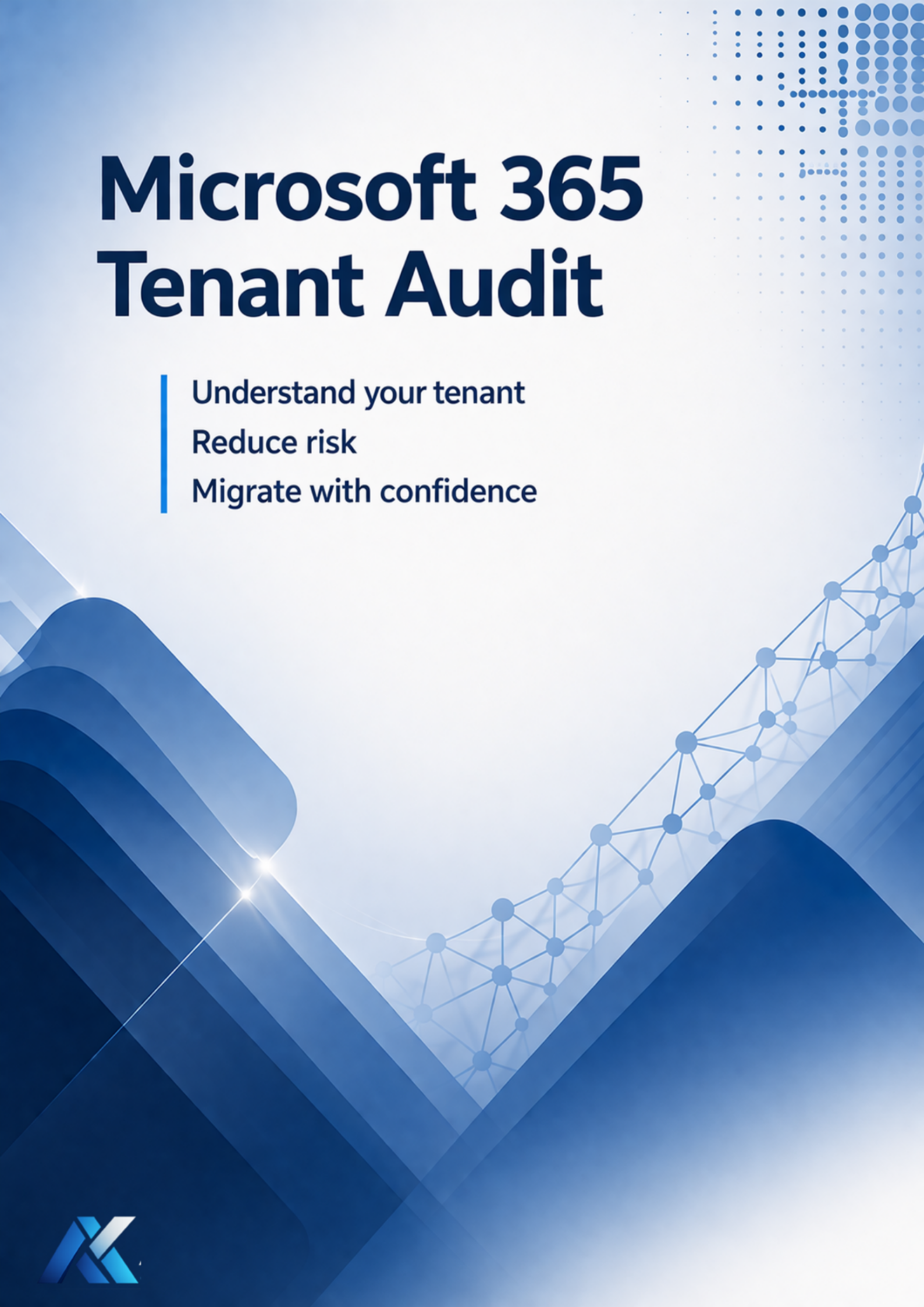
Microsoft 365 Tenant Audit

Understand your tenant

Reduce risk

Migrate with confidence



Most Microsoft 365 tenants don't lack tools...

They lack visibility

Privileged access is unclear

Permissions grow over time

"Temporary" access becomes permanent

This is where risk starts to build and where this audit uncovers the **real picture.**

SAMPLE ENTERPRISE REPORT

Deep insight across your Microsoft 365 tenant

Identity & Access

Users, roles, groups and privileged access analysed

Security & Risk

Configuration, controls and exposure assessed

Configuration & Governance

Settings, policies and architectural alignment reviewed

Clarity & Action

Structured findings with prioritised recommendations you can use

Microsoft 365

Tenant Audit Report

Tenant:

Andy Kemp Dev

Enterprise Report

ANDY KEMP
CONSULTING

10 April 2026

audit.andykemp.com | www.andykemp.com

Audit Scorecard

74	16	78
Security Risk	**Migration Complexity**	**Compliance Posture**
Low Risk	Simple	Low Risk

Microsoft Secure Score: 65% (356.92/547)

High-Priority Findings

CRITICAL	Only 38% of users have MFA registered — critical gap.
HIGH	1 break-glass account(s) do not have FIDO2 / phishing-resistant authentication registered (Andrew Kemp). Break-glass accounts should use phishing-resistant credentials only.
HIGH	3 stale accounts (21% of users) — inactive 90+ days. Disable or remove.
HIGH	No PIM eligible assignments found — all role assignments are permanent.
HIGH	No sensitivity labels — data classification not implemented.
HIGH	No Purview retention labels configured — data lifecycle management not implemented.
HIGH	8 users without MFA — accounts vulnerable to credential attacks.
HIGH	Hybrid AD sync enabled — identity cutover/co-existence planning required.

Report Level: Enterprise

Enterprise migration & compliance — complete intelligence suite with external exposure, migration readiness, roadmap, and recommended actions.

Executive Summary

This report provides an independent assessment of the Microsoft 365 tenant's security posture, operational readiness, and migration complexity. It is designed to support executive decision-making by surfacing control gaps, identifying blockers, and providing actionable, prioritised recommendations.

This assessment of Andy Kemp Dev was completed on 10/04/2026. The audit examined 10 user accounts, 1 shared mailboxes, 4 M365 groups, 2 Teams, 12 SharePoint sites, 13 Conditional Access policies, and 44 app registrations across 3 registered domain(s).

Assessment Summary

Security Risk Score: 74/100 (Low Risk). Migration Complexity: 16/100 (Simple). Compliance Posture: 78/100 (Low Risk). Microsoft Secure Score: 65%.

Key Findings

- 1 critical finding requiring immediate attention
- 6 high-severity findings
- MFA adoption at 38% — 62% of users unprotected
- 3 stale accounts (90+ days inactive)
- 1 external guest account
- Estimated migration effort: 14 working day(s)

Metric	Value
Users	10
Guest Users	1
Shared Mailboxes	1
M365 Groups	4
Distribution Lists	1
Security Groups	12
Teams	2
SharePoint Sites	12
Domains	3
Conditional Access Policies	13
App Registrations	44
Intune Policies	6
Mailbox Storage	147.0 MB
User Mailboxes	10 (140.7 MB)
Shared Mailboxes	1 (6.3 MB)
Room/Equipment	2 (0 B)
Mailbox Items	23,508
OneDrive Storage	457.9 MB
OneDrive Files	0
Secure Score	65% (356.92/547)
MFA Registration	38% of 13 users
Stale Accounts (90+ days)	3

Table of Contents

Security Risk Assessment

The Security Risk Assessment evaluates the tenant's identity and access controls, data protection measures, device compliance posture, and application security configuration. A higher score indicates a more secure environment. Scores below 50 indicate significant risk areas that should be addressed as a priority.

74 **Security Risk Score** — Low Risk

Category	Score	Weight
Identity & Access	48/100	40%
Data Protection	90/100	25%
Device Compliance	100/100	15%
App Security	84/100	20%

Global Administrator Analysis: 2 permanent assignment(s) detected. Based on the indicated break-glass configuration (2 accounts), the permanent GA count is within the expected range for emergency access.

Key Actions Required

CRITICAL Only 38% of users have MFA registered — critical gap.

HIGH 1 break-glass account(s) do not have FIDO2 / phishing-resistant authentication registered (Andrew Kemp). Break-glass accounts should use phishing-resistant credentials only.

HIGH 3 stale accounts (21% of users) — inactive 90+ days. Disable or remove.

Severity	Category	Finding
CRITICAL	Identity & Access	Only 38% of users have MFA registered — critical gap.
HIGH	Identity & Access	1 break-glass account(s) do not have FIDO2 / phishing-resistant authentication registered (Andrew Kemp). Break-glass accounts should use phishing-resistant credentials only.
HIGH	Identity & Access	3 stale accounts (21% of users) — inactive 90+ days. Disable or remove.
MEDIUM	App Security	15 admin-consented OAuth grants — review for over-permissioned apps.
MEDIUM	App Security	2 app registrations have expired credentials.
MEDIUM	Data Protection	No sensitivity labels configured — consider implementing data classification.
LOW	Identity & Access	2 Conditional Access policies are disabled — review if still needed or should be enabled.
LOW	App Security	1 app registrations have credentials expiring within 30 days.
INFO	Identity & Access	2 permanent Global Admin assignments — within break-glass account allowance.

Migration Complexity Assessment

The Migration Complexity Assessment evaluates the effort required to migrate this tenant's workloads to a new environment. It considers mail volume, Teams and collaboration complexity, SharePoint and OneDrive data, identity configuration, and application integrations. A lower score indicates a simpler migration. Organisations with scores above 60 should expect a phased migration with dedicated project management.

16 **Migration Complexity** — Simple

Estimated Migration Effort: 14 working day(s). This estimate is based on the volume and complexity of data discovered during the audit.

Category	Score	Weight
Mail & Messaging	9/100	30%
Teams & Collaboration	8/100	20%
SharePoint & OneDrive	8/100	20%
Identity & Security	48/100	20%
Applications & Integrations	0/100	10%

Key Actions Required

HIGH Hybrid AD sync enabled — identity cutover/co-existence planning required.

Severity	Category	Finding
HIGH	Identity & Security	Hybrid AD sync enabled — identity cutover/co-existence planning required.
MEDIUM	Mail & Messaging	1 shared mailboxes — require delegate permission mapping.
MEDIUM	Identity & Security	5 hybrid-synced objects.
MEDIUM	Identity & Security	13 CA policies — require recreation/reconfiguration in destination.
LOW	Mail & Messaging	2 room/equipment mailboxes — need booking policy configuration.
LOW	Teams & Collaboration	2 Teams.
LOW	SharePoint & OneDrive	12 SharePoint sites.
INFO	Mail & Messaging	10 user mailboxes — small migration.

Compliance & Governance Assessment

The Compliance & Governance Assessment reviews access governance controls, data governance policies, threat protection configuration, and audit and monitoring readiness. This score reflects the organisation's preparedness for regulatory requirements and best-practice governance. Tenants scoring below 50 have significant compliance gaps that could expose the organisation to regulatory risk.

78 **Compliance Score** — Low Risk

Category	Score	Weight
Access Governance	80/100	30%
Data Governance	65/100	25%
Threat Protection	79/100	25%
Audit & Monitoring	95/100	20%

Key Actions Required

HIGH No PIM eligible assignments found — all role assignments are permanent.

HIGH No sensitivity labels — data classification not implemented.

HIGH No Purview retention labels configured — data lifecycle management not implemented.

HIGH 8 users without MFA — accounts vulnerable to credential attacks.

Severity	Category	Finding
HIGH	Access Governance	No PIM eligible assignments found — all role assignments are permanent.
HIGH	Data Governance	No sensitivity labels — data classification not implemented.
HIGH	Data Governance	No Purview retention labels configured — data lifecycle management not implemented.

Severity	Category	Finding
HIGH	Threat Protection	8 users without MFA — accounts vulnerable to credential attacks.
MEDIUM	Threat Protection	2 apps with expired credentials — may indicate abandoned integrations.
LOW	Audit & Monitoring	No security alerts found — verify alert policies are configured and being monitored.

