

Security Assessment Report

Generated by ARGOS Cloud Security



Table of Contents

Executive Summary.....	3
Overview	3
Key Findings and Critical Vulnerabilities	3
Roadmap	4
Conclusion	4
Secure Score.....	5
Global Administrators	5
Security Compliance	5
Compliance Heatmap.....	5
Environment Scoring.....	6
Detections by Score	7
Detection Summary by Cloud Service Type	7
Actionable Security Recommendations	16
Quick Wins - Immediate Actions.....	18
Detailed Technical Findings	20
Appendix	37
Resource Overview by Type.....	38
How we Score Findings	39
Control Definitions.....	39



Executive Summary

Overview

Through our assessment of the Entra ID environment, we identified overall strengths in cloud identity administration as well as several opportunities to strengthen security controls. The primary security themes observed include gaps in application ownership and identity governance, discoveries of potentially privileged user paths that can escalate to administrator-level permissions, and inconsistently enforced Conditional Access Policies. While no resources were found to be exposed to the internet, there remains a need to address potential attack paths and continue refining the organization's monitoring and patch management processes. Taken together, these observations indicate moderate maturity with room for clear, high-impact improvements.

Key Findings and Critical Vulnerabilities

- **Lack of Entra ID Application Ownership:** Some applications were discovered without a designated owner, which may lead to unmaintained or unmonitored apps, increasing the risk of unauthorized access or neglected security updates.
- **Privileged Role Escalation Paths:** Multiple attack paths were identified in which standard user accounts could gain significant privileges through direct role assignments, service principals with privileged roles, or group owner privilege escalation. These scenarios raise the risk of widespread compromise if any user account on that path is breached.
- **Conditional Access Policy Gaps:** Certain user accounts and high-risk sign-ins were not consistently protected by Conditional Access, allowing potential unauthorized or unsafe access. Additional controls such as blocking high-risk sign-ins or requiring multi-factor authentication were not fully enforced in all cases.
- **Inconsistent Patch Management:** Critical updates for operating systems and applications are not universally applied within recommended time frames, posing an increased risk of vulnerabilities being exploited.
- **Centralized Logging and Review:** While logging is partially in place, there is room to strengthen central monitoring of Entra ID and critical events such as multi-factor authentication prompts, ensuring timely alerting and investigation of anomalies.
- **No publicly accessible resources:** Our scan did not reveal any internet-exposed assets, which positively reduces immediate risks of direct intrusion.



Roadmap

- **Immediate (Next 1-2 Weeks)**
 - Implement or tighten Conditional Access Policies to ensure high-risk sign-ins are fully blocked or require stronger authentication methods.
 - Designate clear ownership for critical Entra ID applications, ensuring that an accountable individual reviews security settings and update cycles.
- **Next 3 Months**
 - Conduct a comprehensive review of privileged roles and attack paths, removing any unnecessary direct assignments to privileged roles. Harden service principals with privileged permissions.
 - Establish a more rigorous patch management process to ensure all systems and applications receive timely updates, especially those managed through Intune.
 - Enhance logging mechanisms to include all Entra ID and multifactor authentication events in a centralized monitoring solution.
- **Next 6 Months**
 - Roll out advanced Conditional Access policies to cover more complex scenarios, including device compliance checks and geolocation factors.
 - Expand the scope of automated remediation where possible, such as prompting users for identity verification when anomalous sign-ins occur.
 - Institute regular access reviews and recertifications for elevated roles to continuously validate the necessity of privileged access.
- **12 Months**
 - Adopt ongoing application modernization, phasing out legacy authentication and implementing the latest phishing-resistant multifactor solutions.
 - Formalize identity lifecycle management processes so that new, updated, or retired applications undergo strict security baseline checks under assigned ownership.
 - Leverage continuous security assessments and pen-testing, ensuring your cloud identity environment remains aligned with evolving best practices and regulatory mandates.

Conclusion

Based on the findings, the environment demonstrates a moderate level of maturity. Although there were no resources exposed to the internet, the presence of multiple high-severity items - particularly in the areas of conditional access and privileged role assignments - indicates that focused improvements are warranted. By addressing these key areas and following the recommended roadmap, the organization can significantly strengthen its cloud security posture and reduce the risk of unauthorized access across Entra ID services. Proactive monitoring, consistent patching, and rigorous identity governance will elevate the overall security maturity and help safeguard critical workloads and data.



Secure Score

This Entra ID environment has a secure score of **35%**.

The secure score is a measure of the security posture of your Entra ID environment as reported by [Microsoft Entra ID](https://argos-security.io), with a higher score indicating better security practices. While this assessment generally goes beyond the findings contributing to the secure score, it is a good measure of the security posture of your Entra ID environment.

Global Administrators

This table lists all the user names of the global administrators in the scanned Entra ID environments.

admin@argosdev.onmicrosoft.com
david_argos-security.io#EXT#@argosdev.onmicrosoft.com
EntraGoat-admin-s1@argosdev.onmicrosoft.com
EntraGoat-admin-s2@argosdev.onmicrosoft.com
EntraGoat-admin-s3@argosdev.onmicrosoft.com
EntraGoat-admin-s5@argosdev.onmicrosoft.com

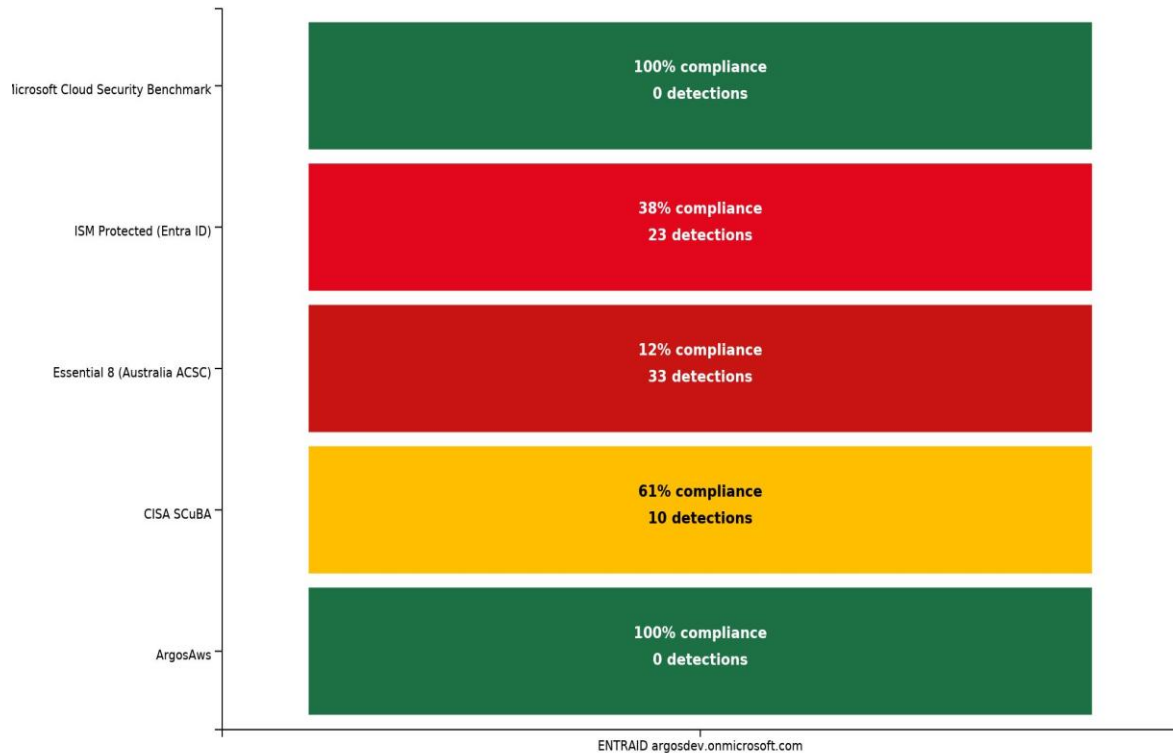
We detected too many users with the Global Administrator role. Please also search for the finding "Number of Global Administrators should be limited".

Security Compliance

Compliance Heatmap

This heatmap gives an overview of the assessed environment's compliance with the appropriate frameworks.





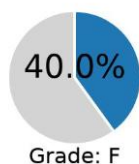
Environment Scoring

The environment scoring is calculated based on the number of findings for each control within a cloud service type. Each control contributes to the total score as follows:

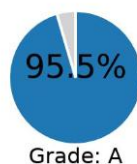
- If a control has 0 findings, it adds 10 points.
- If a control has fewer than 5 findings, it adds 5 points.
- If a control has 5 or more findings, it adds 0 points.

The final score is the percentage of the total possible points (sum of all scores per service type multiplied by 10), and a grade is assigned based on this score.

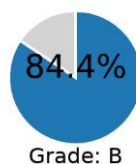
**Defender
Threat
Intelligence**



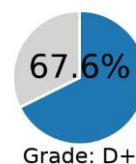
**Entra ID User
Access**



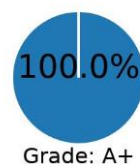
**Entra ID
Authentication**

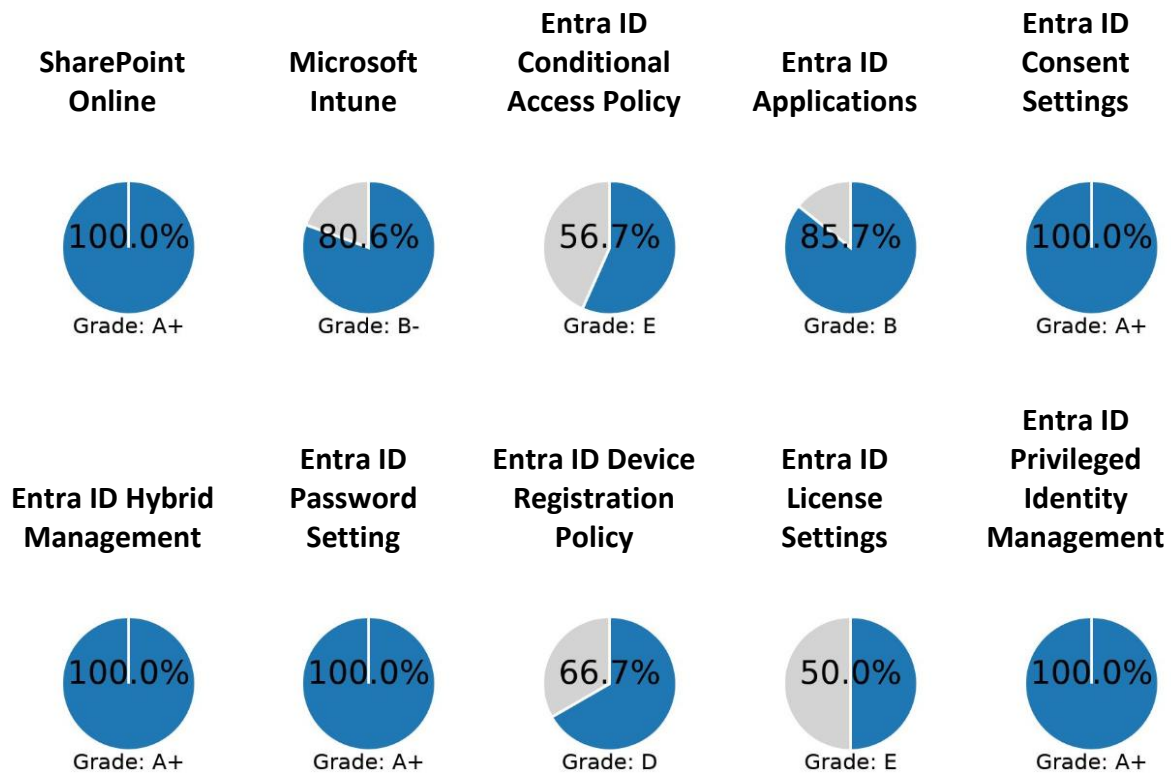


**Entra ID
Authorization
Policy**



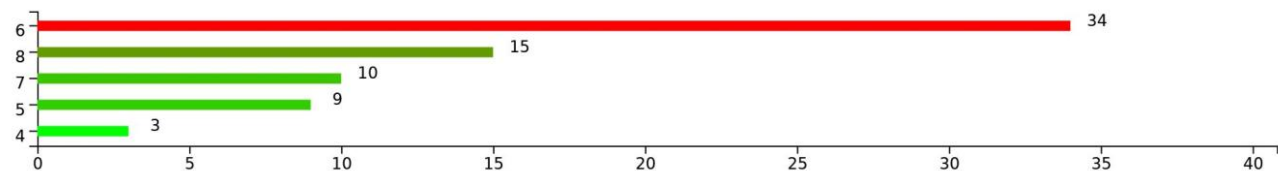
**Microsoft
Teams**





Detections by Score

The number of detections (x-axis) per score (y-axis) in the assessed cloud environments.



Detection Summary by Cloud Service Type

This table lists all the controls applied to the scanned cloud environments. For detailed information about each control, please refer to the controls definitions section in the appendix of this report.

Defender Threat Intelligence

Control Name	Detections Count
Patch non-Office applications within 30 days	1
Attack Path: Group owner privilege escalation	1

Control Name	Detections Count
Attack Path: User has direct privileged role assignment	6
Attack Path: User owns Service Principal with privileged role	2
Vulnerability scanning at least fortnightly	1

Entra ID User Access

Control Name	Detections Count
Privileged access auto-expires within 12 months	0
Shared Accounts Controlled	0
Administrators should have dedicated admin accounts	0
Global Administrators should be cloud only	0
User activation of the highly privileged role SHALL trigger an alert.	0
Eligible and Active highly privileged role assignments SHALL trigger an alert	0
Permanent active role assignments SHALL NOT be allowed for highly privileged roles	0
Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system	0
Use Granular Roles (Least Privilege)	0
Disable inactive privileged accounts after 45 days	0
Activation of the Global Administrator role SHALL require approval	0
Number of Global Administrators should be limited	0
Regular privileged access reviews and re-certification	1
Contractors Identified as Such	0

Entra ID Authentication



Control Name	Detections Count
Show application name in push and passwordless notifications	0
Microsoft Authenticator allows for use of OTP	0
Microsoft Authenticator Authentication Method enabled	0
Microsoft Authenticator Authentication Method enabled	0
Require number matching for push notifications	0
Excluded users/groups of number matching for push notifications	0
Included users/groups of number matching for push notifications	0
Admin group changes are centrally logged	0
Admin logons are centrally logged	0
Phishing-resistant MFA required	1
MFA events centrally logged	1
Checks if weak Entra Id Authentication Methods are disabled	0
Enforce MFA registration for user	18
Reporting suspicious activity allowed for all users	0
Authentication Methods Migration Complete	0
Check Authentication Methods policy for Microsoft Authenticator is set appropriately	0
Reporting suspicious activity allowed	1

Entra ID Authorization Policy

Control Name	Detections Count
Restrict 3rd party app consent to admins	0
User consent policy for Entra Applications	0
Centralized logging and monitoring of Entra ID and M365 activities	1



Control Name	Detections Count
Restrict creation of Entra ID Application	1
An admin consent workflow SHALL be configured for applications	0
Block Creation of Entra ID Application Secrets	1
Block access to MSOL PowerShell legacy endpoint	1
Limit guest user access to tenant	0
Restrict non-admin users from creating tenants	1
Restrict who can invite guests to Entra ID	1
Guest invites should only be allowed to specific external domains that have been authorized for legitimate business purposes.	1
User can join the tenant by email validation	1
Sign-up for email based subscription	1
Restrict creation of M365 Groups	0
Restrict creation of Entra ID Security Groups	1
Restrict creation of Entra ID Tenants	1
Self-service password reset should be enabled	0

