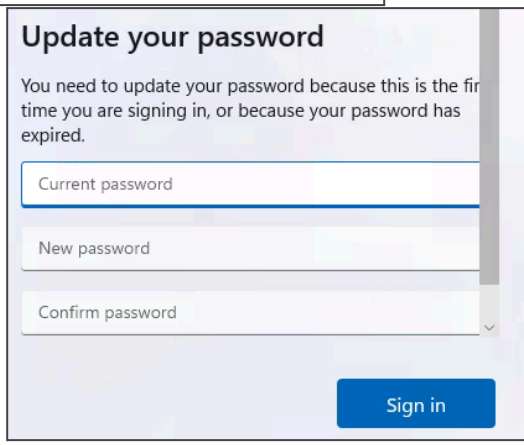
WHY?: Validates that back-end directory rules auto-assign groups accurately and ensures Conditional Access policies actively force MFA and initial password changes before entering production.











TECHNICAL SUMMARY:

SECURITY DOMAIN	TECH. & CONTROLS CONFIGURED
Identity Governance	RBAC, Dynamic Group Membership (user.JobTitle -eq “Contractor”), Lifecycle Management
Self-Service & Productivity	SSPR Deployment, Custom Security Question Enrollment, 2-Factor Auth Recovery
Access Control & Zero Trust	Conditional Access (ENFORCE-MFA-ALL-USERS), Mandatory MFA Enforcement
Directory Options	User Provisioning, Temporary Password Management, Authenticator Onboarding

RESULT & BUSINESS IMPACT:

AUTOMATED IDENTITY GOVERNANCE: Dynamic group rules automated role-based access for contractors, eliminating manual group assignment tasks and stopping “Privilege Creep” before it starts.

STREAMLINED SUPPORT OPERATIONS: Deploying SSPR with mandatory MFA self-service drastically lowers the volume of password reset tickets, freeing up Tier 1 Support capacity

ENFORCED ZERO-TRUST SECURITY: Mandatory MFA enforced via Conditional Access (ENFORCE-MFA-ALL-USERS) secures cloud endpoints against single-factor credential attacks and compromised passwords.

VERIFIED PRODUCTION READINESS: End-To-End identity testing with Jordan Vance validated seamless dynamic evaluation, required initial password changes, and Microsoft Authenticator enrollment prior to full deployment

Author: Darnell Maiden | **Certifications:** CompTIA Security+, Google IT Support Professional Certificate, Google Cybersecurity Professional Certificate | **Target Environment:** Microsoft Entra Admin Center (Entra ID P2) |
PORTFOLIO WEBSITE: https://www.saintmaiden.site/