Security + Migration Intelligence Overview

2 critical control gaps were identified during this assessment. Critical control gaps identified — 2 critical and 6 high-severity findings require prioritised remediation. These findings should be treated as immediate priorities, irrespective of the overall score.

Score	Value
Security Risk Score	74
Compliance Posture Score	78
Migration Complexity Score	16
Migration Readiness Score	82
Identity Attack Surface Score	85
Privileged Access Exposure Score	64
Conditional Access Coverage Score	54
Device Trust Score	86
External Exposure Score	95
App Risk Score	67

Identity Attack Surface

Moderate risk profile — 3 findings identified with targeted hardening opportunities.

85

Section Score — Strong

Metric	Value
Enabled users	10
Users without MFA	6
Privileged users without MFA	0
Enabled stale accounts	3
No sign-in history	4

Severity	Title	Description	Recommendation
MEDIUM	Low MFA adoption	6 of 10 enabled user accounts (60%) have no MFA registration, leaving the majority of identities exposed to credential-based attacks such as phishing, password spray, and token theft.	Enforce MFA registration via Conditional Access registration campaign. Exclude only verified emergency access accounts.
MEDIUM	Stale accounts remain enabled	3 enabled accounts have not signed in for 90+ days. Dormant accounts with active credentials represent an unmonitored attack surface for lateral movement and persistent access.	Disable stale accounts immediately, enforce joiner/mover/leaver lifecycle controls, and schedule recurring access reviews.
MEDIUM	Accounts with no sign-in history	4 enabled accounts have no recorded sign-in. These may be provisioned but unused accounts — or service accounts that bypass interactive sign-in. Either way, they represent credentials that could be compromised without detection.	Investigate each account: disable if orphaned, apply lifecycle governance, or confirm non-interactive use and restrict sign-in scope.
LOW	Emergency access	No accounts matching a recognised break-glass naming convention were detected among Global Administrator assignments. Emergency	Ensure dedicated break-glass accounts are clearly named, documented, excluded from Conditional Access,

Severity	Title	Description	Recommendation
LOW	accounts not explicitly identified	access accounts may exist but could not be validated from the available configuration data.	monitored for sign-in activity, and not dependent on any federated identity provider.

High-Risk Accounts

UPN	Risk Type
andrew.kemp_delaware.co.uk#EXT#@andykempdev.onmicrosoft.com	Enabled stale account
Pete.Mitchel@andykemp.dev	Enabled stale account
Tony.Stark@andykemp.dev	Enabled stale account
Clint.Barton@andykemp.dev	No sign-in history
Equio1@andykemp.dev	No sign-in history
Nick.Fury@andykemp.dev	No sign-in history
Room1@andykemp.dev	No sign-in history

Conditional Access Coverage Analysis

Critical control gaps identified — 1 critical and 2 high-severity findings require prioritised remediation.

54 **Section Score** — Needs Attention

Metric	Value
Enabled policies	11
Report-only policies	0
Disabled policies	2
Users protected (%)	54
Admins protected (%)	0
All cloud apps policy detected	No

Severity	Title	Description	Recommendation
CRITICAL	No dedicated admin Conditional Access policy	No Conditional Access policy explicitly targeting administrative directory roles was detected. Privileged accounts should be subject to stricter controls than standard users, including phishing-resistant MFA, compliant device requirements, and location restrictions.	Create a dedicated privileged-role policy requiring phishing-resistant MFA (FIDO2 or certificate-based), compliant device, and named-location restrictions.
HIGH	No broad user coverage policy detected	No enabled policy explicitly targets all users. Without an all-user baseline, a significant proportion of identities may bypass MFA and other security controls depending on individual policy scope.	Create an "All Users" baseline policy requiring MFA, then manage exceptions through a minimal, documented exclusion group.
HIGH	Legacy authentication not blocked	No policy appears to block legacy authentication clients (POP, IMAP, SMTP, Exchange ActiveSync, etc.). Legacy protocols cannot enforce MFA, making them a primary vector for password-spray and brute-force attacks.	Create a CA policy blocking all legacy authentication clients. Verify no line-of-business applications depend on these protocols before enforcement.
MEDIUM	No device compliance requirement detected	Enabled policies do not appear to require a compliant or hybrid Azure AD joined device. Without device trust, users can access tenant resources from unmanaged or compromised endpoints.	Introduce device-based grant controls for high-value applications and privileged users. Start with report-only mode to assess impact before enforcement.
LOW	Disabled Conditional Access policies present	2 CA policies are disabled. Disabled policies may indicate incomplete deployments, configuration drift, or intentional but undocumented exclusions.	Review disabled policies: re-enable or retire as appropriate, and document the reason for any intentional disablement.

Top Conditional Access Gaps

Gap	Status
All users coverage	Gap
Admin role coverage	Gap
Guest user coverage	Detected
Legacy auth block	Gap
Compliant/Hybrid device requirement	Gap

Privileged Access Exposure

Critical control gaps identified — 1 critical finding requiring immediate remediation.

64 **Section Score** — Control Gaps Identified

Metric	Value
Privileged assignments	4
Permanent privileged assignments	4
Global Administrators	2
Identities with 3+ privileged roles	0

Severity	Title	Description	Recommendation
CRITICAL	No Privileged Identity Management (PIM) detected	No PIM-eligible role assignments were detected — all privileged access is permanently active. Without just-in-time activation, every privileged identity is a standing, always-on target. This is the single highest-impact control gap for limiting credential compromise blast-radius.	Enable Entra ID PIM for all privileged roles. Convert permanent assignments to time-limited eligible access with multi-person approval workflows and phishing-resistant MFA gating.

Top Privileged Identities

Identity	Privileged Roles
Andrew Kemp	2
TenantLift MRS Migration	1
TenantLift	1

Service Principals with Elevated Access

Principal	Role	Assignment Type
TenantLift MRS Migration	Exchange Administrator	Active
TenantLift	Exchange Administrator	Active

Device Trust & Access

Elevated risk — 1 high-severity finding requiring prioritised remediation.

86 **Section Score** — Strong

Metric	Value
Intune policies	6
Enabled CA policies	11
Device-based CA policies	0
Admin device-trust policies	0

Severity	Title	Description	Recommendation
HIGH	No device-based Conditional Access enforcement detected	No enabled CA policy requires a compliant or hybrid Azure AD joined device for access. Users may access corporate resources from unmanaged, shared, or compromised devices without restriction.	Require compliant or hybrid-joined devices for sensitive applications and administrative workloads. Deploy in report-only mode first to assess user impact.
MEDIUM	Administrators not constrained to trusted devices	No CA policy requiring device compliance or hybrid join was detected for administrative directory roles. Privileged accounts accessing the tenant from unmanaged devices increases the risk of credential theft and token replay attacks.	Create a dedicated admin device-trust policy. For highest-risk roles, consider Privileged Access Workstations (PAWs) or Cloud PCs with strict compliance baselines.
INFO	Device inventory not yet collected	Managed device counts and compliance percentages are not included in this assessment. A future audit revision will incorporate Intune device telemetry.	N/A — no action required.

Device Trust Control Coverage

Control	Status
Intune policy baseline	Detected
CA device trust enforcement	Gap
Admin trusted-device enforcement	Gap

External Access & Data Exposure

Moderate risk profile — 1 finding identified with targeted hardening opportunities.

95 **Section Score** — Strong

Metric	Value
Guest accounts	1
Dormant guests	1
Externally shared OneDrive items	0
Anonymous links	0

Severity	Title	Description	Recommendation
MEDIUM	Dormant guest accounts with active access	1 guest account appears inactive for 90+ days. Dormant external accounts retain whatever access was originally granted and can be exploited if the guest's home tenant is compromised or their credentials are leaked.	Implement recurring guest access reviews using Entra ID Access Reviews. Remove dormant B2B accounts and enforce sponsor ownership for all guest invitations.
INFO	SharePoint sharing configuration not yet assessed	Tenant-level and site-level SharePoint external sharing settings are not included in the current audit scope. A future revision will incorporate SharePoint Admin API telemetry.	N/A — no action required.

Guest Users

Guest UPN	Status
andrew.kemp_delaware.co.uk#EXT#@andykempdev.onmicrosoft.com	Dormant

Shared Content Exposure Summary

Scope	Count
Internal	8
External	0
Anonymous	0

OAuth / App Risk

Elevated risk — 2 high-severity findings requiring prioritised remediation.

67 **Section Score** — Moderate

Metric	Value
App registrations	44
OAuth grants	15
Risky grants	7
Admin-consented grants	15
Expired credentials	2
Expiring credentials (30d)	1

Severity	Title	Description	Recommendation
HIGH	High-risk OAuth permissions detected	7 OAuth grants include high-risk scopes (e.g., Directory.ReadWrite.All, Mail.ReadWrite). These permissions allow applications to read or modify sensitive directory, mailbox, or file data — a compromised or malicious application with these scopes could exfiltrate data or escalate privileges silently.	Audit each grant: remove unnecessary scopes, re-consent with least privilege, and revoke access for unrecognised or unused applications.
HIGH	Expired application credentials	2 applications have expired credentials. While expired credentials cannot be used for authentication, they indicate a breakdown in credential lifecycle management. The associated workloads may have silently failed, or alternative (potentially less secure) credentials may have been created.	Rotate expired credentials immediately. Migrate high-value workloads to certificate-based or managed identity authentication to eliminate secret management overhead.
MEDIUM	Tenant-wide admin-consented application grants	15 OAuth grants are admin-consented for all users in the tenant. Admin consent bypasses individual user approval, granting the application access to data for every user. If any of these applications are compromised, the blast radius is the entire organisation.	Validate publisher trust for each admin-consented application. Enable the admin consent workflow to prevent future uncontrolled grants, and revoke consent for any unrecognised publishers.
MEDIUM	Application credentials expiring within 30 days	1 application has credentials expiring within 30 days. Proactive rotation prevents service outages and reduces the window of exposure for long-lived secrets.	Schedule credential rotation before expiry. Add Azure Monitor or Key Vault alerts for credential expiry to prevent future surprises.
INFO	Publisher trust verification limited	First-party vs third-party application classification is currently based on heuristics. Verified publisher metadata will be incorporated in a future audit revision for more precise risk attribution.	N/A — no action required.

Top Risky Applications

Application	Consent Type	Risky Scope
SharePoint Online Web Client Extensibility	AllPrincipals	SensitivityLabel.Read TeamsTab.Create AppCatalog.Read.All AppCatalog.Submit Channel.ReadBasic.All EduAssignments.ReadBasic EduRoster.ReadBasic Files.Read.All Files.ReadWrite.All Group.Read.All People.Read People.Read.All Presence.Read.All TeamsAppInstallation.ReadWriteSelfForTeam User.Read User.ReadBasic.All Tasks.ReadWrite Group-Conversation.ReadWrite.All Team.ReadBasic.All Channel.Create Sites.Read.All

Application	Consent Type	Risky Scope
		PrinterShare.ReadBasic.All PrintJob.Create PrintJob.ReadBasic FileStorageContainer.Selected Calendars.Read Files.Read GroupMember.Read.All InformationProtectionPolicy.Read TeamsAppInstallation.ReadWriteForTeam ChatMember.Read
SharePoint Online Web Client Extensibility	AllPrincipals	Files.ReadWrite.All TermStore.ReadWrite.All Sites.ReadWrite.All Sites.FullControl.All
SharePoint Online Web Client Extensibility	AllPrincipals	Sites.FullControl.All ExternalConnection.ReadWrite.All
Microsoft Graph Command Line Tools	AllPrincipals	User.Read Device.ReadWrite.All openid profile offline_access DeviceManagementManagedDevices.PrivilegedOperations.All User.Read.All User.ReadWrite.All Domain.ReadWrite.All Directory.AccessAsUser.All Policy.ReadWrite.ConditionalAccess Policy.Read.All DeviceManagementManagedDevices.ReadWrite.All Group.ReadWrite.All Application.Read.All Policy.ReadWrite.ApplicationConfiguration ConsentRequest.ReadWrite.All Policy.ReadWrite.AuthenticationMethod UserAuthenticationMethod.ReadWrite.All UserAuthenticationMethod.Read.All UserAuthenticationMethod.ReadWrite UserAuthenticationMethod.Read DeviceManagementServiceConfig.ReadWrite.All GroupMember.ReadWrite.All Directory.ReadWrite.All Organization.ReadWrite.All DeviceManagementConfiguration.ReadWrite.All Application.ReadWrite.All RoleManagement.ReadWrite.Directory Sites.FullControl.All AppRoleAssignment.ReadWrite.All email Directory.Read.All
Graph Explorer	AllPrincipals	openid profile User.Read offline_access Directory.ReadWrite.All Policy.Read.All UserAuthenticationMethod.Read.All UserAuthenticationMethod.ReadWrite UserAuthenticationMethod.Read UserAuthenticationMethod.ReadWrite.All
Azure Logic Apps - Azure AD	AllPrincipals	Group.ReadWrite.All User.ReadWrite.All offline_access
AKD-MFA-Upload-Portal	AllPrincipals	User.Read openid profile offline_access

Expired / Expiring Credentials

Application	Credential Expiry	Status
akdev-arc	2024-12-13T15:55:48.694Z	Expired
P2P Server	2025-06-27T00:00:00Z	Expired
AndyKempDev-SCEP	2026-05-02T15:40:01.6882459Z	Expiring <30d

Licensing Optimisation

Elevated risk — 1 high-severity finding requiring prioritised remediation.