Microsoft Teams

Control Name	Detections Count
Is Teams Chat Resource-Specific Consent Enabled	0
Is Teams user Resource-Specific Consent Enabled	0

SharePoint Online

Control Name	Detections Count
External sharing for SharePoint and OneDrive SHALL be limited to Existing guests or Only People in your organization	0



Control Name	Detections Count
External sharing SHALL be restricted to approved external domains and/or users in approved security groups per collaboration needs.	0

Microsoft Intune

Control Name	Detections Count
ASR: Block PSEXEC and WMI Lateral Movement	0
Credential Guard Enabled	0
Unique Passwords for Local Admin Accounts	0
ASR: Block Credential Theft (LSASS)	0
ASR: Block Executable Content in Email	0
ASR: Block Obfuscated Scripts	0
ASR: Block JavaScript/VBScript Launching EXEs	0
ASR: Block Untrusted Executables (Prevalence-Based)	0
ASR: Block Persistence via WMI Events	0
LSA Protection Enabled	0
Memory Integrity (HVCI) Enabled	0
Intune - Application Control (Application Allow Listing)	0
Office macros blocked from Win32 API calls	0
Intune - Patch Applications	1
Intune - Patch Operating Systems	1
Office applications cannot create executables	0
ASR rule – Office cannot inject code	0
Office applications cannot spawn child processes	0
Microsoft recommended blocklist in place	1



Control Name	Detections Count
ASR: Block Office Communication Apps Creating Processes	0
ASR: Block Untrusted USB Processes	0
Command-line process creation logging enabled	0
Edge / Chrome hardening per ASD & vendor baseline	0
PowerShell logging enabled	0
Intune - Regular Backups	1
ASR rule – PDF reader cannot spawn child processes	1
WDAC not deployed to internet-facing servers	1
Intune - Configure Microsoft Office Macro Settings	0
Intune - User Application Hardening	0
Internet Explorer 11 Disabled	0
.NET Framework 3.5 Disabled	0
Office OLE Package Activation Blocked	0
Windows PowerShell 2.0 Disabled	0
Intune - Built-in device compliance policy should mark devices without compliance policy as 'Not compliant'.	0
Intune - Ensure device clean-up rule is configured.	1

Entra ID Conditional Access Policy

Control Name	Detections Count
Block High Risk Sign-Ins in Entra ID Conditional Access Policies	1
Block High Risk User in Entra ID Conditional Access Policies	1
Conditional Access Policy - Block Access to M365 Office unless compliant	1



Control Name	Detections Count
User detected that is excluded from Conditional Access Policy	1
Protect Enterprise Copilot Platform (Microsoft 365 Copilot) using Entra ID Conditional Access Policies	1
Protect Microsoft Security Copilot Platform using Entra ID Conditional Access Policies	1
Trusted Location should be configured in Conditional Access Policies	1
Block Device Code Flow in Entra ID Conditional Access Policies	1
Block Legacy Authentication in Entra ID Conditional Access Policies	0
Managed devices SHOULD be required for authentication	1
Managed devices SHOULD be required for MFA registration	1
Ensure Conditional Access Policy requiring MFA is enabled	1
Phishing-resistant MFA shall be enforced for all users	1
Phishing-resistant MFA shall be enforced for all highly privileged roles	1
Block High Risk User in Entra ID Conditional Access Policies	0

Entra ID Applications

Control Name	Detections Count
Entra ID Application has dangerously extensive permissions	0
Entra ID Graph CLI Service Principal should not have permanent permissions consented to	1
Entra ID Service Principal has dangerously extensive permissions	0
Entra ID Application redirects to insecure URI	0
Entra ID Application has no Owner configured	3
Entra ID Application uses password credentials	0
Entra ID Application has expired secret	0



Entra ID Consent Settings

Control Name	Detections Count
Block User Consent for Risky Applications	0
Ensure only Admins can consent to 3rd party applications	0
Prevent Non-Admin User Consent to Third-Party Apps	0

Entra ID Hybrid Management

Control Name	Detections Count
Entra ID Connect Synchronisation is unhealthy	0
Entra ID Synchronization Check	0

Entra ID Password Setting

Control Name	Detections Count
Activate Banned Password Enforcement	0
Smart Lockout - Lockout duration in seconds	0
Smart Lockout - Lockout threshold	0
Manage Banned Password Check Modes	0
Configure custom banned list	0
Enable Banned Password Check for On-Premises Active Directory	0
User passwords SHALL NOT expire	0

Entra ID Device Registration Policy

Control Name	Detections Count
Global Administrators are added to Device Local Administrators Group	0
Registering User is added to Device Local Administrators Group	1



Control Name	Detections Count
User should not be allowed to join device to Entra ID	1

Entra ID License Settings

Control Name	Detections Count
Entra ID Premium P2 licenses should be purchased.	1

Entra ID Privileged Identity Management

Control Name	Detections Count
Entra ID Privileged Identity Management should be used.	0



Actionable Security Recommendations

This section focuses on turning numerous detections into a few strategic actions. Rather than addressing each finding individually, these recommendations target root causes that resolve multiple security issues simultaneously.

Priority Actions - Turn 71 Detections into 5 Strategic Actions

1. Eliminate direct privileged roles and enforce least privilege CRITICAL

What this addresses: Users have direct or ownership-based privileged role assignments, increasing the risk of privilege escalation. Consolidate roles under just-in-time and least-privilege models to prevent unauthorized elevation.

Impact: Permission issue • Risk Score: 9/10

Estimated Effort: 2 Weeks

Action Steps:

- 1. Review all direct role assignments in Entra ID to confirm actual business requirements**
Technical details: Use Entra ID roles and administrators interface or PowerShell (AzureAD and MSGraph modules) to list direct privileged assignments
- 2. Remove direct privileged role assignments where possible and implement Entra ID Privileged Identity Management (PIM) for just-in-time access**
Technical details: Deploy PIM to manage high-privilege roles, set up approval workflow
- 3. Mandate MFA for all privileged role activations**
Technical details: Configure Conditional Access policies in Entra ID for PIM activation

2. Disable group-based privilege escalation CRITICAL

What this addresses: Owners of certain groups can escalate privileges, creating a lateral attack path. Remove privileged roles from group owners and apply just-in-time or approval-based access to mitigate threats.

Impact: Permission issue • Risk Score: 8/10

Estimated Effort: 1 Week

Action Steps:

- 1. Inventory group owners who have privileged roles in Entra ID**
Technical details: Use Graph API or Entra ID portal to list group owners and their roles



2. **Remove or reduce privileged roles for group owners and leverage PIM for temporary escalation only when necessary**
Technical details: Implement role assignment policies in Entra ID and enforce just-in-time assignment
3. **Continuously monitor group membership using Entra ID access reviews**
Technical details: Schedule access reviews for groups with potential privileged access

3. Implement robust patch management MEDIUM

What this addresses: Unpatched operating systems and applications expose the environment to exploitable vulnerabilities. Enforcing organization-wide patch compliance via Intune and vulnerability management policies reduces security risk.

Impact: Policy issue • Risk Score: 7/10

Estimated Effort: 3 Weeks

Action Steps:

1. **Configure Intune policies to enforce both OS and application patching across all devices**
Technical details: Enable quality and feature updates and configure patch schedules in Intune policy
2. **Enable automatic updates for critical third-party applications**
Technical details: Utilize third-party patch catalogs in Intune or integrated solutions like WSUS/Endpoint Manager
3. **Leverage compliance reports and threat intelligence to verify patch status and prioritize urgent updates**
Technical details: Use Intune reporting and threat feeds to correlate high-risk vulnerabilities

4. Ensure no user is excluded from Conditional Access HIGH

What this addresses: A user excluded from critical Conditional Access policies weakens defenses against credential theft and brute-force attacks. Enforce consistent policy application to all accounts.

Impact: Policy issue • Risk Score: 7/10

Estimated Effort: Hours

Action Steps:

1. **Audit existing Conditional Access policies to identify any explicitly excluded users**
Technical details: Check Entra ID Conditional Access policy filters in the Entra ID portal



2. **Remove unnecessary user exclusions and require MFA enrollment for all accounts**
Technical details: Update policy scope in Entra ID to include all users/groups and enforce MFA
3. **Maintain a break-glass or emergency access account with strict monitoring if needed**
Technical details: Document usage procedures, enable alerting for sign-ins

5. Remove permanent permissions from Graph CLI service principal HIGH

What this addresses: A service principal with longstanding, high-level Graph permissions poses a significant risk if that principal is compromised. Restrict or remove these permissions and implement a just-in-time model.

Impact: Permission issue • Risk Score: 7/10



Estimated Effort: Days


Action Steps:

1. **Review permanent permissions granted to the Microsoft Graph Command Line Tools service principal and revoke unnecessary consents**
Technical details: Use Graph API or Entra ID portal to list applicable OAuth2PermissionGrants and remove them
2. **Implement just-in-time or scoped delegation for required Graph permissions**
Technical details: Utilize Entra ID PIM or app role assignments that expire after a set time
3. **Regularly monitor service principal consent grants via Entra ID logs**
Technical details: Enable audit logging and review changes in OAuth2PermissionGrant objects

Quick Wins - Immediate Actions

These actions can be completed quickly but provide significant security improvements:

Action	Description	Attack Paths Prevented	Detections Addressed
  HIGH: Strengthen Identity & Access Controls	IMMEDIATE ACTIONS: Enforce MFA for 3 privileged accounts using Conditional Access policies. Enable Privileged Identity Management for 9 high-privilege roles. Conduct access review for all administrative roles and remove inactive assignments. ATTACK PATHS PREVENTED:	3	24

Action	Description	Attack Paths Prevented	Detections Addressed
	Lateral movement via overprivileged access; Credential compromise → account takeover; Initial access → admin privilege escalation.		
 MEDIUM: Enable Security Monitoring & Alerting	IMMEDIATE ACTIONS: . ATTACK PATHS PREVENTED: Attack activity → undetected persistence.	1	1

Detailed Technical Findings

Note: This section provides detailed technical information for each finding. For strategic guidance, refer to the Actionable Security Recommendations section above.

Resource Name: admin

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [admin](#)

Detection	Score
1. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq '4e361fd4-3aa6-4628-b35d-45d8c2926edd'"	



Resource Name: amanda.thompson@argosdev.onmicrosoft.com

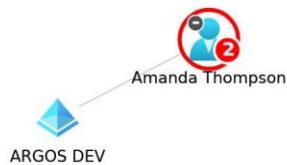
Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [amanda.thompson@argosdev.onmicrosoft.com](#)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: User owns Service Principal with privileged role	8
Command to fix: Connect-MgGraph -Scopes 'Application.ReadWrite.All','User.ReadWrite.All'; # Review service principal ownership: Get-MgServicePrincipal -Filter "displayName eq ''" Get-MgServicePrincipalOwner	





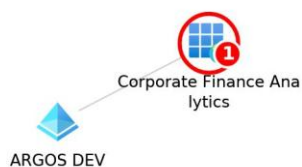
Resource Name: Corporate Finance Analytics

Cloud Service Type: microsoft.graph.application

Publicly Exposed: No

Link to ARGOS dashboard: [Corporate Finance Analytics](#)

Detection	Score
1. Entra ID Application has no Owner configured	6



Resource Name: David Martinez

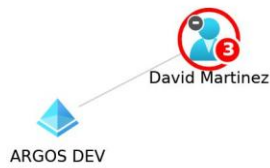
Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [David Martinez](#)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. User detected that is excluded from Conditional Access Policy	8
Command to fix: Connect-MgGraph -Scopes 'User.ReadWrite.All'; Update-MgUser -UserId 34c3ed5c-5468-4fcc-83bb-975d1cef7e76 -AccountEnabled \$false	
3. Attack Path: User owns Service Principal with privileged role	8
Command to fix: Connect-MgGraph -Scopes 'Application.ReadWrite.All','User.ReadWrite.All'; # Review service principal ownership: Get-MgServicePrincipal -Filter "displayName eq ''" Get-MgServicePrincipalOwner	





Resource Name: David O'Brien

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [David O'Brien](#)

Detection	Score
1. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq '2088f8a2-903d-4361-b45f-42f5d2b74ff8'"	



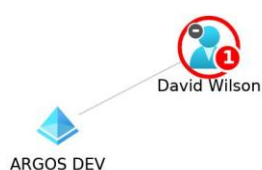
Resource Name: david.wilson@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [david.wilson@argosdev.onmicrosoft.com](#)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



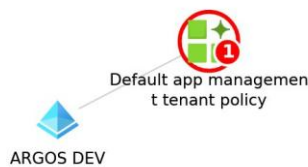
Resource Name: Default app management tenant policy

Cloud Service Type: microsoft.graph.appmanagementpolicy

Publicly Exposed: No

Link to ARGOS dashboard: [Default app management tenant policy](#)

Detection	Score
1. Block Creation of Entra ID Application Secrets	6
Command to fix: Connect-MgGraph -Scopes 'Application.ReadWrite.All'; Remove-MgApplicationPassword -ApplicationId 00000000-0000-0000-0000-000000000000 -KeyId 00000000-0000-0000-0000-000000000000	



Resource Name: ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c

Cloud Service Type: microsoft.graph.security.vulnerabilities

Publicly Exposed: No

Link to ARGOS dashboard: [ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c](#)

Detection	Score
1. Reporting suspicious activity allowed	4
2. Entra ID Premium P2 licenses should be purchased.	4
3. Intune - Ensure device clean-up rule is configured.	4
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
4. Sign-up for email based subscription	5
5. Restrict creation of Entra ID Tenants	5
6. Ensure Conditional Access Policy requiring MFA is enabled	5
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Detection	Score
7. Phishing-resistant MFA shall be enforced for all highly privileged roles	5
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
8. Managed devices SHOULD be required for authentication	5
9. Restrict creation of Entra ID Security Groups	5
10. Phishing-resistant MFA shall be enforced for all users	5
Command to fix: Connect-MgGraph -Scopes 'User.ReadWrite.All'; Update-MgUser -UserId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c -AccountEnabled \$false	
11. User can join the tenant by email validation	5
Command to fix: Connect-MgGraph -Scopes 'User.ReadWrite.All'; Update-MgUser -UserId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c -AccountEnabled \$false	
12. Managed devices SHOULD be required for MFA registration	5
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
13. Protect Microsoft Security Copilot Platform using Entra ID Conditional Access Policies	6
14. Registering User is added to Device Local Administrators Group	6
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; Remove-MgDirectoryRoleMemberByRef -DirectoryRoleId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c -DirectoryObjectId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c	
15. Block access to MSOL PowerShell legacy endpoint	6
16. Restrict non-admin users from creating tenants	6
17. Guest invites should only be allowed to specific external domains that have been authorized for legitimate business purposes.	6
18. Block Device Code Flow in Entra ID Conditional Access Policies	6
19. Trusted Location should be configured in Conditional Access Policies	6



Detection	Score
20. Protect Enterprise Copilot Platform (Microsoft 365 Copilot) using Entra ID Conditional Access Policies	6
21. User should not be allowed to join device to Entra ID	6
Command to fix: Connect-MgGraph -Scopes 'User.ReadWrite.All'; Update-MgUser -UserId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c -AccountEnabled \$false	
22. Regular privileged access reviews and re-certification	6
Command to fix: Connect-MgGraph -Scopes 'User.ReadWrite.All'; Update-MgUser -UserId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c -AccountEnabled \$false	
23. MFA events centrally logged	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
24. Restrict who can invite guests to Entra ID	6
25. Phishing-resistant MFA required	7
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
26. Restrict creation of Entra ID Application	7
27. ASR rule – PDF reader cannot spawn child processes	7
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
28. Conditional Access Policy - Block Access to M365 Office unless compliant	7
29. Block High Risk User in Entra ID Conditional Access Policies	7
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Block High Risk Users' -State 'enabled' -Conditions @{UserRiskLevels='high'} -GrantControls @{BuiltInControls='block'}	
30. Block High Risk Sign-Ins in Entra ID Conditional Access Policies	7