90 **Section Score** — Strong

Metric	Value
Total SKUs	3
SKUs with free capacity	3
Potentially over-licensed SKUs	3
Licensed users without MFA	3

Severity	Title	Description	Recommendation
HIGH	Licensed users missing core security controls	3 licensed users are not registered for MFA. Premium licences include security features (e.g., Conditional Access, Identity Protection) that require MFA as a foundation. Without MFA, the investment in premium licensing delivers reduced security return.	Prioritise MFA enforcement for premium-licensed users via Conditional Access registration campaign to realise the full security ROI of the licence investment.
MEDIUM	Potential over-licensing detected	3 SKUs have 25% or more unassigned licences. Unassigned seats represent recurring cost without business value and may indicate incomplete user provisioning or licence assignment drift.	Reconcile seat demand: re-harvest inactive assignments, right-size SKU quantities at renewal, and implement licence assignment automation via group-based licensing.
INFO	Shared mailbox licensing context	1 shared mailboxes detected; many are intentionally unlicensed depending on size and sign-in usage.	Validate shared mailbox size/sign-in patterns before assigning licenses.

Underused / Unused SKUs

SKU	Total	Assigned	Unassigned	Utilisation %
Power Automate Free	10000	1	9999	0%
DEVELOPERPACK_E5	25	7	18	28%
RMSBASIC	1	0	1	0%

Migration Readiness

Moderate risk profile — 4 findings identified with targeted hardening opportunities.

82 **Section Score** — Strong

Metric	Value
Hybrid-synced recipients	5
Custom domains	2
CA policies to recreate	13
Apps to recreate/re-consent	44
Mailbox delegates to preserve	4

Severity	Title	Description	Recommendation
MEDIUM	Hybrid directory sync dependency	5 recipients are synchronised from on-premises Active Directory. This creates a hard dependency on the directory sync infrastructure that must be addressed before any tenant migration or consolidation. UPN and domain reconciliation will also be required.	Define an identity source strategy: Entra Cloud Sync for ongoing hybrid, or staged AD decommission for cloud-only cutover. Map UPN/domain reconciliation path.
MEDIUM	Conditional Access recreation required	13 CA policies require re-implementation and validation in target tenant.	Export CA design and create policy-as-code baseline for migration wave readiness.
MEDIUM	Application migration workload	44 app registrations and enterprise applications require migration planning. Application secrets, certificates, redirect URIs, and API permissions must be recreated in the target tenant. Disruption to business-critical integrations is the primary risk.	Build an application dependency matrix. Sequence high-impact business integrations first and plan secret/certificate rotation alongside migration.
MEDIUM	Mailbox delegate mapping complexity	4 delegate permissions need recreation post-migration.	Extract delegate mappings into migration runbooks and validate with pilot users.

Migration Considerations

Category	Consideration	Recommendation
Hybrid Identity	Hybrid directory sync dependency	Define an identity source strategy: Entra Cloud Sync for ongoing hybrid, or staged AD decommission for cloud-only cutover. Map UPN/domain reconciliation path.
Access Controls	Conditional Access recreation required	Export CA design and create policy-as-code baseline for migration wave readiness.
Applications	Application migration workload	Build an application dependency matrix. Sequence high-impact business integrations first and plan secret/certificate rotation alongside migration.
Messaging	Mailbox delegate mapping complexity	Extract delegate mappings into migration runbooks and validate with pilot users.

Recommended Roadmap

The following prioritised action plan is derived from severity-weighted findings identified during this assessment. Items are ordered by urgency to support remediation planning and resource allocation.

Priority	Category	Action	Reason / Business Impact
Immediate (0-7 days)	Conditional Access	Create a dedicated privileged-role policy requiring phishing-resistant MFA (FIDO2 or certificate-based), compliant device, and named-location restrictions.	No dedicated admin Conditional Access policy — No Conditional Access policy explicitly targeting administrative directory roles was detected. Privileged accounts should be subject to stricter controls than standard users, including phishing-resistant MFA, compliant device requirements, and location restrictions.
Immediate (0-7 days)	Conditional Access	Create an "All Users" baseline policy requiring MFA, then manage exceptions through a minimal, documented exclusion group.	No broad user coverage policy detected — No enabled policy explicitly targets all users. Without an all-user baseline, a significant proportion of identities may bypass MFA and other security controls depending on individual policy scope.
Immediate (0-7 days)	Conditional Access	Create a CA policy blocking all legacy authentication clients. Verify no line-of-business applications depend on these protocols before enforcement.	Legacy authentication not blocked — No policy appears to block legacy authentication clients (POP, IMAP, SMTP, Exchange ActiveSync, etc.). Legacy protocols cannot enforce MFA, making them a primary vector for password-spray and brute-force attacks.
Immediate (0-7 days)	Privileged Access	Enable Entra ID PIM for all privileged roles. Convert permanent assignments to time-limited eligible access with multi-person approval workflows and phishing-resistant MFA gating.	No Privileged Identity Management (PIM) detected — No PIM-eligible role assignments were detected — all privileged access is permanently active. Without just-in-time activation, every privileged identity is a standing, always-on target. This is the single highest-impact control gap for limiting credential compromise blast-radius.
Immediate (0-7 days)	Device Trust	Require compliant or hybrid-joined devices for sensitive applications and administrative workloads. Deploy in report-only mode first to assess user impact.	No device-based Conditional Access enforcement detected — No enabled CA policy requires a compliant or hybrid Azure AD joined device for access. Users may access corporate resources from unmanaged, shared, or compromised devices without restriction.
Immediate (0-7 days)	OAuth Permissions	Audit each grant: remove unnecessary scopes, re-consent with least privilege, and revoke access for unrecognised or unused applications.	High-risk OAuth permissions detected — 7 OAuth grants include high-risk scopes (e.g., Directory.ReadWrite.All, Mail.ReadWrite). These permissions allow applications to read or modify sensitive directory, mailbox, or file data — a compromised or malicious application with these scopes could exfiltrate data or escalate privileges silently.
Immediate (0-7 days)	Application Credentials	Rotate expired credentials immediately. Migrate high-value workloads to certificate-based or managed identity authentication to eliminate secret management overhead.	Expired application credentials — 2 applications have expired credentials. While expired credentials cannot be used for authentication, they indicate a breakdown in credential lifecycle management. The associated workloads may have silently failed, or alternative (potentially less secure) credentials may have been created.
Immediate (0-7 days)	Licensing	Prioritise MFA enforcement for premium-licensed users via Conditional Access registration campaign to realise the full security ROI of the licence investment.	Licensed users missing core security controls — 3 licensed users are not registered for MFA. Premium licences include security features (e.g., Conditional Access, Identity Protection) that require MFA as a foundation. Without MFA, the investment in premium licensing delivers reduced security return.
Short term (30 days)	Identity	Enforce MFA registration via Conditional Access registration campaign. Exclude only verified emergency access accounts.	Low MFA adoption
Short term (30 days)	Identity	Disable stale accounts immediately, enforce joiner/mover/leaver lifecycle controls, and schedule recurring access reviews.	Stale accounts remain enabled
Short term (30 days)	Identity	Investigate each account: disable if orphaned, apply lifecycle governance, or confirm non-interactive use and restrict sign-in scope.	Accounts with no sign-in history
Short term (30 days)	Conditional Access	Introduce device-based grant controls for high-value applications and privileged users. Start with report-only mode to assess impact before enforcement.	No device compliance requirement detected
Short term (30 days)	Device Trust	Create a dedicated admin device-trust policy. For highest-risk roles, consider Privileged Access Workstations (PAWs) or Cloud PCs with strict compliance baselines.	Administrators not constrained to trusted devices
Short term (30 days)	External Access	Implement recurring guest access reviews using Entra ID Access Reviews. Remove dormant B2B accounts and enforce sponsor ownership for all guest invitations.	Dormant guest accounts with active access
Short term (30 days)	OAuth Permissions	Validate publisher trust for each admin-consented application. Enable the admin consent workflow to prevent future uncontrolled grants, and revoke consent for any unrecognised publishers.	Tenant-wide admin-consented application grants
Short term (30 days)	Application Credentials	Schedule credential rotation before expiry. Add Azure Monitor or Key Vault alerts for credential expiry to prevent future surprises.	Application credentials expiring within 30 days
Short term (30 days)	Licensing	Reconcile seat demand: re-harvest inactive assignments, right-size SKU quantities at renewal, and implement licence assignment automation via group-based licensing.	Potential over-licensing detected

Priority	Category	Action	Reason / Business Impact
Short term (30 days)	Hybrid Identity	Define an identity source strategy: Entra Cloud Sync for ongoing hybrid, or staged AD decommission for cloud-only cutover. Map UPN/domain reconciliation path.	Hybrid directory sync dependency
Short term (30 days)	Access Controls	Export CA design and create policy-as-code baseline for migration wave readiness.	Conditional Access recreation required
Short term (30 days)	Applications	Build an application dependency matrix. Sequence high-impact business integrations first and plan secret/certificate rotation alongside migration.	Application migration workload
Short term (30 days)	Messaging	Extract delegate mappings into migration runbooks and validate with pilot users.	Mailbox delegate mapping complexity
Medium term (90 days)	Identity	Ensure dedicated break-glass accounts are clearly named, documented, excluded from Conditional Access, monitored for sign-in activity, and not dependent on any federated identity provider.	Emergency access accounts not explicitly identified
Medium term (90 days)	Conditional Access	Review disabled policies: re-enable or retire as appropriate, and document the reason for any intentional disablement.	Disabled Conditional Access policies present
Medium term (90 days)	Device Trust	N/A — no action required.	Device inventory not yet collected
Medium term (90 days)	Data Exposure	N/A — no action required.	SharePoint sharing configuration not yet assessed
Medium term (90 days)	Application Inventory	N/A — no action required.	Publisher trust verification limited
Medium term (90 days)	Licensing	Validate shared mailbox size/sign-in patterns before assigning licenses.	Shared mailbox licensing context

Organisation Information

Core tenant attributes including directory synchronisation status, verified domains, and administrative contacts. On-premises hybrid sync indicates Active Directory Federation Services (AD FS) or Azure AD Connect is in use, which has implications for identity migration and cutover planning.