Detection	Score
31. Intune - Regular Backups	7
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
32. Centralized logging and monitoring of Entra ID and M365 activities	7
33. Vulnerability scanning at least fortnightly	7
Command to fix: Connect-MgGraph -Scopes 'Directory.Read.All'; Get-MgOrganization	
34. WDAC not deployed to internet-facing servers	7
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
35. Patch non-Office applications within 30 days	8
Command to fix: Connect-MgGraph -Scopes 'Application.ReadWrite.All'; Get-MgApplication -ApplicationId ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c-vulnerabilityscanningsummary	
36. Intune - Patch Applications	8
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
37. Intune - Patch Operating Systems	8
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	
38. Microsoft recommended blocklist in place	8
Command to fix: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementDeviceConfiguration -DisplayName 'Security Baseline'	



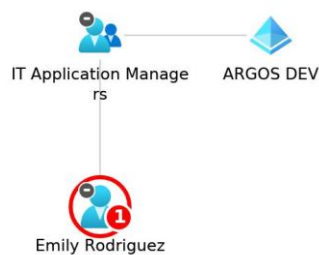
Resource Name: emily.rodriguez@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [emily.rodriguez@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: EntraGoat-admin-s1@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [EntraGoat-admin-s1@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq '71debf0b-62af-455e-b7fd-13d36508f62f'"	





Resource Name: EntraGoat-admin-s2@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [EntraGoat-admin-s2@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com/EntraGoat-admin-s2)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq '552ed831-17f4-4ed7-8274-6c821fbb8f90'"	



Resource Name: EntraGoat-admin-s3@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [EntraGoat-admin-s3@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com/EntraGoat-admin-s3)

Detection	Score
1. Enforce MFA registration for user	6

Detection	Score
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq 'd80809dd-c5f6-47b7-b492-ba2b7c650d44'"	



Resource Name: EntraGoat-admin-s5@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [EntraGoat-admin-s5@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com/EntraGoat-admin-s5)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: User has direct privileged role assignment	8
Command to fix: Connect-MgGraph -Scopes 'RoleManagement.ReadWrite.Directory'; # Review user role assignments: Get-MgRoleManagementDirectoryRoleAssignment -Filter "principalId eq '0e91b742-b4f6-404a-a9f6-5a785a6741f4'"	





Resource Name: Finance Analytics Dashboard

Cloud Service Type: microsoft.graph.application

Publicly Exposed: No

Link to ARGOS dashboard: [Finance Analytics Dashboard](#)

Detection	Score
1. Entra ID Application has no Owner configured	6



Resource Name: goat@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [goat@argosdev.onmicrosoft.com](#)

Detection	Score
1. Enforce MFA registration for user	6

Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}



Resource Name: Identity Management Portal

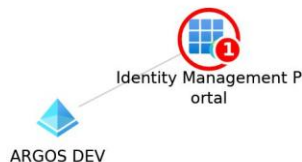


Cloud Service Type: microsoft.graph.application

Publicly Exposed: No

Link to ARGOS dashboard: [Identity Management Portal](#)

Detection	Score
1. Entra ID Application has no Owner configured	6



Resource Name: james.wilson@argosdev.onmicrosoft.com

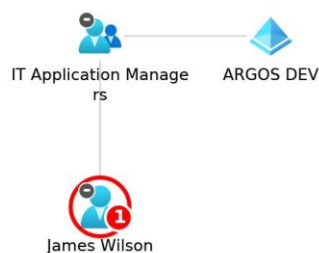
Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [james.wilson@argosdev.onmicrosoft.com](#)

Detection	Score
1. Enforce MFA registration for user	6

Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}



Resource Name: jennifer.clark@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

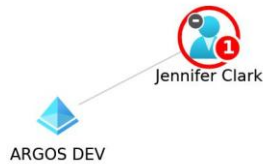
Link to ARGOS dashboard: [jennifer.clark@argosdev.onmicrosoft.com](#)

Detection	Score
1. Enforce MFA registration for user	6

Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State



Detection	Score
'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: jessica.chen@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: jessica.chen@argosdev.onmicrosoft.com

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: lisa.chang@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: lisa.chang@argosdev.onmicrosoft.com

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	





Resource Name: lisa.park@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [lisa.park@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: michael.chen@argosdev.onmicrosoft.com

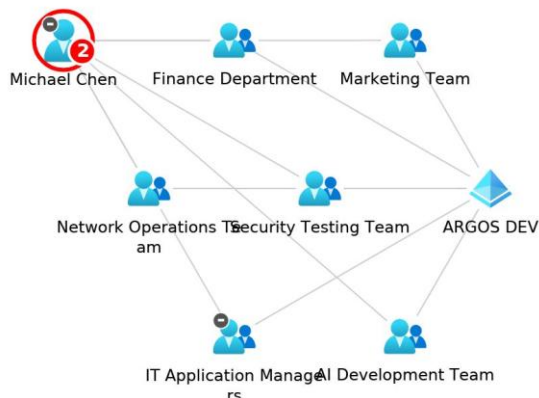
Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [michael.chen@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	
2. Attack Path: Group owner privilege escalation	8

Detection	Score
Command to fix: Connect-MgGraph -Scopes 'Group.ReadWrite.All','RoleManagement.ReadWrite.Directory'; # Review group ownership: Get-MgGroup -Filter "displayName eq ''" Get-MgGroupOwner	



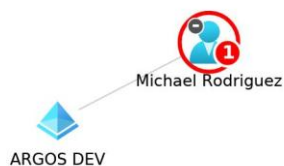
Resource Name: michael.rodriguez@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: michael.rodriguez@argosdev.onmicrosoft.com

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: Microsoft Graph Command Line Tools

Cloud Service Type: microsoft.graph.serviceprincipal

Publicly Exposed: No

Link to ARGOS dashboard: [Microsoft Graph Command Line Tools](#)

Detection	Score
1. Entra ID Graph CLI Service Principal should not have permanent permissions consented to	8



Detection	Score
Command to fix: Connect-MgGraph -Scopes 'Application.ReadWrite.All'; Remove-MgApplicationPermission -ApplicationId cc0eb53d-8ddf-4cde-8741-7b7b01528f02 -PermissionId cc0eb53d-8ddf-4cde-8741-7b7b01528f02	

Error message: exception has occurred. Contact support please. Resource with ID: cc0eb53d-8ddf-4cde-8741-7b7b01528f02 Error details: Inventory graph with entry point cc0eb53d-8ddf-4cde-8741-7b7b01528f02 is missing a root node.

Resource Name: robert.taylor@argosdev.onmicrosoft.com

Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [robert.taylor@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	



Resource Name: sarah.connor@argosdev.onmicrosoft.com

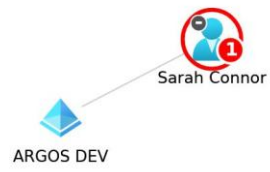
Cloud Service Type: microsoft.graph.user

Publicly Exposed: No

Link to ARGOS dashboard: [sarah.connor@argosdev.onmicrosoft.com](https://argosdev.onmicrosoft.com)

Detection	Score
1. Enforce MFA registration for user	6
Command to fix: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Require MFA for all users' -State 'enabled' -Conditions @{Users=@{IncludeUsers='All'}} -GrantControls @{BuiltInControls='mfa'}	





Appendix

This report is not meant to serve as a replacement for a compliance audit, although it can serve to prepare you for it. In addition, the outcomes of this assessment can be used as input for an action plan to mitigate the discovered findings, enhancing your organization's security posture.

The following cloud environments were scanned:

Environment Name	Environment ID
ARGOS DEV	ef9a30f7-48cf-4b5b-8d40-dfbd97f9d80c



Resource Overview by Type

This table lists the number of resources found in the scanned cloud environments, grouped by resource type.

Type	Count
microsoft.graph.directoryrole	124
microsoft.graph.serviceprincipal	81
microsoft.graph.securescore	40
microsoft.graph.user	21
microsoft.graph.oauth2permissiongrant	9
microsoft.graph.group	7
microsoft.graph.application	5
microsoft.graph.conditionalaccesspolicy	4
microsoft.aadiam.domains	1
microsoft.graph.adminconsentrequestpolicy	1
microsoft.graph.auditlogs.directoryaudits	1
microsoft.graph.auditlogs.signins	1
microsoft.graph.authenticationpolicy	1
microsoft.graph.authorizationpolicy	1
microsoft.graph.crosstenantaccesspolicy	1
microsoft.graph.deviceregistrationpolicy	1
microsoft.graph.fido2authenticationmethodconfiguration	1
microsoft.graph.tenantsettings	1
microsoft.graph.intune.windowsdefenderapplicationcontrolpolicies	1
microsoft.graph.security.vulnerabilities	1
microsoft.graph.subscribedsku	1

Type	Count
microsoft.graph.tenantappmanagementpolicy	1

How we Score Findings

Findings are scored 1-4 (information/compliance), 5-7 (important), and 8-10 (critical).

Scores mentioned below are the default scores for each control. The actual score can deviate from this depending on factors like public exposure.

Control Definitions

Defender Threat Intelligence

1. Patch non-Office applications within 30 days

Ensure Application patches applied within 30 days

Cloud Service Type: Threat Intelligence

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Vulnerability Management

Description: Security patches for non-Office applications are applied within 30 days of their release through Microsoft Defender Vulnerability Management. Requires Microsoft Defender for Endpoint Plan 2 licensing (included in Microsoft 365 E5 or standalone Microsoft Defender for Endpoint P2).

Rationale: This control verifies that security patches for non-Office applications are applied within 30 days of release. Microsoft Defender Vulnerability Management should track patch deployment status and identify unpatched vulnerabilities older than 30 days. Organizations should configure automated patch deployment through Windows Update, Microsoft Intune, or WSUS to ensure timely patching of security vulnerabilities. This requires an active Microsoft Defender for Endpoint Plan 2 license to access vulnerability management APIs.

Impact: How to fix: Enable automatic updates for applications through Microsoft Intune or Windows Update for Business. Configure deployment rings to ensure patches are tested and deployed within 30 days. Use Microsoft Defender Vulnerability Management to track patch deployment status and identify systems requiring urgent patching.

Help Link: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eighthttps://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb>

2. Attack Path: Group owner privilege escalation

Low-privileged user owns security groups with administrative roles enabling privilege escalation



Cloud Service Type: Threat Intelligence

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Essential 8 (Australia ACSC) - Application Control

Description: A low-privileged user owns security groups that have administrative roles assigned, enabling privilege escalation through group membership manipulation and service principal compromise.

Rationale: This attack path identifies complex privilege escalation scenarios where attackers can chain multiple identity relationships to achieve admin privileges. The attack begins with a low-privileged user (e.g., IT support) who owns multiple security groups. Since group ownership provides full control over group membership, the attacker can add themselves to groups with administrative roles like Application Administrator. This role allows management of all service principals in the tenant, including adding credentials. The attacker can then discover service principals that are members of groups with highly privileged roles like Privileged Authentication Administrator, add credentials to those service principals, authenticate as them, and ultimately reset Global Administrator passwords. This multi-hop attack chain exploits legitimate but misconfigured permission relationships.

Tactics and techniques: [Initial Access Persistence Defense Evasion Privilege Escalation](#)

Impact: This attack path enables sophisticated privilege escalation from low-privileged users to Global Administrator through multiple intermediate steps. It represents a complex but realistic threat where legitimate identity relationships are chained together to achieve unauthorized administrative access and complete tenant compromise.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/groups-assign-role><https://learn.microsoft.com/en-us/entra/fundamentals/groups-settings-v2><https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-identity-management/>

3. Attack Path: User has direct privileged role assignment

Regular user has direct assignment to highly privileged administrative roles

Cloud Service Type: Threat Intelligence

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: A regular user account has been directly assigned to highly privileged roles such as Global Administrator or Privileged Authentication Administrator, creating immediate compromise risk if the account is breached.

Rationale: This attack path identifies the simplest but most critical privilege escalation scenario where regular user accounts have direct assignments to highly privileged roles. When attackers compromise such accounts through phishing, credential stuffing, or other methods, they immediately gain administrative privileges without needing additional escalation steps. Roles like Privileged Authentication Administrator can reset any user's password including Global Administrators, while Global Administrator provides complete



tenant control. This represents a fundamental violation of the principle of least privilege and creates single points of failure for entire tenant security.

Tactics and techniques: [Initial Access Persistence Defense Evasion Privilege Escalation](#)

Impact: This attack path creates immediate and complete tenant compromise risk. If any of these privileged user accounts are compromised, attackers gain instant administrative control over the entire Entra ID tenant and connected resources without requiring additional privilege escalation techniques.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access><https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices><https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-identity-management/>

4. Attack Path: User owns Service Principal with privileged role

User owns a Service Principal that has privileged administrative roles

Cloud Service Type: Threat Intelligence

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Control

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: A user has been found to own a service principal that has privileged roles such as Privileged Authentication Administrator, which can be exploited to escalate privileges and compromise Global Administrator accounts.

Rationale: This attack path identifies scenarios where compromised user credentials can lead to full tenant compromise through service principal exploitation. The attack flow begins when an attacker compromises a user account (e.g., through stolen credentials). If that user owns a service principal with privileged roles like Privileged Authentication Administrator, the attacker can add client secrets to the service principal and authenticate as it. Using the privileged role, the attacker can then reset Global Administrator passwords or add Temporary Access Passes (TAP) to bypass MFA, achieving complete tenant compromise. This represents a critical vulnerability in identity governance where service principal ownership lacks proper oversight.

Tactics and techniques: [Initial Access Persistence Defense Evasion Privilege Escalation](#)

Impact: This attack path can lead to complete tenant compromise. Attackers can escalate from a compromised user account to Global Administrator privileges by exploiting service principal ownership. This enables password resets, MFA bypass, and full administrative control over the Entra ID tenant and connected resources.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview><https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-identity-management/><https://learn.microsoft.com/en-us/entra/architecture/service-accounts-principal>

5. Vulnerability scanning at least fortnightly

Ensure Vulnerability scanning at least fortnightly



Cloud Service Type: Threat Intelligence

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Vulnerability Management

Description: Vulnerability scans are conducted at least fortnightly (every 14 days) for non-Office applications through Microsoft Defender Vulnerability Management. Requires Microsoft Defender for Endpoint Plan 2 licensing (included in Microsoft 365 E5 or standalone Microsoft Defender for Endpoint P2).

Rationale: This control verifies that vulnerability scans are conducted at least fortnightly for non-Office applications. Microsoft Defender Vulnerability Management should be configured to automatically scan devices for vulnerabilities every 14 days or less. This helps identify security weaknesses before they can be exploited by threat actors. The rule checks for recent vulnerability assessment activity and ensures scanning is enabled and functioning properly. This requires an active Microsoft Defender for Endpoint Plan 2 license to access vulnerability management capabilities.

Impact: How to fix: Enable Microsoft Defender Vulnerability Management in Microsoft 365 Defender. Navigate to Settings > Endpoints > Advanced features > Microsoft Defender Vulnerability Management. Configure automated scanning schedules and ensure all endpoints are enrolled in Defender for Endpoint with vulnerability assessment enabled. Verify that vulnerability scans are occurring at least every 14 days.