Property	Value
Display Name	Andy Kemp Dev
Tenant Type	AAD
Country	—
Preferred Language	en
Hybrid Sync	Enabled
Verified Domains	3
Created	11/04/2024
Last AD Sync	10/04/2026, 14:38:24
Directory Objects	675 / 300,000
Technical Contacts	andrew@kemponline.co.uk

Licenses & Subscriptions

Active Microsoft 365 subscriptions and licence utilisation. Over-provisioned licences represent unnecessary cost, while under-provisioned licences may indicate users without the features they require. Review licence assignments against actual usage to optimise subscription spend.

SKU	Total	Used	Available
Power Automate Free	10000	1	9999
DEVELOPERPACK_E5	25	7	18
RMSBASIC	1	0	1

Domains & Cutover Readiness

Registered and verified domains within the tenant, with cutover analysis for migration planning. Federated domains require identity provider changes before cutover. The default domain must be reassigned before it can be removed. Objects using each domain must be migrated or re-addressed first.

Domain	Auth Type	Default	Verified	Objects Using	Blockers
andykemp.dev	Managed	Yes	Yes	18	18 objects use this domain — must be migrated or re-addressed first; Default domain — reassign default before removal
andykempdev.mail.onmicrosoft.com	Managed		Yes	5	5 objects use this domain — must be migrated or re-addressed first
andykempdev.onmicrosoft.com	Managed		Yes	13	13 objects use this domain — must be migrated or re-addressed first

User Migration Readiness

Users are categorised by their migration readiness based on mailbox forwarding, delegate dependencies, inbox rules, and litigation holds.

Category	Count	Percentage
Ready to Migrate	9	90%
Ready (With Dependencies)	1	10%
Needs Review	0	0%
Blocked	0	0%

Users & Recipients

All mailbox-enabled objects discovered in the tenant, including user mailboxes, shared mailboxes, guest accounts, room and equipment resources, and mail contacts. On-premises synced objects indicate hybrid identity; these require directory sync consideration during any migration or tenant restructure.

19 total recipients: 10 users, 1 guests, 1 shared mailboxes

Display Name	UPN / Alias	Type	Company	Dept	Licensed	Synced
Han Solo	Han.Solo@andykemp.dev (Han.Solo)	User			Yes	
Steve Rogers	Steve.Rogers@andykemp.dev (Steve.Rogers)	User				Yes
Andrew Kemp	andrew.kemp_delaware.co.uk#EXT#@andykempdev.onmicrosoft.com (andrew.kemp_delaware.co.uk#EXT#)	MailUser				
Andy Kemp	andy@andykemp.dev (andy)	User			Yes	
Bruce Banner	Bruce.Banner@andykemp.dev (Bruce.Banner)	User			Yes	Yes
Andrew Kemp	admin@andykempdev.onmicrosoft.com (admin)	User			Yes	

Display Name	UPN / Alias	Type	Company	Dept	Licensed	Synced
Clint Barton	Clint.Barton@andykemp.dev (Clint.Barton)	User			Yes	Yes
Equio1	Equio1@andykemp.dev (Equio1)	EquipmentMailbox				
Pete Mitchell	Pete.Mitchel@andykemp.dev (Pete.Mitchel)	User			Yes	
Peter Parker	Peter.Parker@andykemp.dev (Peter.Parker)	User			Yes	
Room1	Room1@andykemp.dev (Room1)	RoomMailbox	Andy Kemp Dev	Dept1		
Tony Stark	Tony.Stark@andykemp.dev (Tony.Stark)	User				Yes
MFA Registration	MFARegistration@andykemp.dev (MFARegistration)	SharedMailbox				
Nick Fury	Nick.Fury@andykemp.dev (Nick.Fury)	User				Yes
Another new team	Anothernewteam@andykemp.dev	M365Group				
My New Microsoft TEam	MyNewMicrosoftTEam@andykemp.dev	M365Group				
Purview Early Adopters	PurviewEarlyAdopters@andykemp.dev	M365Group				
My New Group	mynewgroup@andykemp.dev	M365Group				
Delay PAW Shutdown	delay-paw@andykemp.dev	DistributionList				

User Detail — Identity & Addresses

Extended identity information for each user, including email aliases (proxy addresses), office location, phone numbers, and account creation date. SMTP: prefixes indicate secondary addresses; the SMTP (uppercase) entry is the primary.

Han Solo

Alias: Han.Solo
Created: 15/03/2026
Email Addresses:
Han.Solo@andykempdev.onmicrosoft.com
Han.Solo@andykemp.dev (Primary)

Steve Rogers

Alias: Steve.Rogers
Created: 09/10/2025
Email Addresses:
X500: /o=Andy Kemp Dev/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=b5405cc1555f420d9d056674aa1e2161
Steve.Rogers@andykempdev.mail.onmicrosoft.com
X500: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=272115953db34ba699d2189088e9dd14-4cc71ff3-1f
X500: /o=Andy Kemp Dev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=cb243bbfacd3469597c975e865d7ccfd-Steve Roge
Steve.Rogers@andykempdev.onmicrosoft.com
Steve.Rogers@andykemp.dev (Primary)

Andrew Kemp

Alias: andrew.kemp_delaware.co.uk#EXT#
Created: 15/12/2025
Email Addresses:
andrew.kemp@delaware.co.uk (Primary)

Andy Kemp

Alias: andy
Created: 04/09/2025
Email Addresses:
andy@andykemp.dev (Primary)

Bruce Banner

Alias: Bruce.Banner
Created: 09/10/2025
Email Addresses:
X500: /o=Andy Kemp Dev/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=44bbcaecc4804527abd77748c1f1ee14
Bruce.Banner@andykempdev.mail.onmicrosoft.com
X500: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c714a74f70fb4273b6c4edc73a09c3d9-7981196c-8f
X500: /o=Andy Kemp Dev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1d871c491d5f46ca8a6c6463f8652b09-Bruce Bann
Bruce.Banner@andykempdev.onmicrosoft.com
Bruce.Banner@andykemp.dev (Primary)

Andrew Kemp

Alias: admin
Phone: 7800503882
Created: 11/04/2024
Email Addresses:
admin@andykemp.dev
admin@andykempdev.onmicrosoft.com (Primary)

Clint Barton

Alias: Clint.Barton
Created: 30/10/2025
Email Addresses:
X500: /o=Andy Kemp Dev/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=25dde811b91346d68df1d284ddf38dea
X500: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=b60eeb90f52f4cadb9fd5678a3c8529f-872278b8-ae
X500: /o=Andy Kemp Dev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=34272c21dc2b45899d81bb8506d4c880-Clint Bart
Clint.Barton@andykempdev.onmicrosoft.com
Clint.Barton@andykempdev.mail.onmicrosoft.com
Clint.Barton@andykemp.dev (Primary)

Equio1

Alias: Equio1
Created: 23/03/2026
Email Addresses:
Equio1@andykempdev.onmicrosoft.com
Equio1@andykemp.dev (Primary)

Pete Mitchell

Alias: Pete.Mitchel
Created: 16/12/2025
Email Addresses:
petemitchell@andykempdev.onmicrosoft.com (Primary)
Pete.Mitchel@andykemp.dev

Peter Parker

Alias: Peter.Parker
Created: 17/03/2026
Email Addresses:
peter.parker@andykempdev.onmicrosoft.com
Peter.Parker@andykemp.dev (Primary)

Room1

Alias: Room1
Company: Andy Kemp Dev
Office: Top Floor
Location: Street1, City, Edin, EH9 3EN, United Kingdom
Phone: 0123456789
Created: 23/03/2026
Email Addresses:
Room1@andykempdev.onmicrosoft.com
Room1@andykemp.dev (Primary)

Tony Stark

Alias: Tony.Stark
Created: 09/10/2025
Email Addresses:
X500: /o=Andy Kemp Dev/ou=External (FYDIBOHF25SPDLT)/cn=Recipients/cn=f9f3295030ec4601b3e82eda1261f14a
Tony.Stark@andykempdev.mail.onmicrosoft.com
X500: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=5a730ec03f1c48259a66f54443350043-e3a5c6ce-bb
X500: /o=Andy Kemp Dev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0105e5bcdee7465b8c07af6d88b24f51-Tony Stark
Tony.Stark@andykempdev.onmicrosoft.com
Tony.Stark@andykemp.dev (Primary)

MFA Registration

Alias: MFARegistration
Created: 23/01/2026
Email Addresses:
MFARegistration@andykempdev.onmicrosoft.com
MFARegistration@andykemp.dev
MFA-Registration@andykempdev.onmicrosoft.com (Primary)

Nick Fury

Alias: Nick.Fury
Created: 30/10/2025
Email Addresses:
X500: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e71efca3b7734cc6859d564d0b128ecf-fa2b368d-d7
X500: /o=Andy Kemp Dev/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=bf7bdaf3d0524c0bafa36de24898723b-Nick Fury
Nick.Fury@andykempdev.onmicrosoft.com
Nick.Fury@andykempdev.mail.onmicrosoft.com
Nick.Fury@andykemp.dev (Primary)

MFA Registration Status

Multi-factor authentication is one of the most effective security controls available. Microsoft recommends 100% MFA registration. Users without MFA are significantly more vulnerable to credential attacks. Passwordless methods (FIDO2, Windows Hello) offer the strongest protection and best user experience.

38%

5 of 13 users MFA registered

User	MFA	SSPR	Passwordless	Methods	Default Method
Andrew Kemp	Yes	Yes	Yes	windowsHelloForBusiness, passKeyDeviceBound, passKeyDeviceBoundAuthenticator, microsoftAuthenticatorPush, softwareOneTimePasscode	—
Andrew Kemp	Yes	Yes		microsoftAuthenticatorPush, softwareOneTimePasscode	—
Andy Kemp	No			—	—
Bruce Banner	Yes	Yes		microsoftAuthenticatorPush, softwareOneTimePasscode	—
Clint Barton	No			—	—
Equio1	No			—	—
Han Solo	Yes	Yes		microsoftAuthenticatorPush, softwareOneTimePasscode	—
Nick Fury	No			—	—
Pete Mitchell	No			—	—
Peter Parker	Yes	Yes		microsoftAuthenticatorPush, softwareOneTimePasscode	—
Room1	No			—	—
Steve Rogers	No			—	—
Tony Stark	No			—	—

Sign-In Activity

User sign-in activity identifies stale accounts (90+ days inactive) and disabled accounts. Stale accounts are a security risk — they may have valid credentials that could be compromised without detection. Best practice is to disable or remove stale accounts and review them regularly as part of an identity governance programme.

3 stale accounts (90+ days inactive) — 1 disabled accounts

User	Enabled	Last Sign-In	Days Inactive	Stale
Clint Barton	Yes	Never	—	
Equio1	Yes	Never	—	
MFA Registration	No	Never	—	
Nick Fury	Yes	Never	—	

User	Enabled	Last Sign-In	Days Inactive	Stale
Room1	Yes	Never	—	
Tony Stark	Yes	30/10/2025	162	Yes
Andrew Kemp	Yes	16/12/2025	115	Yes
Pete Mitchell	Yes	16/12/2025	114	Yes
Andy Kemp	Yes	20/01/2026	79	
Steve Rogers	Yes	23/01/2026	76	
Han Solo	Yes	17/03/2026	24	
Peter Parker	Yes	20/03/2026	21	
Bruce Banner	Yes	07/04/2026	2	
Andrew Kemp	Yes	08/04/2026	1	

Entra ID Role Assignments

Privileged directory role assignments control administrative access across the tenant. Permanent active assignments should be minimised — Microsoft best practice recommends Privileged Identity Management (PIM) for just-in-time activation of admin roles, with only designated emergency access (break-glass) accounts retaining permanent Global Admin.

Role	Principal	Type	Assignment
Global Administrator	Andrew Kemp	User	Active
Global Administrator	Andrew Kemp	User	Active
Exchange Administrator	TenantLift MRS Migration	ServicePrincipal	Active
Exchange Administrator	TenantLift	ServicePrincipal	Active
	Microsoft Rights Management Services	ServicePrincipal	Active
	Microsoft Office 365 Portal	ServicePrincipal	Active
Directory Readers	Microsoft.Azure.SyncFabric	ServicePrincipal	Active
Directory Readers	MicrosoftAzureActiveAuthn	ServicePrincipal	Active

Privileged Access Strategy

This section assesses the organisation's privileged access maturity against Microsoft's recommended practices. It evaluates PIM adoption, standing privilege exposure, emergency access configuration, and Conditional Access controls targeting privileged roles.