Help Link: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management> <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight>

Entra ID User Access

1. Privileged access auto-expires within 12 months

Ensure Privileged access auto-expires ≤ 12 months

Cloud Service Type: Entra Id User Access

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: This rule verifies that all privileged role assignments are configured to automatically expire within 12 months using Privileged Identity Management (PIM).

Rationale: Essential 8 Maturity Level 2 requires that privileged access assignments automatically expire within 12 months to prevent accumulation of dormant privileged accounts. This control checks Entra ID Privileged Identity Management for role assignments with permanent duration or expiration dates exceeding 12 months. Regular expiration ensures ongoing review and justification of privileged access.

Impact: How to fix: Enable Privileged Identity Management (PIM) in Entra ID Premium P2. Convert permanent role assignments to eligible assignments with maximum 12-month duration. Configure role settings to require justification and approval for activation. Regularly review and renew role assignments before expiration.



Help Link:<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/https://docs.microsoft.com/en-us/graph/api/resources/privilegedidentitymanagement-directory>

2. Shared Accounts Controlled

Shared User Accounts Controlled

Cloud Service Type: Entra Id User Access

Score: 8

Compliance controls:

ISM Protected (Entra ID) - ISM-0415

Description: The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.

Rationale: This is a manual control that requires verification that the organization has implemented policies and procedures to strictly control the use of shared user accounts. Personnel using shared accounts must be uniquely identifiable through logging, authentication mechanisms, or other accountability measures.

Impact: Ensures accountability and traceability for all user actions by eliminating anonymous access through shared accounts and maintaining audit trails.

Help Link:<https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ismhttps://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

3. Administrators should have dedicated admin accounts

Ensure privileged users have separate Entra ID accounts used only for admin duties

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

ISM Protected (Entra ID) - ISM-0445

ISM Protected (Entra ID) - ISM-1175

Description: Administrators have separate Entra ID accounts used only for admin duties (no email or daily use), and these accounts are limited to the necessary roles.

Rationale: This rule identifies privileged role members who have any licenses assigned, indicating they may be used for regular user activities. Dedicated admin accounts should have no licenses assigned to ensure complete isolation from email and web access. The rule checks privileged roles by their role template IDs and validates that members have completely empty assignedLicenses arrays (no Office 365, EMS, or other licenses).

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: Administrators will need to maintain separate accounts for administrative and regular user activities, which may require additional training and processes.

Help Link:<https://docs.microsoft.com/en-us/azure/active-directory/roles/security-planninghttps://docs.microsoft.com/en-us/azure/active-directory/roles/best-practices>



4. Global Administrators should be cloud only

Ensure Global Administrators are cloud only accounts

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.3v1

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: Privileged users SHALL be provisioned cloud-only accounts separate from an on-premises directory or other federated identity providers.

Rationale: By provisioning cloud-only Entra ID user accounts to privileged users, the risks associated with a compromise of on-premises federation infrastructure are reduced. It is more challenging for the adversary to pivot from the compromised environment to the cloud with privileged access.

Tactics and techniques: [Credential Access](#)

Help Link: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#9-use-cloud-native-accounts-for-microsoft-entra-roles><https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad73v1>

5. User activation of the highly privileged role SHALL trigger an alert.

User activation of the highly privileged role SHALL trigger an alert.

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.8v1

CISA SCuBA - MS.AAD.7.9v1

Description: Closely monitor activation of the highly privileged roles for signs of compromise. Send activation alerts to enable the security monitoring team to detect compromise attempts.

Rationale: This requires Entra ID P2 or Governance licence.

Tactics and techniques: [Persistence](#)

Impact: The following roles are considered highly privileged according to CISA: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator, Exchange Administrator, Hybrid Identity Administrator, Application Administrator, Cloud Application Administrator

Help

Link: <https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad78v1><https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad79v1>https://entra.microsoft.com/#view/Microsoft_Azure_PIMC/Common/ResourceMenuBlade/~/_roles/resourceId//resourceType/tenant/provider/aadrolehttps://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-add-role-to-user



6. Eligible and Active highly privileged role assignments SHALL trigger an alert

Eligible and Active highly privileged role assignments SHALL trigger an alert

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.7v1

Description: Closely monitor assignment of the highest privileged roles for signs of compromise. Send assignment alerts to enable the security monitoring team to detect compromise attempts.

Rationale: This requires Entra ID P2 or Governance licence.

Tactics and techniques: [Persistence](#)

Impact: The following roles are considered highly privileged according to CISA: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator, Exchange Administrator, Hybrid Identity Administrator, Application Administrator, Cloud Application Administrator

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad77v1>https://entra.microsoft.com/#view/Microsoft_Azure_PIMCommon/ResourceMenuBlade/~/_roles/resourceId//resourceType/tenant/provider/aadroles

7. Permanent active role assignments SHALL NOT be allowed for highly privileged roles

Permanent active role assignments SHALL NOT be allowed for highly privileged roles

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.4v1

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: Instead of giving users permanent assignments to privileged roles, provisioning access just in time lessens exposure if those accounts become compromised. In Entra ID PIM or an alternative PAM system, just in time access can be provisioned by assigning users to roles as eligible instead of perpetually active.

Rationale: Note: Exceptions to this policy are:\n\n- Emergency access accounts that need perpetual access to the tenant in the rare event of system degradation or other scenarios.\n- Some types of service accounts that require a user account with privileged roles; since these accounts are used by software programs, they cannot perform role activation.

Tactics and techniques: [Persistence](#)

Impact: The following roles are considered highly privileged according to CISA: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator, Exchange Administrator, Hybrid Identity Administrator, Application Administrator, Cloud Application Administrator



Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad74v1>

8. Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system

Provisioning users to highly privileged roles SHALL NOT occur outside of a PAM system

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.5v1

Description: Provisioning users to privileged roles within a PAM system enables enforcement of numerous privileged access policies and monitoring. If privileged users are assigned directly to roles in the M365 admin center or via PowerShell outside of the context of a PAM system, a significant set of critical security capabilities are bypassed.

Rationale: This requires Entra ID P2 or Governance licence.

Impact: The following roles are considered highly privileged according to CISA: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator, Exchange Administrator, Hybrid Identity Administrator, Application Administrator, Cloud Application Administrator

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad75v1>https://entra.microsoft.com/#view/Microsoft_Azure_PIMCommon/ResourceMenuBlade/~/_roles/resourceId//resourceType/tenant/provider/aadroles

9. Use Granular Roles (Least Privilege)

Use Granular Roles Instead of Global Administrator

Cloud Service Type: Entra Id User Access

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.7.2v1

Description: Privileged users SHALL be assigned finer-grained roles instead of Global Admin

Rationale: This is a manual control that requires verification that privileged users are assigned specific, least-privilege roles rather than broad Global Administrator roles.

Impact: Reduces the risk of excessive permissions and ensures users have only the minimum access required for their role.

Help Link:<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

10. Disable inactive privileged accounts after 45 days

Ensure privileged accounts that have not been used for 45+ days are disabled

Cloud Service Type: Entra Id User Access

Score: 6



Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges
ISM Protected (Entra ID) - ISM-1648

Description: Automatically disable privileged accounts that have not been used within 45 days to reduce security risk.

Rationale: Inactive privileged accounts pose a security risk as they may be forgotten and not properly managed. This rule checks privileged role assignments (identified by role template IDs) and validates user sign-in activity through Entra ID sign-in logs to identify accounts with no authentication activity for 45+ days, then verifies if such accounts remain enabled (AccountEnabled=true).

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: Privileged accounts that are not regularly used will be disabled, requiring re-activation when needed.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>
<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

11. Activation of the Global Administrator role SHALL require approval**Activation of the Global Administrator role SHALL require approval**

Cloud Service Type: Entra Id User Access

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.7.6v1

Description: Requiring approval for a user to activate Global Administrator, which provides unfettered access, makes it more challenging for an attacker to compromise the tenant with stolen credentials and it provides visibility of activities indicating a compromise is taking place.

Rationale: This requires Entra ID P2 or Governance licence.

Tactics and techniques: [Persistence](#)

Help

Link: https://entra.microsoft.com/#view/Microsoft_Azure_PIMCommon/ResourceMenuBlade/~/_roles/resourceld//resourceType/tenant/provider/aadroleshttps://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad76v1

12. Number of Global Administrators should be limited**Limit Global Administrator Numbers for Enhanced Security**

Cloud Service Type: Entra Id User Access

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.7.1v1

Description: A minimum of two users and a maximum of eight users SHALL be provisioned with the Global Administrator role.



Rationale: The Global Administrator role provides unfettered access to the tenant. Limiting the number of users with this level of access makes tenant compromise more challenging. Microsoft recommends fewer than five users in the Global Administrator role. However, additional user accounts, up to eight, may be necessary to support emergency access and some operational scenarios.

Tactics and techniques: [Persistence](#)

Impact: Limiting the number of Global Administrators to a small, manageable number minimizes the risk of security breaches and unauthorized access. Fewer administrators mean fewer targets for potential attacks and fewer chances for insider threats. This policy is critical for maintaining secure and controlled management of the organization's resources, reducing the likelihood of a compromised administrator account leading to a wide-scale security incident.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#5-limit-the-number-of-global-administrators-to-less-than-5>
<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad71v1>

13. Regular privileged access reviews and re-certification

Ensure periodic review and revalidation of admin access rights (manual)

Cloud Service Type: Entra Id User Access

Score: 6

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

ISM Protected (Entra ID) - ISM-1507

ISM Protected (Entra ID) - ISM-1647

Description: Periodically review and revalidate admin access rights; remove or expire those no longer needed.

Rationale: Regular access reviews ensure that privileged access is only granted to users who still need it, reducing the risk of excessive or outdated permissions. This rule validates Entra ID Access Reviews configuration for privileged roles, checking if access review campaigns are configured with appropriate frequency (quarterly or better), include privileged role assignments, and have active review cycles with proper reviewer assignments.

Tactics and techniques: [Persistence](#)

Impact: Access reviews require administrative overhead to conduct periodic reviews and may result in access being removed for users who no longer need it.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>
<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>

14. Contractors Identified as Such

Personnel Who Are Contractors Are Identified

Cloud Service Type: Entra Id User Access

Score: 6



Compliance controls:

ISM Protected (Entra ID) - ISM-1583

Description: Personnel who are contractors are identified as such.

Rationale: This is a manual control that requires verification that the organization has implemented policies and procedures to clearly identify contractor personnel within user accounts, directory services, and access management systems. This may include naming conventions, account attributes, group memberships, or other identification mechanisms.

Impact: Enables proper access control, audit trails, and security monitoring by clearly distinguishing contractor access from permanent employee access.

Help Link: <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ismhttps://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>

Entra ID Authentication**1. Show application name in push and passwordless notifications**

Ensure application name is displayed in push and passwordless notifications

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: Determines whether the user's Authenticator app will show them the client app they are signing into.

Tactics and techniques: [Credential Access](#)

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade~/AdminAuthMethodshhttps://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-additional-context

2. Microsoft Authenticator allows for use of OTP

Ensure Microsoft Authenticator allows use of OTP

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: Defines if users can use the OTP code generated by the Authenticator App.

Rationale: Immediate Action: Enable OTP generation in Microsoft Authenticator authentication methods policy. Use PowerShell: Connect-MgGraph -Scopes 'Policy.ReadWrite.AuthenticationMethod'; Update-

MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration -

AuthenticationMethodId 'MicrosoftAuthenticator' to enable software OATH token

generation. Platform Policy: Implement Microsoft Security Baseline for Entra ID that

includes Microsoft Authenticator OTP configuration. Use Conditional Access policies to



require stronger authentication methods based on risk levels. Holistic Approach: Establish multi-layered authentication strategy with Microsoft Authenticator OTP as backup to primary passwordless methods, implement risk-based authentication with Entra ID Identity Protection, establish emergency access procedures with OTP codes, and provide user training on secure OTP usage. Consider transitioning to passwordless authentication with Microsoft Authenticator as the primary authentication method.

Tactics and techniques: [Credential Access](#)

Impact: Enabling OTP generation in Microsoft Authenticator strengthens security protocols by ensuring that user identity verification involves something the user knows (their password) and something the user has (their mobile device generating the OTP). This significantly reduces the risk of unauthorized access, even if a user's password is compromised, thereby protecting sensitive data and systems from potential security breaches.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_AdminAuthMethods<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-authenticator-app>

3. Microsoft Authenticator Authentication Method enabled

Ensure Microsoft Authenticator Authentication Method is enabled

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: This rule requires the activation of the Microsoft Authenticator app as a method of authentication. Microsoft Authenticator provides a second layer of security through two-factor authentication (2FA), using notifications, codes, or biometric verifications to verify user identity.

Rationale: Microsoft Authenticator adds a crucial layer of security by enabling two-factor authentication, which requires users to provide a second form of identification beyond just a password. This can include a code from the app, a phone notification, or a biometric check. It's particularly effective against phishing and credential theft, as the second factor would still be needed to gain access, even if the user's password is compromised.

Tactics and techniques: [Credential Access](#)

Impact: Enabling Microsoft Authenticator enhances security by significantly reducing the risk of unauthorized access. It protects against common threats such as phishing and credential stuffing by ensuring that possession of a password alone is not enough to access sensitive resources. This measure supports compliance with security best practices and regulatory requirements that mandate strong authentication mechanisms.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_AdminAuthMethods<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-authenticator-app>

4. Microsoft Authenticator Authentication Method enabled



Ensure Microsoft Authenticator Authentication Method is enabled

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: Require number matching for push notifications

Tactics and techniques: [Credential Access](#)

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade~/AdminAuthMethodshttps://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-authenticator-app

5. Require number matching for push notifications

Ensure number matching for push notifications is enabled in Authenticator

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: Defines if number matching is required for MFA notifications.

Rationale: This rule mandates that number matching be enabled for MFA push notifications using the Microsoft Authenticator. When this feature is active, the user must enter a number displayed on their sign-in screen into their Authenticator app to approve the sign-in request. This measure is designed to ensure that the user physically has the device and is actively participating in the authentication process, which helps to prevent unauthorized access even if the device itself is compromised.

Tactics and techniques: [Credential Access](#)

Impact: Enabling number matching for push notifications significantly elevates security by adding an interactive layer to the authentication process. This helps thwart attempts at intercepting or automating authentication responses, such as through remote access Trojans or malware. It protects against sophisticated phishing attacks and ensures a higher level of user engagement and verification, thus safeguarding sensitive data and systems more effectively.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade~/AdminAuthMethodshttps://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

6. Excluded users/groups of number matching for push notifications

Ensure no users are excluded from number matching push notifications in Authenticator

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:



ARGOS Entra ID - 3.1

Description: Object Id or scope of users which are excluded from showing number matching in the Authenticator App.

Rationale: This rule checks that no users are excluded from number matching during MFA verification with the Microsoft Authenticator app.

Tactics and techniques: [Credential Access](#)

Impact: Users can't opt out of number matching in Authenticator push notifications. Relevant services will begin deploying this setting after May 8, 2023 and users will start to see number match in approval requests.

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade~/AdminAuthMethodshttps://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

7. Included users/groups of number matching for push notifications

Ensure all users are configured for number matching push notifications in Authenticator

Cloud Service Type: Entra Id Authentication

Score: 8

Compliance controls:

ARGOS Entra ID - 3.1

Description: Object Id or scope of users which will be showing number matching in the Authenticator App.

Rationale: This rule checks that 'all_users' are required to use number matching during MFA verification with the Microsoft Authenticator app. By specifying which accounts must comply with this security feature, the rule ensures that selected users or groups participate in an enhanced verification process, making unauthorized access considerably more difficult.

Tactics and techniques: [Credential Access](#)

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade~/AdminAuthMethodshttps://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match

8. Admin group changes are centrally logged

Ensure administrative group membership changes are properly logged

Cloud Service Type: Entra Id Authentication

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: This rule verifies that changes to administrative group memberships and role assignments are being centrally logged and are available for monitoring and analysis by checking the past 14 days of logs.



Rationale: Centralized logging of administrative group changes is essential for maintaining security oversight of privileged access. This control queries GET /auditLogs/directoryAudits?\$filter=activityDisplayName in ('Add member to role', 'Remove member from role', 'Update user') to check that events exist recently, ensuring that all modifications to administrative privileges are properly tracked.

Impact: Without proper logging of administrative group changes, organizations cannot track modifications to privileged access, potentially missing unauthorized privilege escalations or removals.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs><https://learn.microsoft.com/en-us/graph/api/directoryaudit-list?view=graph-rest-1.0&tabs=http>

9. Admin logons are centrally logged

Ensure administrative logons are properly logged and monitored

Cloud Service Type: Entra Id Authentication

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: This rule verifies that administrative user logons are being centrally logged and are available for monitoring and analysis.

Rationale: Centralized logging of administrative logons is critical for security monitoring and incident response. This control queries GET /auditLogs/signIns?\$filter=roles/any() to verify at least one event per admin in the past 14 days, ensuring that administrative access is properly tracked and auditable.

Impact: Without proper logging of administrative logons, organizations cannot effectively monitor privileged access, detect unauthorized activities, or investigate security incidents involving admin accounts.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins><https://docs.microsoft.com/en-us/graph/api/signin-list>

10. Phishing-resistant MFA required

Ensure MFA is phishing-resistant for online services and system logons

Cloud Service Type: Entra Id Authentication

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: This rule verifies that phishing-resistant MFA methods (FIDO2 or certificate-based authentication) are enforced through conditional access policies and authentication strength policies.

Rationale: Essential 8 Maturity Level 2 requires phishing-resistant MFA for both online services and system logons. This control checks conditional access policies and authentication strength policies for FIDO2 security keys, Windows Hello for Business, or



certificate-based authentication. Phishing-resistant methods prevent attackers from intercepting or replaying authentication factors.

Impact: How to fix: Configure phishing-resistant authentication methods in Entra ID. Deploy FIDO2 security keys or enable Windows Hello for Business. Create authentication strength policies that require phishing-resistant methods and apply them through conditional access policies to all users and applications.

Help Link:<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths><https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eighth><https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2>

11. MFA events centrally logged

Ensure Successful/failed MFA events are centrally logged

Cloud Service Type: Entra Id Authentication

Score: 6

Compliance controls:

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: This rule verifies that both successful and failed MFA authentication events are being centrally logged and are available for monitoring and analysis.

Rationale: Essential 8 Maturity Level 2 requires centralized logging of all MFA events for security monitoring and incident response. This control checks Entra ID sign-in logs of the last 14 days to verify that MFA authentication attempts (both successful and failed) are being recorded and retained. Organizations should integrate these logs with their Security Information and Event Management (SIEM) system for comprehensive monitoring.

Impact: How to fix: Ensure Entra ID audit logging is enabled and configured to retain sign-in logs for the required period. Configure log analytics workspace to collect and analyze Entra ID logs. Set up alerts for suspicious MFA patterns and integrate with your SIEM solution for centralized security monitoring.

Help Link:<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins><https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eighth><https://learn.microsoft.com/en-us/graph/api/signin-list?view=graph-rest-1.0&tabs=http>

12. Checks if weak Entra Id Authentication Methods are disabled

Ensure weak Entra Id Authentication Methods are disabled

Cloud Service Type: Entra Id Authentication

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.3.5v1

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: The authentication methods SMS, Voice Call, and Email One-Time Passcode (OTP) SHALL be disabled.



Rationale: Immediate Action: Disable weak authentication methods in Entra ID. Use PowerShell: Connect-MgGraph -Scopes 'Policy.ReadWrite.AuthenticationMethod'; Update-MgPolicyAuthenticationMethodPolicy to disable SMS, voice call, and email OTP methods. Enable stronger methods like Microsoft Authenticator with number matching. Platform Policy: Implement Microsoft Security Baseline for Entra ID that enforces strong authentication methods. Use Conditional Access policies to require phishing-resistant MFA where possible. Holistic Approach: Establish a phased migration to passwordless authentication using Windows Hello for Business, FIDO2 security keys, and Microsoft Authenticator with passwordless sign-in. Implement risk-based authentication with Entra ID Identity Protection and establish emergency access accounts with strong authentication backup methods.

Tactics and techniques: [Initial Access](#)

Impact: If phishing-resistant MFA has not been deployed yet and Microsoft Authenticator is in use, configure Authenticator to display context information to users when they log in.

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad35v1>

13. Enforce MFA registration for user

Ensure all users are required to register for MFA

Cloud Service Type: Entra Id Authentication

Score: 6

Compliance controls:

Essential 8 (Australia ACSC) - Multi-Factor Authentication (MFA registration enforcement)

ISM Protected (Entra ID) - ISM-1504

ISM Protected (Entra ID) - ISM-1679

ISM Protected (Entra ID) - ISM-1680

Description: All users must have MFA methods configured, and this user was found to not have MFA registered.

Rationale: This control ensures that every user account has MFA methods registered, preventing scenarios where accounts could be compromised without MFA protection. The rule checks if at least one of the following MFA methods are configured for a user: Microsoft Authenticator, Fido2, Software One Time Password (OATH), Windows Hello for Business, Phone/SMS. While a temporary access pass is considered MFA, we do not recommend it as an ongoing MFA, so we exclude it from here.

Tactics and techniques: [Credential Access](#)

Impact: Users will be required to register for MFA before they can access resources, which may require initial setup time.

Help Link:<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-convergedhttps://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

14. Reporting suspicious activity allowed for all users



Ensure suspicious authentication activity can be reported by all users

Cloud Service Type: Entra Id Authentication

Score: 6

Compliance controls:

ARGOS Entra ID - 3.1

Description: Object Id or scope of users which will be included to report suspicious activities if they receive an authentication request that they did not initiate.

Rationale: Apply this feature to all users.

Tactics and techniques: [Credential Access](#)

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_AdminAuthMethods

15. Authentication Methods Migration Complete

Complete Authentication Methods Migration

Cloud Service Type: Entra Id Authentication

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.4v1

Description: The Authentication Methods "Manage Migration" feature SHALL be set to Migration Complete

Rationale: This is a manual control that requires verification that the organization has completed the migration to the new authentication methods management.

Impact: Ensures that authentication methods are properly managed using the latest features and security controls.

Help Link:<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

16. Check Authentication Methods policy for Microsoft Authenticator is set appropriately

Ensure the Authentication Methods policy for Microsoft Authenticator is set appropriately

Cloud Service Type: Entra Id Authentication

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.3v1

Description: If phishing-resistant MFA has not been enforced and Microsoft Authenticator is enabled, it shall be configured to show login context information.

Rationale: Immediate Action: Configure Microsoft Authenticator to show application context and location information. Use PowerShell: Connect-MgGraph -Scopes

'Policy.ReadWrite.AuthenticationMethod'; Update-

MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration for Microsoft Authenticator with showApplicationNameInNotification and

showGeographicalLocationInNotification enabled. Platform Policy: Implement Microsoft



Security Baseline for Entra ID authentication methods with enhanced Authenticator security features. Use Conditional Access to require number matching for high-risk scenarios. Holistic Approach: Transition toward passwordless authentication with Microsoft Authenticator passwordless sign-in, implement Windows Hello for Business for device-bound authentication, use FIDO2 security keys for high-privilege accounts, and establish comprehensive user education program about phishing attacks and secure authentication practices.

Tactics and techniques: [Credential Access](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad33v1>

17. Reporting suspicious activity allowed

Ensure users can report suspicious authentication activity

Cloud Service Type: Entra Id Authentication

Score: 4

Compliance controls:

ARGOS Entra ID - 3.1

Description: Allows to integrate report of fraud attempt by users to identity protection: Users who report an MFA prompt as suspicious are set to High User Risk. Administrators can use risk-based policies to limit access for these users, or enable self-service password reset (SSPR) for users to remediate problems on their own.

Rationale: Allows users to report suspicious activities if they receive an authentication request that they did not initiate. This control is available when using the Microsoft Authenticator app and voice calls. Reporting suspicious activity will set the user's risk to high. If the user is subject to risk-based Conditional Access policies, they may be blocked.

Tactics and techniques: [Credential Access](#)

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/_AdminAuthMethods

Entra ID Authorization Policy

1. Restrict 3rd party app consent to admins

Ensure only administrators can consent to 3rd party applications

Cloud Service Type: Entra Id Authorization Policy

Score: 8

Compliance controls:

CISA SCuBA - MS.AAD.5.2v1

Description: Indicates whether user consent for risky apps is allowed. For example, consent requests for newly registered multi-tenant apps that are not publisher verified and require non-basic permissions are considered risky.



Rationale: This rule restricts user consent to third-party applications considered risky, specifically requiring that only administrators can grant consent. Risky apps typically include those that are newly registered, multi-tenant, not publisher verified, and request non-basic permissions. This policy is designed to mitigate risks associated with unauthorized or unsafe application access to sensitive organizational resources.

Tactics and techniques: [Persistence](#)

Impact: By limiting consent powers to administrators, this rule significantly reduces the risk of malicious or unsafe third-party applications gaining access to critical data and system functions. It helps prevent phishing attacks and unauthorized data access by ensuring that any high-risk application undergoes thorough vetting before being granted the necessary permissions. This approach enhances overall security posture and compliance with best practices in application management.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-consent-requests>https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/_UserSettings<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad52v1>

2. User consent policy for Entra Applications

Ensure user consent policy for Entra Applications is configured

Cloud Service Type: Entra Id Authorization Policy

Score: 8

Compliance controls:

CISA SCuBA - MS.AAD.5.2v1

Description: Microsoft recommends to allow user consent for apps from verified publisher for selected permissions. CISA SCuBA MS.AAD.5.2v1 defines that all Non-Admin Users SHALL Be Prevented From Providing Consent To Third-Party Applications.

Rationale: Defines if user consent to apps is allowed, and if it is, which app consent policy (permissionGrantPolicy) governs the permissions.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: Allowing non-admin users to grant consent to third-party applications increases the risk of unauthorized access and potential data breaches, as malicious apps could gain permissions that compromise user data or organizational resources.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-consent-requests>https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/_UserSettings<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad52v1>

3. Centralized logging and monitoring of Entra ID and M365 activities

Ensure Entra ID sign-in and audit logs are centrally logged and monitored

Cloud Service Type: Entra Id Authorization Policy

Score: 7



Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

ISM Protected (Entra ID) - ISM-1509

ISM Protected (Entra ID) - ISM-1650

ISM Protected (Entra ID) - ISM-1683

Description: Send Entra ID sign-in and audit logs, and M365 audit logs, to a SIEM or Log Analytics for timely analysis.

Rationale: Centralized logging is essential for detecting signs of compromise and suspicious activities. This rule validates Entra ID diagnostic settings configuration to ensure sign-in logs, audit logs, and non-interactive sign-in logs are enabled and forwarded to Log Analytics workspaces, Event Hubs, or Storage Accounts. It also checks Microsoft 365 audit log configuration to ensure unified audit logging is enabled for M365 services.

Tactics and techniques: [Defense Evasion](#)

Impact: Without centralized logging, security teams cannot effectively monitor and respond to security incidents in a timely manner.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor><https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance>

4. Restrict creation of Entra ID Application

Ensure the creation of Entra ID Applications is restricted

Cloud Service Type: Entra Id Authorization Policy

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.5.1v1

Description: CISA SCuBA 2.6: Only Administrators SHALL Be Allowed To Register Third-Party Applications

Rationale: Controls if non-admin users may register custom-developed applications for use within this directory.

Tactics and techniques: [Persistence](#)

Impact: Restricting the ability to register third-party applications solely to administrators helps to significantly enhance security by controlling the proliferation of applications within the organization's environment. This reduces the risk associated with rogue or malicious applications gaining access to sensitive data and system resources. It also mitigates potential phishing attacks and abuses of trusted relationships, as administrators are more likely to scrutinize and validate the legitimacy and safety of applications before registration.

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad51v1>

5. An admin consent workflow SHALL be configured for applications

An admin consent workflow SHALL be configured for applications



Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.5.3v1

Description: Configuring an admin consent workflow reduces the risk of the previous policy by setting up a process for users to securely request access to applications necessary for business purposes. Administrators have the opportunity to review the permissions requested by new applications and approve or deny access based on a risk assessment.

Tactics and techniques: [Persistence](#)

Impact: 1. In Entra create a new Group that contains admin users responsible for reviewing and adjudicating application consent requests. Group members will be notified when users request consent for new applications.\r\n2. Then in Entra under Identity and Applications, select Enterprise applications.\r\n3. Under Security, select Consent and permissions.\r\n4. Under Manage, select Admin consent settings.\r\n5. Under Admin consent requests and Users can request admin consent to apps they are unable to consent to select Yes.\r\n6. Under Who can review admin consent requests, select + Add groups and select the group responsible for reviewing and adjudicating app requests (created in step one above).

Help Link:<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-consent-requests>https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade~/AdminConsentSettings<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad53v1>

6. Block Creation of Entra ID Application Secrets

Ensure Secrets Cannot Be Created for Entra ID Applications

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

Description: Application secrets are long-lived credentials that can be used to authenticate applications. Allowing the creation of application secrets increases the risk of credential theft, misuse, and unauthorized access to cloud resources. This rule ensures that application secrets cannot be created by enforcing tenant-wide application authentication method policies.

Rationale: Blocking the creation of application secrets helps mitigate the risk of credential theft and misuse. Secrets are often stored insecurely or shared improperly, making them a common target for attackers. By enforcing a tenant-wide policy, organizations can ensure that applications use more secure authentication mechanisms, such as certificates or managed identities, which are harder to compromise. Exceptions can be handled by creating specific policies for applications that require Client Secrets.

Tactics and techniques: [Credential Access](#) [Initial Access](#) [Persistence](#) [Defense Evasion](#)

Impact: If this policy is not enforced, attackers may exploit stolen or leaked application secrets to gain unauthorized access to cloud resources. Enforcing this policy reduces the attack surface and strengthens the overall security posture of the tenant by ensuring that only secure authentication methods are used. Additionally, organizations can phase out existing Client Secrets over time while allowing exceptions for specific applications. For



more information check Daniel Bradley's article and the Microsoft documentation in the help links.

Help Link:<https://ourcloudnetwork.com/how-to-block-the-creation-of-client-secrets-on-entra-applications><https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-app-management-policies?tabs=portal#enable-a-restriction-for-all-applications><https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals><https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mgpolicyappmanagementpolicy?view=graph-powershell-1.0>

7. Block access to MSOL PowerShell legacy endpoint

Ensure user-based access to MSOL PowerShell legacy endpoint is blocked

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 5.3

Description: Specifies whether the user-based access to the legacy service endpoint used by MSOL PowerShell is blocked or not. This does not affect Entra ID Connect or Microsoft Graph.