25 **Maturity** — Low

No PIM detected. All privileged access is permanent, though the Global Admin count is within a limited range.

Metric	Value
Total Role Assignments	8
User Assignments	2
Service Principal Assignments	6
Permanent (Active) Assignments	8
PIM Eligible Assignments	0
Unique Privileged Users	2
Global Administrators (Total)	2

Metric	Value
Permanent Global Admins	2
PIM In Use	No

Identified Risks

- No PIM-eligible assignments detected — all privileged access is permanently active, creating a standing attack surface
- 6 service principal role assignments — review for necessity and apply least-privilege scoping

Protection Controls

Control	Status
PIM for Just-In-Time Access	NOT IN USE — All access is permanently active
CA Policies Targeting Admin Roles	Detected
Compliant Device Requirement	Detected
Emergency Access Account Strategy	2 permanent GA (within best practice range)

Recommendations

#	Recommendation
1	Enable Entra ID PIM for all administrative roles. Require time-limited activation, multi-person approval workflows, and phishing-resistant MFA.
2	Maintain separate cloud-only admin accounts not synchronised from on-premises Active Directory.
3	Conduct quarterly reviews of privileged role assignments and remove stale or unnecessary access.

Mailbox Usage

Per-user mailbox storage consumption, item counts, and archive mailbox status. Large mailboxes (>50 GB) add complexity and time to migrations. Archive mailboxes indicate users with retention or compliance requirements that must be preserved during any migration.

13 mailboxes — Total storage: 147.0 MB — 23,508 items — 0 with archive

10 user (140.7 MB) • 1 shared (6.3 MB) • 2 room/equipment (0 B)

3 on-prem synced mailbox(es) have no Exchange Online stats in this run.

Display Name	Primary SMTP / UPN	Type	Storage Used	Item Count	Archive	Delegates
Andrew Kemp	admin@andykempdev.onmicrosoft.com	User	120.0 MB	7,021		—
MFA Registration	MFA-Registration@andykempdev.onmicrosoft.com	Shared	6.3 MB	330		—
Bruce Banner	Bruce.Banner@andykemp.dev	User	4.8 MB	4,629		—
Peter Parker	Peter.Parker@andykemp.dev	User	4.6 MB	2,324		—
Clint Barton	Clint.Barton@andykemp.dev	User	4.0 MB	3,365		—
Pete Mitchell	petemitchell@andykempdev.onmicrosoft.com	User	2.9 MB	2,124		—
Andy Kemp	andy@andykemp.dev	User	2.8 MB	1,984		—
Han Solo	Han.Solo@andykemp.dev	User	1.7 MB	1,731		Bruce Banner
Steve Rogers	Steve.Rogers@andykemp.dev	User (OnPrem/no EXO stats)	0 B	0		—
Equio1	Equio1@andykemp.dev	Equipment	0 B	0		Peter Parker, Bruce Banner
Room1	Room1@andykemp.dev	Room	0 B	0		Bruce Banner
Tony Stark	Tony.Stark@andykemp.dev	User (OnPrem/no EXO	0 B	0		—

Display Name	Primary SMTP / UPN	Type	Storage Used	Item Count	Archive	Delegates
		stats)				
Nick Fury	Nick.Fury@andykemp.dev	User (OnPrem/no EXO stats)	0 B	0		—

Resource Mailbox Settings

Room and equipment mailbox configuration including physical location, capacity, and booking policy settings. These settings determine how rooms and equipment can be booked, who can book them automatically, and any scheduling restrictions. This data is critical for migration planning to ensure room/equipment booking workflows are preserved.

1 room, 1 equipment mailbox

Name	Type	Building	Floor	Label	Capacity	Booking	Processing	Window	Max (min)	Conflicts
Equio1	Equipment	—	—	—	—	—	—	—	—	—
Room1	Room	Top Floor	—	—	5	standard	—	—	—	—

Mailbox Delegate Access

Mailbox delegate permissions (Full Access, Send As, Send on Behalf) allow users to operate on other mailboxes. These permissions are often used for shared workflows and must be carefully mapped and recreated during migration. Unexpected delegate access may also indicate a security risk that should be reviewed.

Mailbox	Delegate	Access Rights
Han Solo	Bruce Banner	SendOnBehalf
Equio1	Peter Parker	SendOnBehalf
Equio1	Bruce Banner	SendOnBehalf
Room1	Bruce Banner	SendOnBehalf

OneDrive Usage

Per-user OneDrive storage consumption and file counts. Large OneDrive libraries extend migration timelines and may require delta-sync approaches. Users with very high file counts may also experience sync client issues.

5 users with OneDrive — Total storage: 457.9 MB

Display Name	UPN	Storage Used	Files
Peter Parker	Peter.Parker@andykemp.dev	456.9 MB	0
Bruce Banner	Bruce.Banner@andykemp.dev	407.9 KB	0
Andrew Kemp	admin@andykempdev.onmicrosoft.com	347.5 KB	0
Han Solo	Han.Solo@andykemp.dev	178.3 KB	0
Pete Mitchell	Pete.Mitchel@andykemp.dev	106.7 KB	0

OneDrive Sharing

Files and folders shared from OneDrive, categorised by sharing scope. External and anonymous sharing represent data exposure risk and should be reviewed. During migration, sharing permissions must be recreated or users will lose access to shared content.

8 Internal • 0 External • 0 Anonymous

Owner	Item	Type	Scope
Han.Solo@andykemp.dev	Meetings	Folder	internal
Han.Solo@andykemp.dev	Recordings	Folder	internal

Owner	Item	Type	Scope
admin@andykempdev.onmicrosoft.com	Meetings	Folder	internal
admin@andykempdev.onmicrosoft.com	Recordings	Folder	internal
Peter.Parker@andykemp.dev	ben vane	Folder	internal
Peter.Parker@andykemp.dev	DLA	Folder	internal
Peter.Parker@andykemp.dev	Meetings	Folder	internal
Peter.Parker@andykemp.dev	Recordings	Folder	internal

External Access & Collaboration Posture

This section assesses the tenant's external exposure: guest users, OneDrive/SharePoint sharing, mailbox forwarding, and cross-tenant trust. An overly permissive external posture increases the risk of data leakage, while overly restrictive settings may hinder legitimate business collaboration.

Restricted

The tenant has 1 guest user across 1 external domain. External sharing and guest access appear limited. This is appropriate for organisations with strict data confidentiality requirements.

Metric	Value
Guest Users	1
Guest Domains	1
Guest Invite Policy	Unknown
Cross-Tenant Policies	2
OneDrive External Shares	0
OneDrive Anonymous Links	0
Users with External OD Shares	0
Mailboxes with Forwarding	0

Top Guest Domains

Domain	Guest Count
delaware.co.uk	1

Teams

Microsoft Teams workloads with membership, channel counts, and archive status. Teams with external guests require cross-tenant collaboration policies. Archived teams should be reviewed for retention and may be candidates for removal to reduce migration scope.

Name	Visibility	Members	Owners	Guests	Channels	Archived
My New Microsoft TEam	Private	3	1	0	1	
Another new team	Public	4	1	0	1	

SharePoint Sites

SharePoint Online sites with storage and document library information. Large sites and those with customisations (workflows, custom web parts) add complexity to migrations. Review site permissions, external sharing settings, and any third-party

integrations before planning a migration.

12 sites — 28.4 MB total storage — 18 libraries — 0 items — 2 Teams sites — 0 personal sites

Title	URL	Storage	Libraries	Items
Another new team	https://andykempdev.sharepoint.com/sites/Anothernewteam	1.5 MB	1	0
My New Microsoft TEam	https://andykempdev.sharepoint.com/sites/MyNewMicrosoftTEam	1.4 MB	1	0
MFA Ops	https://andykempdev.sharepoint.com/sites/MFA	1.4 MB	1	0
My New Group	https://andykempdev.sharepoint.com/sites/mynewgroup	1.3 MB	1	0
Purview Early Adopters	https://andykempdev.sharepoint.com/sites/PurviewEarlyAdopters	1.3 MB	1	0
Andrew Kemp 3	https://andykempdev.sharepoint.com/sites/customer2	3.7 MB	2	0
Andrew Kemp	https://andykempdev.sharepoint.com/sites/Customer1	3.7 MB	2	0
Customer2	https://andykempdev.sharepoint.com/sites/12345678	3.7 MB	3	0
Customer2	https://andykempdev.sharepoint.com/sites/qrstuvw1	3.7 MB	2	0
Customer3	https://andykempdev.sharepoint.com/sites/567899sdfg	3.7 MB	2	0
Communication site	https://andykempdev.sharepoint.com	1.5 MB	1	0
Team Site	https://andykempdev.sharepoint.com/sites/contentTypeHub	1.5 MB	1	0

Libraries & Lists — Another new team

Name	Type	Items	Last Modified
Documents	Document Library	0	08/04/2026

Libraries & Lists — My New Microsoft TEam

Name	Type	Items	Last Modified
Documents	Document Library	0	03/04/2026

Libraries & Lists — MFA Ops

Name	Type	Items	Last Modified
Events	List	0	11/01/2026
Documents	Document Library	0	11/01/2026
MFA Onboarding	List	0	10/04/2026

Libraries & Lists — My New Group

Name	Type	Items	Last Modified
Documents	Document Library	0	11/01/2026

Libraries & Lists — Purview Early Adopters

Name	Type	Items	Last Modified
Documents	Document Library	0	01/11/2025

Libraries & Lists — Andrew Kemp 3

Name	Type	Items	Last Modified
Tasks	List	0	10/12/2024
Site Collection Images	List	0	02/04/2026
Reusable Content	List	0	10/12/2024
Documents	Document Library	0	02/04/2026
Workflow Tasks	List	0	10/12/2024
Content and Structure Reports	List	0	10/12/2024
Site Collection Documents	Document Library	0	02/04/2026

Libraries & Lists — Andrew Kemp

Name	Type	Items	Last Modified
Documents	Document Library	0	03/04/2026
Content and Structure Reports	List	0	10/12/2024
Workflow Tasks	List	0	10/12/2024
Site Collection Documents	Document Library	0	03/04/2026
Tasks	List	0	10/12/2024
Reusable Content	List	0	10/12/2024
Site Collection Images	List	0	03/04/2026

Libraries & Lists — Customer2

Name	Type	Items	Last Modified
Content and Structure Reports	List	0	02/12/2024
Site Collection Images	List	0	02/04/2026
Tasks	List	0	02/12/2024
Manual Uploads	Document Library	0	02/04/2026
Site Collection Documents	Document Library	0	02/04/2026
Reusable Content	List	0	02/12/2024
Documents	Document Library	0	02/04/2026
Workflow Tasks	List	0	02/12/2024

Libraries & Lists — Customer2

Name	Type	Items	Last Modified
Content and Structure Reports	List	0	02/12/2024
Site Collection Images	List	0	03/04/2026
Tasks	List	0	02/12/2024
Workflow Tasks	List	0	02/12/2024
Site Collection Documents	Document Library	0	03/04/2026
Documents	Document Library	0	03/04/2026
Reusable Content	List	0	02/12/2024

Libraries & Lists — Customer3

Name	Type	Items	Last Modified
Documents	Document Library	0	02/04/2026
Site Collection Documents	Document Library	0	02/04/2026
Tasks	List	0	02/12/2024
Site Collection Images	List	0	02/04/2026
Workflow Tasks	List	0	02/12/2024
Content and Structure Reports	List	0	02/12/2024
Reusable Content	List	0	02/12/2024

Libraries & Lists — Communication site

Name	Type	Items	Last Modified
Documents	Document Library	0	07/04/2024
Events	List	0	07/04/2024

Libraries & Lists — Team Site

Name	Type	Items	Last Modified
Documents	Document Library	0	07/04/2024

M365 Groups

Microsoft 365 groups are the backbone of collaboration services (Teams, SharePoint, Planner, Outlook). Each group provisions a shared mailbox, calendar, SharePoint site, and Planner board. During migration, group membership, ownership, and associated resources must all be preserved.