Rationale: Blocking access to the MSOL PowerShell legacy endpoint is essential for preventing the use of outdated authentication methods that lack modern security features like MFA. It ensures administrative tasks are performed through interfaces that uphold current security standards.

Tactics and techniques: [Credential Access](#)

Impact: Permitting access to legacy endpoints increases susceptibility to attacks, compromising security. Blocking access mitigates unauthorized access risks but necessitates updating administrative practices to current standards, potentially disrupting legacy processes.

Help Link:<https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication>

8. Limit guest user access to tenant

Ensure Guest user access is limited.

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.8.1v1

Description: Guest users should have limited or restricted access to Microsoft Entra ID directory objects.

Rationale: This rule specifies that guest users within the Entra ID environment should have restricted access to directory objects, enforcing a principle of least privilege to enhance security.

Tactics and techniques: [Discovery](#)



Impact: Without strict access controls, guest users may inadvertently or maliciously access sensitive information or resources, leading to potential security risks. Implementing this policy helps mitigate unauthorized access and ensures compliance with best practices and regulations.

1. In Entra ID and External Identities, select External collaboration settings.

2. Under Guest user access, select either Guest users have limited access to properties and memberships of directory objects or Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).

Help

Link: https://entra.microsoft.com/#view/Microsoft_AAD_IAM/CompanyRelationshipsMenuBade/~Settings/menuld/Settingshttps://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissionshttps://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/bases/aad.md#msaad81v1

9. Restrict non-admin users from creating tenants

Ensure 'Restrict non-admin users from creating tenants' is set to 'Yes'

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 5.4

Description: Restricting tenant creation prevents unauthorized or uncontrolled deployment of resources and ensures that the organization retains control over its infrastructure. User generation of shadow IT could lead to multiple, disjointed environments that can make it difficult for IT to manage and secure the organization's data, especially if other users in the organization began using these tenants for business purposes under the misunderstanding that they were secured by the organization's security team.

Tactics and techniques: [Credential Access](#)

Impact: Non-admin users will need to contact I.T. if they have a valid reason to create a tenant.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication>

10. Restrict who can invite guests to Entra ID

Ensure only admins and Guest inviters can invite guests.

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.8.2v1

Description: Only users with the Guest Inviter role SHOULD be able to invite guest users

Rationale: Manages controls over who can invite guests to your directory to collaborate on resources secured by your Entra ID, ensuring that only authorized personnel can extend such invitations. Expecting \

Tactics and techniques: [Persistence](#)



Impact: Failing to restrict invitation capabilities increases the risk of unauthorized access and potential data breaches, complicates access management and audit processes, and may lead to non-compliance with data protection regulations. It is crucial for security and compliance to limit guest invitations to admins and designated Guest Inviters.

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad82v1>https://entra.microsoft.com/#view/Microsoft_AAD_IAM/CompanyRelationshipsMenuBlade/~/_/Settings/menuId/Settings<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>

11. Guest invites should only be allowed to specific external domains that have been authorized for legitimate business purposes.

Guest invites should only be allowed to specific external domains that have been authorized for legitimate business purposes.

Cloud Service Type: Entra Id Authorization Policy

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.8.3v1

Description: Limiting which domains can be invited to create guest accounts in the tenant helps reduce the risk of users from unauthorized external organizations getting access.

Rationale: This is different to the way CISA implements this control, but the outcome is similar.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad83v1>https://entra.microsoft.com/#view/Microsoft_AAD_IAM/CompanyRelationshipsMenuBlade/~/_/Settings/menuId/Settings<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>https://entra.microsoft.com/#view/Microsoft_AAD_IAM/InboundAccessSettings.ReactView/isDefault~/true/name//id/

12. User can join the tenant by email validation

Ensure email validated users cannot self join the Entra ID tenant.

Cloud Service Type: Entra Id Authorization Policy

Score: 5

Compliance controls:

ARGOS Entra ID - 5.1

Description: Controls whether users can join the tenant by email validation. To join, the user must have an email address in a domain which matches one of the verified domains in the tenant.

Rationale: This rule governs the self-service tenant joining process, ensuring that only users with email addresses from verified domains can join the tenant. It aims to streamline user access while safeguarding against unauthorized tenant access.



Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: Allowing unrestricted self-join could expose the tenant to unauthorized access, potentially leading to security vulnerabilities. Conversely, too restrictive a policy may hinder collaboration and operational flexibility by limiting access for legitimate users.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup><https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

13. Sign-up for email based subscription

Control email-based self-service sign-up

Cloud Service Type: Entra Id Authorization Policy

Score: 5

Compliance controls:

ARGOS Entra ID - 5.2

Description: Indicates whether users can sign up for email based subscriptions.

Rationale: Enables or disables the ability for users to sign up for services using self-service based on their email, offering a balance between accessibility and security.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: If unrestricted, this could lead to unauthorized access and potential security risks. Properly managed, it streamlines access to services, enhancing productivity.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup>

14. Restrict creation of M365 Groups

Restrict Microsoft 365 group creation to administrators only.

Cloud Service Type: Entra Id Authorization Policy

Score: 5

Compliance controls:

ARGOS Entra ID - 5.7

Description: Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'.

Rationale: Restricting Microsoft 365 group creation to administrators only ensures that creation of Microsoft 365 groups is controlled by the administrator. Appropriate groups should be created and managed by the administrator and group creation rights should not be delegated to any other user.

Tactics and techniques: [Persistence Initial Access Defense Evasion](#)

Help Link: <https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-creation-of-groups?view=o365-worldwide&redirectSourcePath=%252fen-us%252farticle%252fControl-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618>

15. Restrict creation of Entra ID Security Groups



Ensure the creation of Entra ID Security Groups is restricted

Cloud Service Type: Entra Id Authorization Policy

Score: 5

Compliance controls:

ARGOS Entra ID - 5.6

Description: Limits the ability to create security groups to global administrators and user administrators, preventing standard users from creating security groups in Azure portals, API, or PowerShell.

Rationale: Defines default permission of user to create security groups in Azure portals, API or PowerShell. Global administrators and user administrators can still create security groups.

Tactics and techniques: [Persistence Initial Access Defense Evasion](#)

Impact: Unrestricted security group creation can lead to over-proliferation of groups, complicating management and potentially leading to misconfigured permissions. Restricting this ability ensures a more controlled and secure environment.

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/GroupsManagementMenuBlade/~/_General

16. Restrict creation of Entra ID Tenants

Ensure the creation of Entra ID Tenants is restricted

Cloud Service Type: Entra Id Authorization Policy

Score: 5

Compliance controls:

ARGOS Entra ID - 5.7

Description: Restricts the creation of Entra ID tenants to the global administrator or tenant creator roles. Anyone who creates a tenant will become the global administrator for that tenant.

Rationale: This rule aims to control the proliferation of Entra ID tenants by limiting tenant creation to individuals in specific roles. By doing so, it ensures a centralized control over new tenant creation, reducing risks associated with unauthorized tenant sprawl and ensuring a consistent governance model.

Tactics and techniques: [Exfiltration Impact](#)

Impact: Allowing unrestricted tenant creation can lead to an unmanageable number of tenants, potential governance challenges, security risks, and unnecessary cost implications. Limiting this ability helps maintain organizational control and security compliance.

Help

Link: https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/_UserSettings

17. Self-service password reset should be enabled

Ensure self-service password reset is enabled for users.



Cloud Service Type: Entra Id Authorization Policy

Score: 4

Compliance controls:

ARGOS Entra ID - 5.8

Description: Designates whether users in this directory can reset their own password.

Rationale: Enabling Self-service Password Reset (SSPR) allows users to independently reset their passwords using various verification methods, such as phone, email, or security questions. This feature enhances security by supporting strong password practices and reduces the administrative burden on IT departments. It also ensures that users can promptly regain access to their accounts, maintaining productivity and operational efficiency.

Tactics and techniques: [Discovery](#)

Impact: Not enabling SSPR increases security risks due to potentially weaker password practices and increases operational costs with higher IT support involvement for password resets. It can lead to user downtime and frustration, affecting productivity and overall user satisfaction with IT services.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/PasswordResetMenuBlade/~/Proptieshttps://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices#enable-password-management

Microsoft Teams

1. Is Teams Chat Resource-Specific Consent Enabled

Ensure Teams Chat Resource-Specific Consent is Enabled

Cloud Service Type: Teams

Score: 5

Compliance controls:

Description: This rule checks if the Chat Resource-Specific Consent (RSC) is enabled for Microsoft Teams. RSC allows specific apps to access Teams resources with granular permissions, enhancing security and compliance.

Rationale: Enabling Chat Resource-Specific Consent (RSC) ensures that only authorized applications can access specific Teams resources with the necessary permissions. This reduces the risk of unauthorized access and data exfiltration.

Tactics and techniques: [Exfiltration](#)

Impact: If Chat Resource-Specific Consent is not enabled, unauthorized applications may gain access to Teams resources, leading to potential data breaches and compliance violations.

Help Link:<https://learn.microsoft.com/en-us/microsoftteams/platform/graph-api/rsc/resource-specific-consenthttps://learn.microsoft.com/en-us/microsoftteams/platform/graph-api/rsc/grant-resource-specific-consent>

2. Is Teams user Resource-Specific Consent Enabled

Ensure Teams user Resource-Specific Consent is Enabled



Cloud Service Type: Teams

Score: 5

Compliance controls:

Description: This rule checks if the user Resource-Specific Consent (RSC) is enabled for Microsoft Teams. RSC allows specific apps to access Teams resources with granular permissions, enhancing security and compliance.

Rationale: Enabling user Resource-Specific Consent (RSC) ensures that only authorized applications can access specific Teams resources with the necessary permissions. This reduces the risk of unauthorized access and data exfiltration.

Tactics and techniques: [Exfiltration](#)

Impact: If user Resource-Specific Consent is not enabled, unauthorized applications may gain access to Teams resources, leading to potential data breaches and compliance violations.

Help Link: <https://learn.microsoft.com/en-us/microsoftteams/platform/graph-api/rsc/resource-specific-consent><https://learn.microsoft.com/en-us/microsoftteams/platform/graph-api/rsc/grant-resource-specific-consent>

SharePoint Online

1. External sharing for SharePoint and OneDrive SHALL be limited to Existing guests or Only People in your organization

External sharing for SharePoint and OneDrive SHALL be limited to Existing guests or Only People in your organization

Cloud Service Type: Share Point Online

Score: 7

Compliance controls:

CISA SCuBA - MS.SHAREPOINT.1.1v1

CISA SCuBA - MS.SHAREPOINT.1.2v1

Description: Sharing information outside the organization via SharePoint increases the risk of unauthorized access. By limiting external sharing, administrators decrease the risk of access to information. OneDrive sharing cannot be more permissive (by design) than SharePoint's.

Rationale: Sign in to the SharePoint admin center.\n1. Select Policies > Sharing.\n2. Adjust external sharing slider for SharePoint to Existing guests or Only people in your organization.

Tactics and techniques: [Collection Exfiltration](#)

Help

Link:<https://go.microsoft.com/fwlink/?linkid=2185219><https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/sharepoint.md#mssharepoint11v1><https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/sharepoint.md#mssharepoint12v1>

2. External sharing SHALL be restricted to approved external domains and/or users in approved security groups per collaboration needs.



External sharing SHALL be restricted to approved external domains and/or users in approved security groups per collaboration needs.

Cloud Service Type: Share Point Online

Score: 7

Compliance controls:

CISA SCuBA - MS.SHAREPOINT.1.3v1

Description: By limiting sharing to domains or approved security groups used for interagency collaboration purposes, administrators help prevent sharing with unknown organizations and individuals.

Rationale: 1. Sign in to the SharePoint admin center.\r\n2. Select Policies > Sharing.\r\n3. Expand More external sharing settings.\r\n4. Select Limit external sharing by domain.\r\n5. Select Add domains.\r\n6. Add each approved external domain users are allowed to share files with.\r\n7. Select Manage security groups\r\n8. Add each approved security group. Members of these groups will be allowed to share files externally.\r\n9. Select Save.

Tactics and techniques: [Collection Exfiltration](#)

Impact: This policy is only applicable if the external sharing slider on the admin page is set to any value other than Only people in your organization.

Help

Link:<https://go.microsoft.com/fwlink/?linkid=2185219https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/sharepoint.md#mssharepoint13v1>

Microsoft Intune

1. ASR: Block PSEXec and WMI Lateral Movement

ASR: Block Process Creations from PSEXec and WMI Commands

Cloud Service Type: Intune

Score: 9

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block process creations originating from PSEXec and WMI commands." This thwarts common techniques for lateral movement and remote code execution in networks.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking process creations originating from PSEXec and WMI commands is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents attackers from using PSEXec and WMI for lateral movement and remote code execution, which are common techniques in advanced persistent threats.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-referencehttps://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

2. Credential Guard Enabled

Credential Guard Enabled



Cloud Service Type: Intune

Score: 9

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges - Hardware Security

Description: Enable Windows Defender Credential Guard to isolate LSASS and securely store authentication secrets. This prevents theft of credentials even if malware runs with admin rights.

Rationale: This is a manual control that requires verification that Windows Defender Credential Guard is enabled on all compatible managed devices through Intune endpoint security policies or device configuration to provide virtualization-based security for credentials.

Impact: Provides hardware-based isolation of authentication credentials, preventing credential theft attacks even when attackers have administrative privileges.

Help Link: <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy>

3. Unique Passwords for Local Admin Accounts

Unique Passwords for Local Administrator Accounts

Cloud Service Type: Intune

Score: 9

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges - Password Management

Description: Ensure local administrator accounts use long, unique, randomly generated passwords managed via a solution (e.g. LAPS). This prevents shared or default local admin credentials.

Rationale: This is a manual control that requires verification that all managed devices have unique, randomly generated local administrator passwords managed through Microsoft LAPS (Local Administrator Password Solution) or equivalent solution deployed via Intune.

Impact: Prevents lateral movement attacks that rely on shared local administrator passwords across multiple systems.

Help Link: <https://docs.microsoft.com/en-us/windows-server/identity/laps/laps-overview><https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10>

4. ASR: Block Credential Theft (LSASS)

ASR: Block Credential Theft from LSASS Process

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction



Description: Enable Defender ASR rule to "Block credential stealing from the Windows Local Security Authority (LSASS) process." This prevents malware from dumping credentials from memory.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking credential theft from LSASS is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents credential harvesting attacks that target the LSASS process, which stores authentication credentials in memory.

Help Link: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

5. ASR: Block Executable Content in Email

ASR: Block Executable Content from Email Clients

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block executable content from email clients and webmail." This stops users from inadvertently executing malicious email attachments or downloads.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking executable content from email clients is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents execution of malicious attachments and downloads from email clients, which is a primary attack vector for malware distribution.

Help Link: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

6. ASR: Block Obfuscated Scripts

ASR: Block Execution of Potentially Obfuscated Scripts

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block execution of potentially obfuscated scripts." This mitigates attacks using heavily obfuscated scripts (e.g. malicious PowerShell/JavaScript).

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking obfuscated scripts is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents execution of obfuscated scripts commonly used by malware to evade detection and analysis.



Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

7. ASR: Block JavaScript/VBScript Launching EXEs

ASR: Block JavaScript/VBScript from Launching Executables

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block JavaScript or VBScript from launching downloaded executable content." This prevents script-based threats (e.g. in browsers or WSH) from executing binaries.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking JavaScript/VBScript from launching executables is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents script-based attacks from executing downloaded or dropped executables, which is a common malware distribution technique.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

8. ASR: Block Untrusted Executables (Prevalence-Based)

ASR: Block Untrusted Executables Based on Prevalence

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block executable files from running unless they meet a prevalence, age, or trusted list criterion." This uses cloud heuristics to block uncommon or suspicious programs.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking untrusted executables based on prevalence is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Blocks execution of rare or suspicious executables that don't meet Microsoft's cloud intelligence criteria for trustworthiness.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

9. ASR: Block Persistence via WMI Events

ASR: Block Persistence through WMI Event Subscription



Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block persistence through WMI event subscription." This prevents malware from establishing persistence on endpoints via malicious WMI event hooks.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking persistence through WMI event subscription is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents malware from using WMI event subscriptions to maintain persistence on compromised systems, which is a sophisticated persistence technique.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

10. LSA Protection Enabled

LSA Protection Enabled

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges - Hardware Security

Description: Enable Local Security Authority (LSA) protection so LSASS process memory cannot be easily read or injected by non-protected processes. This hardens credential protection in the OS.

Rationale: This is a manual control that requires verification that LSA (Local Security Authority) protection is enabled on all managed devices through Intune endpoint security policies, registry settings, or group policy to prevent unauthorized access to LSASS process memory.

Impact: Prevents credential theft attacks that target the LSASS process by restricting access to process memory and preventing code injection.

Help Link:<https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy>

11. Memory Integrity (HVCI) Enabled

Memory Integrity (HVCI) Enabled

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges - Hardware Security



Description: Enable Hypervisor-Enforced Code Integrity ("Memory integrity") on Windows 10/11 devices. HVCI blocks malicious or untrusted kernel-mode code, mitigating kernel-level attacks.

Rationale: This is a manual control that requires verification that Hypervisor-Enforced Code Integrity (HVCI) / Memory Integrity is enabled on all compatible managed devices through Intune endpoint security policies or device configuration.

Impact: Provides hardware-based protection against kernel-level attacks and code injection by ensuring only trusted code can run in kernel mode.

Help Link:<https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/enable-virtualization-based-protection-of-code-integrity><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-account-protection-policy>

12. Intune - Application Control (Application Allow Listing)

Intune - Application Control

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Control

ISM Protected (Entra ID) - ISM-0843

ISM Protected (Entra ID) - ISM-1490

ISM Protected (Entra ID) - ISM-1665

Description: This rule checks if application control (application allow listing) is configured according to Essential 8 guidelines using AppLocker or Windows Defender Application Control (WDAC).

Rationale: Application control prevents malicious or untrusted software from running by only allowing approved applications to execute. This rule verifies Intune device configurations for WindowsDefenderApplicationControlPolicyEnabled or ApplicationGuardEnabled properties, and checks app protection policies for managed app data transfer restrictions (AllowedInboundDataTransferSources and AllowedOutboundDataTransferDestinations set to 'managedApps').

Impact: How to fix: Configure Intune device configuration policies to enable Windows Defender Application Control or deploy AppLocker policies. Navigate to Microsoft Intune admin center > Devices > Configuration profiles > Create profile > Windows 10 and later > Endpoint protection > Windows Defender Application Control.

Help Link:<https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol><https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/applocker/applocker-overview>

13. Office macros blocked from Win32 API calls

Ensure Office macros are prevented from making Win32 API calls

Cloud Service Type: Intune



Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Restrict Administrative Privileges

Description: This rule verifies that Office macros are configured to be blocked from making Win32 API calls, preventing potentially malicious macro execution.

Rationale: Blocking Office macros from Win32 API calls is a critical security control that prevents macros from executing system-level operations that could be used by attackers.

This control checks Intune Settings-catalog profile OMA-URI

./Vendor/MSFT/Policy/Config/Office16/BlockWin32API with value=Enabled must be present for all devices via GET /deviceManagement/deviceConfigurations/{id}/omaSettings.

Impact: This configuration may break legitimate macros that require Win32 API access, but significantly improves security by preventing macro-based attacks from accessing system APIs.

Help Link:<https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked><https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10>

14. Intune - Patch Applications

Intune - Patch Applications

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Patch Applications

ISM Protected (Entra ID) - ISM-1496

ISM Protected (Entra ID) - ISM-1497

ISM Protected (Entra ID) - ISM-1498

Description: This rule checks if application patching is configured according to Essential 8 guidelines.

Rationale: Applications should be configured to automatically install security patches. This rule validates Intune managed app policies for automatic update settings

(AutoUpdateEnabled=true, BlockUpdatesFromNonApprovedSources=true,

ForceUpdateIfCritical=true, MaxDeferralDaysForUpdates<=30) and app protection

policies for minimum version requirements (MinimumRequiredAppVersion,

MinimumRequiredOsVersion, MinimumRequiredSdkVersion).

Impact: How to fix: Configure Intune managed app policies to enable automatic application updates. Navigate to Microsoft Intune admin center > Apps > App protection policies > Create policy. Enable automatic updates and restrict updates from non-approved sources.

Help Link:<https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/patch-applications><https://intune.microsoft.com/https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies>

15. Intune - Patch Operating Systems



Intune - Patch Operating Systems

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Patch Operating Systems

ISM Protected (Entra ID) - ISM-1493

ISM Protected (Entra ID) - ISM-1494

ISM Protected (Entra ID) - ISM-1495

Description: This rule checks if operating system patching is configured according to Essential 8 guidelines.

Rationale: Operating systems should be configured to automatically install security patches. This rule validates Intune Windows Update for Business configurations for automatic update settings (AutoUpdateEnabled=true, SecurityUpdatesForced=true, CriticalUpdatesForced=true, MaxDeferralDays<=30) and checks traditional Windows Update settings (AutomaticUpdateMode with quality updates deferral <=30 days and feature updates deferral <=180 days).

Impact: How to fix: Configure Intune Windows Update for Business policies to enable automatic patching. Navigate to Microsoft Intune admin center > Devices > Windows > Update rings for Windows 10 and later > Create profile. Set quality update deferral period to 0 days for critical systems.

Help Link: <https://intune.microsoft.com/https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure>

16. Office applications cannot create executables

Ensure ASR rule – Office cannot create executables

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that the Attack Surface Reduction (ASR) rule preventing Office applications from creating executable content is enabled and configured to block.

Rationale: Immediate Action: Configure Attack Surface Reduction rule in Microsoft Intune to block Office applications from creating executable content. Use PowerShell: Connect-MgGraph; New-MgDeviceManagementDeviceConfigurationPolicy for ASR rules with rule ID '3b576869-a4ec-4529-8536-b80a7769e899' set to block mode. Platform Policy: Implement Microsoft Security Baselines for Windows 10/11 and Office 365 which include recommended ASR rule configurations. Holistic Approach: Deploy comprehensive endpoint protection strategy with Microsoft Defender for Business, implement Application Control (WDAC), enable macro blocking policies in Office 365, and establish user security awareness training to recognize social engineering attacks that rely on malicious documents.

Impact: How to fix: In Microsoft Intune, create an Endpoint Security policy for Attack surface reduction rules. Enable rule 'Block Office applications from creating executable content' and set to Block mode. Deploy to all managed devices.



Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction><https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules>

17. ASR rule – Office cannot inject code

Ensure Attack Surface Reduction rule blocks Office from injecting code into other processes

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that the Attack Surface Reduction (ASR) rule preventing Office applications from injecting code into other processes is enabled and configured to block.

Rationale: Immediate Action: Configure Attack Surface Reduction rule to block Office applications from injecting code into other processes. Use PowerShell: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-MgDeviceManagementAttackSurfaceReductionRule -RuleId '75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84' -Action 'Block' -DisplayName 'Block Office apps from injecting code into other processes'. Platform Policy: Implement Microsoft Security Baselines for Windows 10/11 and Office 365 that include comprehensive ASR rule configurations. Use Microsoft Intune compliance policies to enforce endpoint protection across all managed devices. Holistic Approach: Deploy comprehensive endpoint protection strategy with multiple ASR rules, Microsoft Defender for Business for advanced threat protection, implement application isolation with Windows Defender Application Guard for Office, establish user education on macro security, and implement controlled folder access to protect against ransomware attacks.

Impact: This configuration may impact legitimate Office add-ins or extensions that require code injection capabilities, but significantly improves security against sophisticated attack techniques.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction><https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules>

18. Office applications cannot spawn child processes

Ensure Office applications blocked from creating child processes

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: Attack Surface Reduction (ASR) rule preventing Office applications from creating child processes is enabled and configured to block.

Rationale: This control verifies that the ASR rule preventing Office applications from spawning child processes is enabled. The rule checks Microsoft Intune device security



policies and endpoint protection profiles for ASR rule 'Block Office applications from spawning child processes' configured in 'Block' mode. This prevents malware from using Office documents to launch malicious executables or scripts, which is a common attack vector.

Impact: How to fix: Create an Endpoint Security policy in Microsoft Intune. Navigate to Endpoint security > Attack surface reduction > Create Policy > Windows 10 and later > Attack surface reduction rules. Enable rule 'Block Office applications from creating child processes' and set to Block mode. Assign to all users and devices.

Help Link:<https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction><https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eighth><https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference>

19. Microsoft recommended blocklist in place

Ensure Microsoft recommended application blocklist is implemented

Cloud Service Type: Intune

Score: 8

Compliance controls:

Essential 8 (Australia ACSC) - Application Control

Description: This rule verifies that the Microsoft recommended application blocklist is implemented in Windows Defender Application Control policies. Requires Microsoft Intune licensing (included in Microsoft 365 E3/E5 or standalone Intune licenses).

Rationale: Immediate Action: Deploy Microsoft recommended blocklist through Windows Defender Application Control. Use PowerShell: Connect-MgGraph -Scopes 'DeviceManagementConfiguration.ReadWrite.All'; New-

MgDeviceManagementWindowsDefenderApplicationControlSupplementalPolicy with Microsoft-provided rule IDs. Platform Policy: Implement Microsoft Security Baselines for Windows 10/11 which include recommended WDAC policies. Use Microsoft Intune compliance policies to enforce application control across all managed devices. Holistic Approach: Establish comprehensive endpoint protection strategy combining WDAC with Microsoft Defender for Business, implement application allowlisting for critical systems, establish Software Restriction Policies (SRP) for legacy systems, and create incident response procedures for blocked application events. Regular updates from Microsoft's threat intelligence ensure protection against emerging threats.

Impact: Implementing the Microsoft recommended blocklist may block some applications that organizations use, but provides protection against known malicious and vulnerable software.

Help Link:<https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/applications-that-can-bypass-appcontrol><https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/appcontrol>

20. ASR: Block Office Communication Apps Creating Processes

ASR: Block Office Communication Apps from Creating Child Processes



Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block Office communication applications from creating child processes." This stops apps like Teams/Skype from spawning executables, foiling certain phishing malware.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking Office communication applications from creating child processes is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents communication applications from being exploited to launch malicious processes, which is a technique used in some phishing and social engineering attacks.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

21. ASR: Block Untrusted USB Processes

ASR: Block Untrusted and Unsigned Processes from USB

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Attack Surface Reduction

Description: Enable ASR rule to "Block untrusted and unsigned processes that run from USB." This helps prevent malware introduced via removable media by blocking unauthorized executables on USB drives.

Rationale: This is a manual control that requires verification that the Attack Surface Reduction rule for blocking untrusted and unsigned processes that run from USB is enabled through Intune endpoint security policies or Microsoft Defender configuration.

Impact: Prevents malware distribution through USB drives and removable media, which is a common attack vector for air-gapped environments and physical security breaches.

Help Link:<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy>

22. Command-line process creation logging enabled

Ensure command-line process creation logging is enabled and configured

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that command-line process creation logging is enabled through Intune configuration to capture detailed process execution information.



Rationale: Command-line process creation logging provides visibility into process execution including command-line arguments, which is essential for detecting malicious activity and investigating security incidents. This control checks for OMA-URIs:

Audit_ProcessCreation_Success and IncludeCommandLineInProcessCreationEvents, and retrieves compliance state via Graph to report non-compliant devices.

Impact: Enabling process creation logging with command-line details may generate significant log volume but provides critical security visibility for threat detection and investigation.

Help Link: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-process-creation><https://learn.microsoft.com/en-us/intune/intune-service/configuration/custom-settings-windows-10>

23. Edge / Chrome hardening per ASD & vendor baseline

Ensure Edge and Chrome browsers are hardened according to ASD and vendor baselines

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that Microsoft Edge and Chrome browsers are configured according to Australian Signals Directorate (ASD) and vendor security baselines through Intune baseline policies.

Rationale: Browser hardening is essential for protecting against web-based attacks and reducing the attack surface of commonly used applications. This control checks Intune Baselines: GET /deviceManagement/templates?filter=displayName eq 'Microsoft Edge Baseline' and GET /deviceManagement/intents/{id}/deviceSettingStateSummaries for compliance. It alerts if any device is non-compliant or if the template is not assigned to all Windows endpoints.

Impact: Browser hardening may impact user experience by restricting certain features, but significantly improves security posture against web-based threats.

Help Link: <https://learn.microsoft.com/en-us/intune/intune-service/protect/security-baselines><https://learn.microsoft.com/en-us/deployedge/microsoft-edge-security-endpoints>

24. PowerShell logging enabled

Ensure PowerShell module/script-block logging centrally logged

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that PowerShell module logging, script-block logging, and transcription are enabled through Intune configuration and that logs are centrally collected.

Rationale: Essential 8 Maturity Level 2 requires PowerShell module and script-block logging to be centrally logged for security monitoring. This control checks Microsoft Intune device



configuration policies for PowerShell logging settings including module logging, script-block logging, and transcription. These logs are essential for detecting malicious PowerShell activity and conducting security investigations.

Impact: How to fix: Create a Device Configuration profile in Microsoft Intune. Navigate to Devices > Configuration profiles > Create profile > Windows 10 and later > Templates > Custom. Add OMA-URI settings for PowerShell logging: EnableModuleLogging, EnableScriptBlockLogging, and EnableTranscripting. Deploy to all devices and configure log forwarding to your SIEM.

Help Link:https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging?view=powershell-5.1<https://learn.microsoft.com/en-us/intune/intune-service/configuration/custom-settings-windows-10>

25. Intune - Regular Backups

Intune - Regular Backups (Data Recovery Capability)

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Regular Backups

ISM Protected (Entra ID) - ISM-1511

ISM Protected (Entra ID) - ISM-1547

ISM Protected (Entra ID) - ISM-1705

Description: This rule checks if regular backups are configured according to Essential 8 guidelines, including Microsoft 365 retention policies and OneDrive backup configurations.

Rationale: Regular backups ensure data recovery capability in case of ransomware, data corruption, or system failure. This rule validates Microsoft 365 retention policies (checking IsEnabled and retention duration >= 365 days for Exchange, SharePoint, OneDrive, and Teams), OneDrive Known Folder Move configuration (KnownFolderMoveEnabled, DesktopFolderEnabled, DocumentsFolderEnabled), and Exchange deleted item retention policies.

Impact: How to fix: Configure Microsoft 365 retention policies for Exchange, SharePoint, and Teams data. Enable OneDrive Known Folder Move to back up user Desktop/Documents/Pictures folders. Navigate to Microsoft Purview compliance portal > Data lifecycle management > Adaptive protection.

Help Link:<https://learn.microsoft.com/en-us/purview/retention><https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange><https://docs.microsoft.com/en-us/onedrive/redirect-known-folders>

26. ASR rule – PDF reader cannot spawn child processes

Ensure Attack Surface Reduction rule blocks PDF readers from creating child processes

Cloud Service Type: Intune

Score: 7



Compliance controls:

Essential 8 (Australia ACSC) - Application Hardening

Description: This rule verifies that the Attack Surface Reduction (ASR) rule preventing PDF reader applications from spawning child processes is enabled and configured to block.