Name	Visibility	Members	Owners
Another new team	Public	4	0
My New Microsoft TEam	Private	3	0
Purview Early Adopters	Private	3	0
My New Group	Public	0	0

Members of "Another new team" (4)

Member	UPN	Type
Andrew Kemp	admin@andykempdev.onmicrosoft.com	user
Tony Stark	Tony.Stark@andykemp.dev	user
Bruce Banner	Bruce.Banner@andykemp.dev	user
Peter Parker	Peter.Parker@andykemp.dev	user

Members of "My New Microsoft TEam" (3)

Member	UPN	Type
Andrew Kemp	admin@andykempdev.onmicrosoft.com	user
Bruce Banner	Bruce.Banner@andykemp.dev	user
Han Solo	Han.Solo@andykemp.dev	user

Members of "Purview Early Adopters" (3)

Member	UPN	Type
Bruce Banner	Bruce.Banner@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user
Nick Fury	Nick.Fury@andykemp.dev	user

Distribution Lists

Mail-enabled distribution lists for email broadcasting. Distribution lists are a legacy construct — many organisations are migrating these to M365 groups for richer collaboration. During migration, distribution lists must be recreated or converted, and email flow rules updated accordingly.

Name	Mail	Members	Owners
Delay PAW Shutdown	delay-paw@andykemp.dev	0	0

Security Groups

Security groups control access to resources, applications, and conditional access policies. Dynamic groups use rules based on user attributes, while assigned groups have manually managed membership. On-premises synced groups require special handling during migration to maintain access continuity.

Name	Type	Members	On-Prem Synced
MFA-Reg	Assigned	0	
Licenses	Assigned	0	
AVD-Admin	Assigned	1	
Regular MFA	Assigned	3	
Access Review Group	Assigned	0	
Office	Assigned	1	
AVD-Users	Assigned	2	
Passkey	Assigned	2	
_Grp-Passkey	Assigned	4	
License	Assigned	5	
MFA Enabled Users	Assigned	1	
Early Adopters	Assigned	2	

Members of "AVD-Admin" (1)

Member	UPN	Type
Andrew Kemp	admin@andykempdev.onmicrosoft.com	user

Members of "Regular MFA" (3)

Member	UPN	Type
Tony Stark	Tony.Stark@andykemp.dev	user
Bruce Banner	Bruce.Banner@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user

Members of "Office" (1)

Member	UPN	Type
AKD-C1	—	device

Members of "AVD-Users" (2)

Member	UPN	Type
Bruce Banner	Bruce.Banner@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user

Members of "Passkey" (2)

Member	UPN	Type
Andrew Kemp	admin@andykempdev.onmicrosoft.com	user
Tony Stark	Tony.Stark@andykemp.dev	user

Members of "_Grp-Passkey" (4)

Member	UPN	Type
Andy Kemp	andy@andykemp.dev	user
Bruce Banner	Bruce.Banner@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user
Nick Fury	Nick.Fury@andykemp.dev	user

Members of "License" (5)

Member	UPN	Type
Tony Stark	Tony.Stark@andykemp.dev	user
Bruce Banner	Bruce.Banner@andykemp.dev	user
Steve Rogers	Steve.Rogers@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user
Nick Fury	Nick.Fury@andykemp.dev	user

Members of "MFA Enabled Users" (1)

Member	UPN	Type
Bruce Banner	Bruce.Banner@andykemp.dev	user

Members of "Early Adopters" (2)

Member	UPN	Type
Bruce Banner	Bruce.Banner@andykemp.dev	user
Clint Barton	Clint.Barton@andykemp.dev	user

Microsoft Secure Score

Microsoft Secure Score is a measurement of an organisation's security posture based on configuration and behavioural metrics. A higher score indicates more security controls are in place. Each control represents a specific best practice recommendation from

Microsoft. Review low-scoring controls for quick security wins.

65% — 356.92 of 547 points — Services: HasAADP1, HasAADP2, HasOCAS, HasMCAS, HasAATP, HasCLB, HasMDOP1, HasMDOP2, HasEXOP2, HasAIPP1, HasAIPP2, HasSPOP2

Control	Score
meeting_restrictanonymousjoin_v1	0
meeting_pstnusersbypasslobby_v1	1
meeting_externalrequestcontrol_v1	1
meeting_anonymousstartmeeting_v1	1
meeting_autoadmitusers_v1	0
meeting_designatedpresenter_v1	0
IntegratedApps	4
PasswordHashSync	5
PWAgePolicyNew	8
SelfServicePasswordReset	1
BlockLegacyAuthentication	4.92
MFARegistrationV2	9
AdminMFAV2	5
SigninRiskPolicy	0
UserRiskPolicy	0
OneAdmin	1
RoleOverlap	0
forms_phishing_protection	6
spo_block_onedrive_sync_unmanaged_devices	0
spo_external_sharing_managed	0
spo_external_users_sharing	0
admincenter_owned_apps_and_services	0
mip_DLP_policies_Teams	3
aad_third_party_apps	0
aad_sign_in_freq_session_timeout	0
aad_phishing_MFA_strength	0
aad_limited_administrative_roles	0
aad_admin_consent_workflow	0
aad_admin_accounts_separate_unassigned_cloud_only	0
aad_password_protection	6
aad_custom_banned_passwords	5
aad_linkedin_connection_disables	0
sway_block_sharing_with_outside_users	0
mcas_mda_enabled	5
exo_SPF_records_for_all_domains	5

Control	Score
AATP_DefenderForIdentityIsNotInstalled	5
spo_idle_session_timeout	0
spo_legacy_auth	0
AATP_AdminSDHolder	5
AATP_ClearText	5
AATP_DomainControllerLocalUsers	5
AATP_DormantAccounts	5
AATP_KerberosDelegations	5
AATP_HoneyToken	0
AATP_NonAdminDCSyncAccounts	5
AATP_PathRisk	5
AATP_PrintSpooler	5
AATP_PwdLAPS	5
AATP_SIDHistory	5
AATP_UnsecureAccount	5
AATP_Vpn	0
AATP_WeakCipher	5
AATP_Sensor	4
AATP_UnsecureDomain	5
mdo_atpprotection	5
dlp_datalossprevention	5
exo_individualsharing	0
mdo_safedocuments	5
mdo_connectionfilter	1
mip_purviewlabelconsent	0
CustomerLockBoxEnabled	0
exo_oauth2clientprofileenabled	3
exo_mailtipsenabled	0
exo_transportrulesallowlistdomains	3
mip_search_auditlog	0
exo_mailboxaudit	0
exo_storageproviderrestricted	0
exo_outlookaddins	3
mdo_zapspam	1
mdo_zapphish	3
mdo_zapmalware	6
mdo_safeattachments	8
mdo_safelinksforemail	9

Control	Score
mdo_commonattachmentsfilter	5
mip_sensitivitylabelspolicies	2
mip_autosensitivitylabelspolicies	0
mdo_highconfidencespamaction	0
mdo_phisspamacation	0
mdo_highconfidencephishaction	5
mdo_bulkspamaction	3
mdo_quarantineretentionperiod	0
mdo_allowedsenderscombined	2
mdo_bulkthreshold	0
mdo_spamaction	5
mdo_autoforwardingmode	0
mdo_recipientexternallimitperhour	1
mdo_recipientinternallimitperhour	1
mdo_recipientlimitperday	1
mdo_thresholdreachedaction	0
mdo_enablemailboxintelligence	8
mdo_mailboxintelligenceprotection	0
mdo_mailboxintelligenceprotectionaction	0
mdo_enabledomainstoprotect	0
mdo_phishthresholdlevel	0
mdo_similardomainssafetytips	0
mdo_similaruserssafetytips	0
mdo_targeteddomainprotectionaction	0
mdo_targeteduserprotectionaction	0
mdo_targetedusersprotection	0
mdo_unusualcharacterssafetytips	0
mdo_spam_notifications_only_for_admins	0
mdo_safeattachmentpolicy	5
mdo_safelinksforOfficeApps	0
mdo_antiphishingpolicies	0
mdo_blockmailforward	0
McasFirewallLogUpload	0
AATP_DnsAdminsGroupWithUnsafePermissions	8
AATP_GroupPolicyAbnormalModificationAssignment	5
AATP_GroupPolicyPasswordInPreferences	8
AATP_GroupPolicyAssignsUnprivilegedIdentitiesToElevatedLocalGroups	7
AATP_AccountsWithNonDefaultPrimaryGroup	5

Control	Score
AATP_BuiltinGuestAccountIsEnabled	5
AATP_DomainControllersWithOldPassword	5
AATP_BuiltinKrbtgtAccountWithOldPassword	5
AATP_BuiltinAdministratorAccountWithOldPassword	5
AATP_PrivilegedAccountsWithDelegationAllowed	5
AATP_SingleManagedServiceAccountsWithOldPassword	6
AATP_GroupManagedServiceAccountWithUnrecommendedPasswordChangeInterval	6
AATP_ExposedPasswordsInADAttributes	8
AATP_InactiveServiceAccounts	5
AATP_AdAccountWithPotentiallyLeakedCredentials	5
AATP_AccountWithLeakedCredentials	5
AATP_AccountsInOperatorGroups	8
AATP_ServiceAccountsInPrivilegedGroup	7
AATP_StaleAccounts	5
AATP_PrivilegedEntraIdAndActiveDirectoryAccounts	9

Conditional Access Policies

Conditional Access is the Zero Trust control plane for Microsoft 365. Policies define conditions under which access is granted, blocked, or requires additional verification. This section provides a coverage analysis and deep-dive into each policy's conditions and grant controls to identify gaps and opportunities for hardening.

Coverage Analysis

Metric	Value
Total Policies	13
Enabled	11
Report-Only (Testing)	0
Disabled	2
Targeting All Users	1
Targeting Admin Roles	0
Requiring MFA	5
Using Phishing-Resistant Auth	0
Referencing Named Locations	0
Using Risk-Based Conditions	0
Using Device Filters	5
Disabled but Important	2
Broad Scope (No Exclusions)	0
With Exclusions to Review	3

Gaps Identified

- No policies specifically target admin roles — privileged accounts share standard-user controls.
- No policies use sign-in or user risk conditions — Identity Protection signals are not leveraged.
- 2 disabled policy(ies) contain MFA or block controls — may have been accidentally disabled.

Policy Detail

101 - All Users Phishing Resistant MFA (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	All
Auth Strength	Passkey Authentication
Client App Types	all
Created	19/02/2025
Last Modified	19/01/2026

801 - Temp Number Match MFA (Enabled)

Setting	Value
Included Users / Groups	Group: 1c3476a1-a4f3-4e80-8a75-89f7ace10fc2
Included Applications	All
Grant Controls	mfa
Client App Types	all
Created	19/02/2025

999 - Re-auth for PIM (Enabled)

Setting	Value
Included Users / Groups	Group: 80dd087d-7d88-494c-b7c0-a8916882508f
Excluded Users / Groups	Group: 1c3476a1-a4f3-4e80-8a75-89f7ace10fc2
Grant Controls	mfa
Session Controls	signInFrequency
Client App Types	all
Created	19/02/2025
Last Modified	19/02/2025

901 - Privileged Access Workstation Access only (Disabled)

Setting	Value
Included Users / Groups	Group: 7fc56f52-9dfb-4da7-a175-914f65b80e6f
Excluded Users / Groups	Group: 1c3476a1-a4f3-4e80-8a75-89f7ace10fc2
Included Applications	All
Excluded Applications	d4ebce55-015a-49b5-a083-c84d1797ae8c, 9cdead84-a844-4324-93f2-b2e6bb768d07, 0af06dc6-e4b5-4f28-818e-e78e62d137a5, 270efc09-cd0d-444b-a71f-39af4910ec45
Grant Controls	block
Device Filter	device.extensionAttribute1 -eq "cloud Privileged Access Workstation"

Setting	Value
Client App Types	all
Created	19/02/2025
Last Modified	29/04/2025

998 - Reauthenticate every 8 hrs (Enabled)

Setting	Value
Included Users / Groups	Group: 7fc56f52-9dfb-4da7-a175-914f65b80e6f
Included Applications	All
Auth Strength	Passkey Authentication
Session Controls	signInFrequency
Client App Types	all
Created	26/03/2025
Last Modified	26/03/2025

902 - Restrict Access to the cloud PAW (Disabled)

Setting	Value
Included Users / Groups	Group: 7fc56f52-9dfb-4da7-a175-914f65b80e6f
Included Applications	9cdead84-a844-4324-93f2-b2e6bb768d07, 0af06dc6-e4b5-4f28-818e-e78e62d137a5, 270efc09-cd0d-444b-a71f-39af4910ec45
Grant Controls	block
Device Filter	device.extensionAttribute1 -eq "Access to cPAW"
Client App Types	all
Created	27/03/2025
Last Modified	29/04/2025

MFA (Enabled)

Setting	Value
Included Users / Groups	All Users
Excluded Users / Groups	834bc9aa-557b-4e4d-8f2e-6882bbbeaeb7, Group: 770eaa24-3048-434c-baa9-ecd347384fae, Group: 6743ec51-ae72-4a7a-9c28-abe5f353acf6
Included Applications	All
Grant Controls	mfa
Client App Types	all
Created	28/09/2025
Last Modified	19/01/2026

101-EarlyAdopters-AllResources-EnforcedModernMFA-Default (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	All
Auth Strength	Passkey Authentication
Client App Types	all
Created	13/10/2025

102-EarlyAdopters-AllResources-EnforcedRegularMFA-Default (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	All
Grant Controls	mfa
Client App Types	all
Created	13/10/2025

201-EarlyAdopters-AllResources-ManageDevice-Default (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	All
Grant Controls	block
Device Filter	device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD"
Client App Types	exchangeActiveSync, mobileAppsAndDesktopClients, other
Platforms	windows, macOS
Created	13/10/2025

301-EarlyAdopters-AllResources-PersonalDesktop-Restriction (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	All
Session Controls	cloudAppSecurity, signInFrequency
Device Filter	device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD"
Client App Types	all
Platforms	windows, macOS
Created	13/10/2025

302-EarlyAdopters-AllResources-PersonalMobileDevice-Restriction (Enabled)

Setting	Value
Included Users / Groups	None
Included Applications	00000002-0000-0ff1-ce00-000000000000
Grant Controls	block
Device Filter	device.deviceOwnership -eq "Company"
Client App Types	exchangeActiveSync, browser, other
Platforms	android, iOS
Created	13/10/2025

MFA Registration (Enabled)

Setting	Value
Included Users / Groups	Group: 8fca5ba6-a9b4-4bb6-a720-914e48098276
Included Applications	All
Grant Controls	mfa
Client App Types	all
Created	19/01/2026
Last Modified	19/01/2026

App Registrations & Credential Health

Application registrations and enterprise applications with credential lifecycle analysis. Applications with expired or expiring secrets and certificates create service outage risk. Third-party apps with broad permissions should be reviewed against the principle of least privilege. During migration, app registrations must be recreated in the target tenant and client IDs will change — impacting all dependent integrations.

Credential Expiry Status

4 expired • 5 expiring within 30 days • 0 within 60 days • 0 within 90 days

Status	Application	Type	Expiry Date
CRITICAL	akdev-arc	Secret	13/12/2024
CRITICAL	P2P Server	Secret	27/06/2025
CRITICAL	P2P Server	Certificate	27/06/2025
CRITICAL	ConnectSyncProvisioning_DEV-EX_d15d8fce809f	Certificate	28/03/2026
HIGH	func-mfa-enrol-2213	Certificate	19/04/2026
HIGH	invite-orchestrator	Certificate	20/04/2026
HIGH	func-mfa-enrol-534430	Certificate	23/04/2026
HIGH	mfa-invite-orchestrator	Certificate	23/04/2026
HIGH	AndyKempDev-SCEP	Secret	02/05/2026

Application Inventory

Name	Type	Secrets	Certs	Earliest Expiry
DevGenie-SSO	Application	0	0	
DelDev	Application	0	0	

Name	Type	Secrets	Certs	Earliest Expiry
ConnectSyncProvisioning_SERVER1_3cc7ca2758cb	Application	0	1	
TAPManager	Application	0	2	
AKD-SPO-Automation-MFA	Application	0	1	
Migration Manager	Application	0	2	
akdev-arc	Application	1	0	13/12/2024
AKD-MFA-Upload-Portal	Application	0	0	
DevGenie-SAML	Application	0	0	
P2P Server	Application	0	0	
ConnectSyncProvisioning_DEV-EX_d15d8fce809f	Application	0	1	
test	Application	0	0	
SPO-Automation-MFA	Application	0	1	
AndyKempDev-SCEP	Application	1	0	02/05/2026
OpenVPN Access Server (Edinburgh)	Application	0	0	
Migration Manager	ServicePrincipal	0	0	
func-mfa-enrol-534430	ManagedIdentity	0	1	
AKD-SPO-Automation-MFA	ServicePrincipal	0	0	
O365 LinkedIn Connection	ServicePrincipal	0	0	
avd-1	ManagedIdentity	0	0	
avd-2	ManagedIdentity	0	0	
TAPManager	ServicePrincipal	0	0	
SPO-Automation-MFA	ServicePrincipal	0	0	
func-mfa-enrol-2213	ManagedIdentity	0	1	
invite-orchestrator	ManagedIdentity	0	1	
AKD-MFA-Upload-Portal	ServicePrincipal	0	0	
Graph Explorer	ServicePrincipal	0	0	
TenantLift MRS Migration	ServicePrincipal	0	0	
akdev-arc	ServicePrincipal	0	0	
test	ServicePrincipal	0	0	
Microsoft Graph Command Line Tools	ServicePrincipal	0	0	
DevGenie-SSO	ServicePrincipal	0	0	
DelDev	ServicePrincipal	0	0	
TenantLift	ServicePrincipal	0	0	
DevGenie-SAML	ServicePrincipal	1	2	15/10/2028
avd-0	ManagedIdentity	0	0	
ConnectSyncProvisioning_SERVER1_3cc7ca2758cb	ServicePrincipal	0	0	
ConnectSyncProvisioning_DEV-EX_d15d8fce809f	ServicePrincipal	0	0	
Azure Logic Apps - Azure AD	ServicePrincipal	0	0	
AndyKempDev-SCEP	ServicePrincipal	0	0	

Name	Type	Secrets	Certs	Earliest Expiry
mfa-invite-orchestrator	ManagedIdentity	0	1	
OpenVPN Access Server (Edinburgh)	ServicePrincipal	1	2	18/09/2027
P2P Server	ServicePrincipal	2	2	27/06/2025
AKC M365 Tenant Audit	ServicePrincipal	0	0	

Intune Device Management

Device management policies including configuration profiles, compliance policies, and app protection policies. These policies define the device security baseline and must be recreated in any target tenant. Review platform coverage — gaps may indicate unmanaged device populations in the organisation.

Metric	Value
Total Policies	6
Total Assignments	7
Policies for Windows	6
ConfigurationProfile	6

No compliance policies detected — devices cannot be evaluated for conditional access.

No app protection policies detected — corporate data on unmanaged devices is unprotected.

Policies only cover 1 platform(s) — potential gap for other device types.

Policy Inventory

Name	Type	Platform	Assignments
AK365 Windows 365 Boot Windows Update Policy Boot	ConfigurationProfile	Windows	1
Andy Kemp 365 Boot Windows 365 Boot Windows Update Policy Boot	ConfigurationProfile	Windows	1
Cloud Kerberos	ConfigurationProfile	Windows	1
Enable FIDO2 Login	ConfigurationProfile	Windows	1
PAW Device Restrictions	ConfigurationProfile	Windows	2
Updates	ConfigurationProfile	Windows	1

OAuth2 Permission Grants

Delegated and application permission grants to third-party applications. Each grant is rated for risk based on the scopes granted. High-risk grants include write access to directory, mail, or files. Admin-consented grants apply organisation-wide and should be reviewed for least-privilege compliance. During migration, grants must be re-consented in the target tenant — use this as an opportunity to right-size permissions.

15 grants total — 6 high-risk — 1 medium-risk

High-Risk Grants

Risk	Application	Resource	Consent	Risky Scopes	Reason
HIGH	SharePoint Online Web Client Extensibility	Microsoft Graph	Admin consent	Files.ReadWrite.All	Grants write/admin access: Files.ReadWrite.All. Review whether this application requires these permissions.
HIGH	SharePoint Online Web Client Extensibility	Office 365 SharePoint Online	Admin consent	Files.ReadWrite.All, Sites.FullControl.All	Grants write/admin access: Files.ReadWrite.All, Sites.FullControl.All. Review whether this application requires these permissions.
HIGH	SharePoint Online Web Client Extensibility	Graph Connector Service	Admin consent	Sites.FullControl.All	Grants write/admin access: Sites.FullControl.All. Review whether this application requires these permissions.

Risk	Application	Resource	Consent	Risky Scopes	Reason
HIGH	Microsoft Graph Command Line Tools	Microsoft Graph	Admin consent	User.ReadWrite.All, Directory.AccessAsUser.All, Group.ReadWrite.All, Directory.ReadWrite.All, Application.ReadWrite.All, RoleManagement.ReadWrite.Directory, Sites.FullControl.All, AppRoleAssignment.ReadWrite.All	Grants write/admin access: User.ReadWrite.All, Directory.AccessAsUser.All, Group.ReadWrite.All, Directory.ReadWrite.All, Application.ReadWrite.All, RoleManagement.ReadWrite.Directory, Sites.FullControl.All, AppRoleAssignment.ReadWrite.All. Review whether this application requires these permissions.
HIGH	Graph Explorer	Microsoft Graph	Admin consent	Directory.ReadWrite.All	Grants write/admin access: Directory.ReadWrite.All. Review whether this application requires these permissions.
HIGH	Azure Logic Apps - Azure AD	Microsoft Graph	Admin consent	Group.ReadWrite.All, User.ReadWrite.All	Grants write/admin access: Group.ReadWrite.All, User.ReadWrite.All. Review whether this application requires these permissions.

All Grants

Application	Resource	Consent	Risk	Scope
SharePoint Online Web Client Extensibility	Microsoft Graph	Admin consent	HIGH	SensitivityLabel.Read TeamsTab.Create AppCatalog.Read.All AppCatalog.Submit C...
SharePoint Online Web Client Extensibility	Office 365 SharePoint Online	Admin consent	HIGH	Files.ReadWrite.All TermStore.ReadWrite.All Sites.ReadWrite.All Sites.FullCon...
SharePoint Online Web Client Extensibility	Office 365 Exchange Online	Admin consent	LOW	Calendars.Read User.Read User.ReadBasic.All
SharePoint Online Web Client Extensibility	Dataverse	Admin consent	LOW	user_impersonation
SharePoint Online Web Client Extensibility	Microsoft Forms	Admin consent	LOW	Forms.ReadWrite
SharePoint Online Web Client Extensibility	Power BI Service	Admin consent	LOW	MLModel.Execute.All Report.Read.All UserState.ReadWrite.All Dataset.Read.All
SharePoint Online Web Client Extensibility	PowerApps Service	Admin consent	LOW	user_impersonation
SharePoint Online Web Client Extensibility	Graph Connector Service	Admin consent	HIGH	Sites.FullControl.All ExternalConnection.ReadWrite.All
Microsoft Graph Command Line Tools	Microsoft Graph	Admin consent	HIGH	User.Read Device.ReadWrite.All openid profile offline_access DeviceManagement...
Graph Explorer	Microsoft Graph	Admin consent	HIGH	openid profile User.Read offline_access Directory.ReadWrite.All Policy.Read....
AndyKempDev-SCEP	Microsoft Graph	Admin consent	LOW	User.Read
Migration Manager	Microsoft Graph	Admin consent	LOW	User.Read
TAPManager	Microsoft Graph	Admin consent	LOW	User.Read
Azure Logic Apps - Azure AD	Microsoft Graph	Admin consent	HIGH	Group.ReadWrite.All User.ReadWrite.All offline_access
AKD-MFA-Upload-Portal	Microsoft Graph	Admin consent	MEDIUM	User.Read openid profile offline_access

Cross-Tenant Access Policies

Cross-tenant collaboration policies govern inbound and outbound access between this tenant and partner organisations. Automatic redemption settings affect the guest user experience. Review inbound trust settings to ensure external organisations are not granted excessive trust.

Policy	Type	Inbound Trust	Auto Redeem
Default Cross-Tenant Policy	Default	None	
a00420fd-aec3-4f80-9296-ee3f64ee6c2d	Partner	None	

Security Defaults

Microsoft Security Defaults provide a baseline set of identity security mechanisms at no extra cost. They enforce MFA registration, block legacy authentication, and protect privileged actions. Security Defaults are recommended for organisations without Conditional Access. If Conditional Access is in use, Security Defaults should typically be disabled to avoid conflicts.

Name	Enabled	Description
Security Defaults	No	Security defaults is a set of basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity related attacks.

Named Locations

IP-based and country-based named locations used in Conditional Access policies. Trusted locations bypass certain controls (e.g., MFA) — ensure only verified corporate IP ranges are marked as trusted. Review country-based locations for accuracy against the organisation's operational footprint.

Name	Type	Trusted	Details
home	ipNamedLocation	Yes	

Authentication Method Policies

Authentication method policies control which sign-in methods are available to users. Methods are classified by strength: phishing-resistant (FIDO2, Windows Hello for Business), strong (Microsoft Authenticator, software OATH), and weak (SMS, voice call). Organisations should prioritise enabling phishing-resistant methods and disabling weak methods.

38% of users have MFA registered (5 of 13). 8 users have no MFA method registered. 1 user has phishing-resistant methods (FIDO2/WHfB). Weak authentication methods are still enabled at the tenant level: Sms.

Method	State	Strength
Fido2	enabled	Phishing-Resistant
Microsoft Authenticator	enabled	Strong
Sms	enabled	Weak
Temporary Access Pass	enabled	Strong
Software Oath	disabled	Strong
Voice	disabled	Weak
Email	disabled	Weak
X509 Certificate	disabled	Strong
Q R Code Pin	disabled	Strong

Users Without MFA

8 user(s) have no MFA method registered. These accounts are vulnerable to password-based attacks.

User	MFA Registered	Passwordless	Default Method
Andy Kemp	No		—
Clint Barton	No		—
Equio1	No		—
Nick Fury	No		—

User	MFA Registered	Passwordless	Default Method
Pete Mitchell	No		—
Room1	No		—
Steve Rogers	No		—
Tony Stark	No		—

Directory & Group Settings

Directory-level settings governing group creation, naming policies, and expiration. Self-service group creation should be restricted to prevent sprawl. Naming policies enforce consistency and make groups easier to manage at scale.

Setting Group	Setting	Value
Password Rule Settings	BannedPasswordCheckOnPremisesMode	Enforce
Password Rule Settings	EnableBannedPasswordCheckOnPremises	True
Password Rule Settings	EnableBannedPasswordCheck	True
Password Rule Settings	LockoutDurationInSeconds	60
Password Rule Settings	LockoutThreshold	10
Password Rule Settings	BannedPasswordList	Pa55w0rd1234% K3yb04rd1234# Kemponline1234%

Identity Protection: Risky Users

Users flagged by Microsoft Entra ID Identity Protection based on sign-in anomalies, leaked credentials, or suspicious activity. High-risk users should have their credentials reset immediately and sessions revoked. Medium-risk users should be investigated and may require MFA re-registration. Unresolved risks indicate gaps in the incident response process.

0 high, 0 medium, 0 low

User	Risk Level	Risk State	Detail	Last Updated
Andrew Kemp	none	dismissed	none	20/12/2024
	none	dismissed	none	16/02/2025

Recommended Actions

Prioritised actions derived from the assessment findings. Actions are categorised by urgency (Immediate, Pre-Migration, Security Improvements, Post-Migration) and rated by severity. Each action identifies the affected objects, business justification, recommended remediation, and migration impact.

9 actions: 1 critical, 4 high, 4 medium, 0 low

Immediate Actions

CRITICAL

Enforce MFA registration for all users

Affected: 8 object(s) | Risk: Security Risk
Reason: 8 users have no MFA registered. Accounts without MFA are vulnerable to credential-based attacks.
Action: Deploy a Conditional Access policy requiring MFA registration and enforce during next sign-in.
Migration Impact: MFA state must be re-established post-migration. Address before migration to establish baseline.

HIGH

Rotate expired application credentials

Affected: 4 object(s) | Risk: Operational Risk
Reason: 4 application credential(s) have expired. Applications using these credentials will fail authentication.
Action: Rotate expired secrets/certificates immediately. Implement a credential management lifecycle process.
Migration Impact: Expired credentials indicate apps that may already be broken. Verify before migration.

Pre-Migration Actions

HIGH

Plan AD Connect decommission or reconfiguration

Affected: 5 object(s) | Risk: Migration Risk
Reason: Active Directory Connect sync is enabled with 5 synced objects. Hybrid identity adds significant migration complexity.
Action: Plan AD Connect cutover: stop sync, convert objects to cloud-only, validate UPN matching in target tenant.
Migration Impact: Critical path item. Synced objects cannot be migrated without AD Connect decommission planning.

MEDIUM

Review disabled Conditional Access policies

Affected: 2 object(s) | Risk: Governance Risk
Reason: 2 disabled CA policies contain MFA or block controls. These may have been intentionally or accidentally disabled.
Action: Review each disabled policy, determine whether to re-enable, update, or remove before migration.
Migration Impact: Disabled policies will not be migrated. Decide on intended state before cutover.

MEDIUM

Review and disable stale user accounts

Affected: 3 object(s) | Risk: Security Risk
Reason: 3 accounts have not signed in for 90+ days. Stale accounts increase attack surface and licensing cost.
Action: Disable or remove stale accounts. Exclude from migration scope to reduce cost and complexity.
Migration Impact: Migrating stale accounts wastes effort and licensing. Clean up before migration.

MEDIUM

Rotate application credentials expiring within 30 days

Affected: 5 object(s) | Risk: Operational Risk
Reason: 5 credential(s) expire within 30 days. Rotate before migration to avoid service disruption.
Action: Renew certificates and secrets before migration window.
Migration Impact: Credentials that expire during migration will cause app outages.

MEDIUM

Recreate named locations and CA dependencies in target tenant

Affected: 1 object(s) | Risk: Migration Risk
Reason: 1 named locations are configured and referenced by Conditional Access policies.
Action: Document all named locations (IP ranges, countries). Recreate in target tenant before CA policy deployment.
Migration Impact: Named locations are not migrated. CA policies referencing them will fail without recreation.

Security Improvements

HIGH

Enable Privileged Identity Management (PIM)

Affected: 8 object(s) | Risk: Security Risk
Reason: No PIM-eligible assignments detected. All privileged access is permanently active, creating a standing attack surface that violates least-privilege and zero-trust principles.
Action: Enable Entra ID PIM for all privileged roles. Convert permanent assignments to time-limited eligible access with approval workflows and phishing-resistant MFA gating.
Migration Impact: Establishing PIM governance before migration ensures clean access controls carry into the target tenant.

HIGH

Review high-risk OAuth permission grants

Affected: 6 object(s) | Risk: Security Risk
Reason: 6 OAuth grant(s) have high-risk permissions (e.g., Directory.ReadWrite.All, Mail.Send). These grants allow broad tenant access.
Action: Review each grant for business necessity. Revoke unnecessary permissions and apply least-privilege scoping.
Migration Impact: OAuth grants must be re-consented in target tenant. Use this as an opportunity to right-size permissions.

Action Summary Table

Severity	Action	Category	Risk Type	Affected
CRITICAL	Enforce MFA registration for all users	Immediate Actions	Security Risk	8
HIGH	Enable Privileged Identity Management (PIM)	Security Improvements	Security Risk	8
HIGH	Rotate expired application credentials	Immediate Actions	Operational Risk	4
HIGH	Review high-risk OAuth permission grants	Security Improvements	Security Risk	6
HIGH	Plan AD Connect decommission or reconfiguration	Pre-Migration Actions	Migration Risk	5
MEDIUM	Review disabled Conditional Access policies	Pre-Migration Actions	Governance Risk	2
MEDIUM	Review and disable stale user accounts	Pre-Migration Actions	Security Risk	3
MEDIUM	Rotate application credentials expiring within 30 days	Pre-Migration Actions	Operational Risk	5
MEDIUM	Recreate named locations and CA dependencies in target tenant	Pre-Migration Actions	Migration Risk	1

Appendix A: Mailbox Delegate Permissions

Mailbox delegate permissions grouped by mailbox. Each entry shows the delegate and the permissions they hold on that mailbox.

Equio1 (Equio1@andykemp.dev)

Delegate	Permissions
Peter Parker (Peter.Parker@andykemp.dev)	SendOnBehalf
Bruce Banner (Bruce.Banner@andykemp.dev)	SendOnBehalf

Han Solo (Han.Solo@andykemp.dev)

Delegate	Permissions
Bruce Banner (Bruce.Banner@andykemp.dev)	SendOnBehalf

Room1 (Room1@andykemp.dev)

Delegate	Permissions
Bruce Banner (Bruce.Banner@andykemp.dev)	SendOnBehalf

Appendix B: OneDrive Permissions (User by User)

Detailed OneDrive sharing relationships grouped by owner to show exactly what content is shared, who it is shared with, and whether access is internal, external, or anonymous.

admin@andykempdev.onmicrosoft.com

Item	Type	Shared With	Scope
Meetings	Folder	Link/unspecified	internal
Recordings	Folder	Link/unspecified	internal

Han.Solo@andykemp.dev

Item	Type	Shared With	Scope
Meetings	Folder	Link/unspecified	internal
Recordings	Folder	Link/unspecified	internal

Peter.Parker@andykemp.dev

Item	Type	Shared With	Scope
ben vane	Folder	Link/unspecified	internal
DLA	Folder	Link/unspecified	internal
Meetings	Folder	Link/unspecified	internal
Recordings	Folder	Link/unspecified	internal

Errors During Audit

Issues encountered during the audit that may have affected data completeness. Errors typically occur when the audit application lacks the required API permissions or when the tenant has restricted access to certain Graph API endpoints. Missing data should be noted when interpreting the findings above.

Module	Error
inboxRules	Expect simple name=value query, but observe property 'assignedLicenses' of complex type 'AssignedLicense'.
mailboxForwarding	Expect simple name=value query, but observe property 'assignedLicenses' of complex type 'AssignedLicense'.

SAMPLE ENTERPRISE REPORT

Deep insight across your Microsoft 365 tenant

Identity & Access

Users, roles, groups and privileged access analysed

Security & Risk

Configuration, controls and exposure assessed

Configuration & Governance

Settings, policies and architectural alignment reviewed

Clarity & Action

Structured findings with prioritised recommendations you can use

Most Microsoft 365 tenants don't lack tools...

They lack visibility

Privileged access is unclear

Permissions grow over time

"Temporary" access becomes permanent

This is where risk starts to build and where this audit uncovers the **real picture.**

Get clarity on your Microsoft 365 tenant

A detailed audit gives you the visibility to:

- **Understand risk**
- **Simplify access**
- **Prepare for change**

If you don’t have a clear view today, that’s usually the **first risk.**

Get in touch to **run an audit**

audit.andykemp.com