Rationale: Preventing PDF readers from spawning child processes helps protect against malware that uses malicious PDF documents to execute additional payloads or commands. This control verifies ASR GUID 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c via the same API endpoint and ensures it is set to block.

Impact: This configuration may impact PDF readers that legitimately need to spawn child processes for certain features, but significantly improves security against PDF-based attacks.

Help Link: <https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction><https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference>

27. WDAC not deployed to internet-facing servers

Ensure Windows Defender Application Control on internet-facing servers

Cloud Service Type: Intune

Score: 7

Compliance controls:

Essential 8 (Australia ACSC) - Application Control

Description: Windows Defender Application Control (WDAC) policies are deployed to internet-facing servers with enforcement level set to enforced. Requires Microsoft Intune licensing (included in Microsoft 365 E3/E5 or standalone Intune licenses).

Rationale: Immediate Action: Deploy WDAC policies to internet-facing servers with enforcement mode enabled. Use PowerShell: Connect-MgGraph -Scopes

'DeviceManagementConfiguration.ReadWrite.All'; New-

MgDeviceManagementWindowsDefenderApplicationControlSupplementalPolicy targeting server groups. Identify internet-facing servers through Azure VM assessments. Platform Policy: Implement Microsoft Security Baselines for Windows Server that include WDAC enforcement. Use Microsoft Intune compliance policies to ensure WDAC deployment to high-risk systems. Holistic Approach: Establish tiered application control strategy with strictest policies on internet-facing infrastructure, implement application allowlisting based on Microsoft recommended blocklist, use Microsoft Defender for Servers for additional threat protection, and establish monitoring for application control violations. Consider implementing Just Enough Administration (JEA) for privileged server access.

Impact: How to fix: Create WDAC policies in Microsoft Intune using the Windows Defender Application Control Supplemental Policies. Identify and group internet-facing servers in Intune. Deploy WDAC policies with enforcement mode enabled to these server groups. Ensure policies allow necessary applications while blocking unauthorized software.

Help Link: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control><https://docs.microsoft.com/en-us/graph/api/resources/intune-deviceconfig-windowsdefenderapplicationcontrols supplementalpolicy>

28. Intune - Configure Microsoft Office Macro Settings



Intune - Configure Microsoft Office Macro Settings

Cloud Service Type: Intune

Score: 6

Compliance controls:

Essential 8 (Australia ACSC) - Configure Microsoft Office Macro Settings

ISM Protected (Entra ID) - ISM-1488

ISM Protected (Entra ID) - ISM-1489

ISM Protected (Entra ID) - ISM-1490

Description: This rule checks if Microsoft Office macro settings are configured securely according to Essential 8 guidelines.

Rationale: Microsoft Office macros can be used to execute malicious code. This rule verifies Intune device configurations for macro security settings (AllowMacros=false, BlockMacrosFromInternet=true, MacroSecurityLevel='Disabled' or 'SignedMacrosOnly') and checks app protection policies for Office-specific macro controls (BlockOfficeMacros, BlockMacrosFromInternet, RequireSignedMacros).

Impact: How to fix: Configure Intune device configuration policies to disable macros in Office applications, or set them to only allow signed macros from trusted publishers. Navigate to Microsoft Intune admin center > Devices > Configuration profiles > Create profile > Windows 10 and later > Administrative templates > Microsoft Office.

Help Link: <https://intune.microsoft.com/https://learn.microsoft.com/en-us/compliance/anz/e8-macro>

29. Intune - User Application Hardening

Intune - User Application Hardening

Cloud Service Type: Intune

Score: 6

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening

ISM Protected (Entra ID) - ISM-1467

ISM Protected (Entra ID) - ISM-1468

ISM Protected (Entra ID) - ISM-1469

Description: This rule checks if user applications are hardened according to Essential 8 guidelines.

Rationale: User applications should be configured with security settings to reduce attack surface. This rule validates Intune device configurations for application hardening features (ApplicationGuardEnabled, SmartScreenEnabled, SmartScreenBlockOverrideForFiles, SmartScreenBlockOverrideForSites, WindowsDefenderApplicationControlPolicyEnabled) and checks app protection policies for data protection settings (SaveAsBlocked, PrintBlocked, DataBackupBlocked).

Impact: How to fix: Configure Intune device configuration policies to enable application hardening features such as Windows Defender Application Guard, SmartScreen, and application control policies. Navigate to Microsoft Intune admin center > Devices >



Configuration profiles > Create profile > Windows 10 and later > Endpoint protection.

Help Link:<https://intune.microsoft.com/https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview>

30. Internet Explorer 11 Disabled

Internet Explorer 11 Disabled/Removed

Cloud Service Type: Intune

Score: 5

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Legacy Components

Description: Internet Explorer 11 is retired and should be disabled or removed to eliminate a legacy attack vector. Ensures users rely on modern, secure browsers (e.g. Edge with IE mode for legacy needs).

Rationale: This is a manual control that requires verification that Internet Explorer 11 has been disabled or removed from all managed devices through Intune device configuration policies.

Impact: Reduces attack surface by eliminating legacy browser vulnerabilities and forces users to use modern, secure browsers.

Help Link:<https://docs.microsoft.com/en-us/internet-explorer/ie11-end-of-supporthttps://docs.microsoft.com/en-us/microsoft-edge/web-platform/ie-to-microsoft-edge-redirection>

31. .NET Framework 3.5 Disabled

.NET Framework 3.5 Disabled/Removed

Cloud Service Type: Intune

Score: 5

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Legacy Components

Description: Legacy frameworks like .NET 3.5 (which includes .NET 2.0/3.0) should be removed or turned off. This reduces exposure to old vulnerabilities.

Rationale: This is a manual control that requires verification that .NET Framework 3.5 and earlier versions have been disabled or removed from all managed devices through Intune device configuration policies or Windows features management.

Impact: Reduces attack surface by eliminating legacy framework vulnerabilities and ensures applications use modern, supported frameworks.

Help Link:<https://docs.microsoft.com/en-us/dotnet/framework/migration-guidehttps://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10>

32. Office OLE Package Activation Blocked



Office OLE Package Activation Blocked

Cloud Service Type: Intune

Score: 5

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Office Security

Description: Microsoft Office should be configured to prevent activation of OLE packages (embedded objects) in documents. This hardening measure blocks a known malware technique exploiting OLE objects.

Rationale: This is a manual control that requires verification that Microsoft Office applications are configured through Intune app protection policies or administrative templates to block OLE package activation and embedded object execution.

Impact: Prevents malware from exploiting OLE object vulnerabilities in Office documents, which is a common attack vector for document-based threats.

Help Link: <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-surface-reduction-rules-reference><https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies>

33. Windows PowerShell 2.0 Disabled

Windows PowerShell 2.0 Disabled/Removed

Cloud Service Type: Intune

Score: 5

Compliance controls:

Essential 8 (Australia ACSC) - User Application Hardening - Legacy Components

Description: Outdated PowerShell 2.0 lacks modern security enhancements and should be removed or disabled. This helps prevent attacks using older, less secure scripting engines.

Rationale: This is a manual control that requires verification that Windows PowerShell 2.0 engine has been disabled or removed from all managed devices through Intune device configuration policies or Windows features management.

Impact: Prevents attackers from using legacy PowerShell engines that lack modern security features like script block logging, AMSI integration, and constrained language mode.

Help Link: <https://docs.microsoft.com/en-us/powershell/scripting/install/windows-powershell-system-requirements><https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows>

34. Intune - Built-in device compliance policy should mark devices without compliance policy as 'Not compliant'.

Intune - Ensure the built-in Device Compliance Policy marks devices with no compliance policy assigned as 'Not compliant'

Cloud Service Type: Intune

Score: 4

Compliance controls:

Description:



Rationale: Set your Intune built-in Device Compliance Policy to mark devices with no compliance policy assigned as 'Not compliant'. This ensures that new devices that do not have any policies assigned are not compliant per default.

Impact: How to fix: Navigate to Microsoft Intune admin center

<https://intune.microsoft.com>. Click Devices scroll down to Manage devices. Select Compliance and Select Compliance settings. Set Mark devices with no compliance policy assigned as to Not compliant. Click Save.

Help

Link:https://admin.exchange.microsoft.com/https://intune.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/_compliance

35. Intune - Ensure device clean-up rule is configured.

Intune - Ensure device clean-up rule is configured.

Cloud Service Type: Intune

Score: 4

Compliance controls:

Description: This test checks if a device clean-up rule is configured to clean up devices in after 30 days of inactivity.

Rationale: Set your Intune device cleanup rules to delete Intune MDM enrolled devices that appear inactive, stale, or unresponsive. Intune applies cleanup rules immediately and continuously so that your device records remain current. If the resource name of this detection is the Tenant ID then this means no device clean up rule was detected.

Impact: How to fix: Navigate to Microsoft Intune admin center. Click Devices scroll down to Organize devices. Select Device clean-up rules. Set Delete devices based on last check-in date to Yes. Set Delete devices that haven't checked in for this many days to 30 days or more depending on your organizational needs. Click Save.

Help

Link:https://intune.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_DeviceSettings/DevicesMenu/~/_deviceCleanUp

Entra ID Conditional Access Policy

1. Block High Risk Sign-Ins in Entra ID Conditional Access Policies

Ensure High Risk Sign-ins are blocked in at least one Conditional Access Policy

Cloud Service Type: Entra Id Conditional Access Policy

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.2.3v1

Description: Blocking high-risk sign ins may prevent compromised sign-ins from accessing the tenant. This prevents compromised sign-ins from accessing the tenant.

Rationale: Note: CISA recommends blocking, the Microsoft recommendation is to require multi-factor authentication for high-risk sign-ins

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)



Help

Link: <https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad23v1>

2. Block High Risk User in Entra ID Conditional Access Policies

Ensure High Risk Users are blocked in at least one Conditional Access Policy

Cloud Service Type: Entra Id Conditional Access Policy

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.2.1v1

Description: Users identified as high risk by Microsoft Entra ID Identity Protection can be blocked from accessing the system via a Microsoft Entra ID Conditional Access policy. A high-risk user will be blocked until an administrator remediates their account.

Rationale: Immediate Action: Create a Conditional Access policy to block high-risk users. Use PowerShell: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy -DisplayName 'Block High Risk Users' -State 'enabled' -Conditions @{UserRiskLevels='high'} -GrantControls @{BuiltInControls='block'}. Platform Policy: Enable Entra ID Identity Protection and configure risk policies for automated responses. Holistic Approach: Implement a comprehensive identity risk management program with user and sign-in risk policies, automated remediation workflows, and integration with security operations center (SOC) processes. Configure risk-based conditional access with step-up authentication for medium-risk scenarios.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link: <https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad21v1>

3. Conditional Access Policy - Block Access to M365 Office unless compliant

Ensure only compliant devices can access M365 Office resources

Cloud Service Type: Entra Id Conditional Access Policy

Score: 7

Compliance controls:

Description: This rule checks if at least one Conditional Access Policy within Entra ID is configured that blocks access to M365 Office resources for not compliant devices and is targeted at all users.

Tactics and techniques: [Exfiltration](#)

Help Link: <https://cirriustech.co.uk/blog/outtatune-vulnerability/https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-device-compliance>

4. User detected that is excluded from Conditional Access Policy

Ensure that users are covered by Conditional Access Policy



Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 3.2

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: Checks each user to ensure they are included in at least one Conditional Access Policy (CAP) with MFA enforcement. Users not covered by any MFA CAP might have unrestricted access without multi-factor authentication, posing a security risk.

Rationale: Conditional Access Policies (CAPs) are crucial for securing access to resources by enforcing conditions that users must meet to access resources. This rule identifies users who are not covered by any CAPs with MFA enforcement (including MFA, block, compliant device, domain-joined device, or authentication strength controls), ensuring all users are subjected to multi-factor authentication with no exceptions as required by Essential 8.

Tactics and techniques: [Execution Impact](#)

Impact: Users not covered by any MFA-enforcing CAP may have unrestricted access to resources without multi-factor authentication, potentially bypassing important security measures designed to protect against unauthorized access and breaches. Ensuring all users are covered by MFA CAPs with no exceptions mitigates this risk.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/>

5. Protect Enterprise Copilot Platform (Microsoft 365 Copilot) using Entra ID Conditional Access Policies

Secure Enterprise Copilot with Conditional Access Policies

Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:

Microsoft Cloud Security Benchmark - NS-2

Description: This rule ensures that the Microsoft 365 Copilot platform is protected using Entra ID Conditional Access Policies.

Rationale: Conditional Access policies are essential to secure access to Microsoft 365 Copilot by enforcing specific conditions and controls.

Tactics and techniques: [Impact Collection](#)

Impact: Implementing these policies helps prevent unauthorized access and ensures that only compliant devices and users can access the Copilot platform. Follow the help link to understand how to create fitting Conditional Access Policies.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-copilot-ai-security>

6. Protect Microsoft Security Copilot Platform using Entra ID Conditional Access Policies

Secure Microsoft Security Copilot with Conditional Access Policies

Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:



Microsoft Cloud Security Benchmark - NS-2

Description: This rule ensures that the Microsoft Security Copilot platform is protected using Entra ID Conditional Access Policies.

Rationale: Conditional Access policies are essential to secure access to Microsoft Security Copilot by enforcing specific conditions and controls.

Tactics and techniques: [Impact Collection](#)

Impact: Implementing these policies helps prevent unauthorized access and ensures that only compliant devices and users can access the Copilot platform. Follow the help link to understand how to create fitting Conditional Access Policies.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-copilot-ai-security>

7. Trusted Location should be configured in Conditional Access Policies

Trusted Location should be configured in Conditional Access Policies

Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 2.4

Description: This rule checks if a trusted location is configured in Conditional Access Policies.

Rationale: Configuring a trusted location in Conditional Access Policies helps to ensure that access to resources is only allowed from known and trusted locations, enhancing security. 1. Navigate to the Microsoft Entra ID Conditional Access blade 2. Click on Named locations 3. Within Named locations, click on 'IP ranges location' 4. Enter a name for this location setting in the Name text box 5. Click on the + sign 6. Add an IP address in CIDR notation 7. Click on the Add button 8. Repeat steps 5 through 7 for each IP range that needs to be added 9. If the IP ranges entered are trusted ranges, select the 'Mark as trusted location' check box 10. Click on Create

Impact: Without a trusted location configured, there is a higher risk of unauthorized access from unknown locations.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network><https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition><https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions>https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/_/Overview/fromNav/

8. Block Device Code Flow in Entra ID Conditional Access Policies

Mandatory Blocking of Device Code Flow via Conditional Access Policy

Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:



Description: This rule checks if at least one Conditional Access Policy within Entra ID is configured that blocks Device Code Flow.

Tactics and techniques: [Credential Access](#)

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows#device-code-flow>

9. Block Legacy Authentication in Entra ID Conditional Access Policies

Mandatory Blocking of Legacy Authentication via Conditional Access Policy

Cloud Service Type: Entra Id Conditional Access Policy

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.1.1v1

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: This rule ensures that at least one Conditional Access Policy within Entra ID is configured to block legacy authentication methods, which are less secure and more susceptible to attacks. Implementing this rule significantly enhances the security posture by leveraging modern authentication protocols.

Rationale: Legacy authentication protocols do not support modern security features like multi-factor authentication, making them vulnerable to brute force and password spray attacks. By blocking legacy authentication, organizations can protect against such vulnerabilities and ensure that only secure, modern authentication methods are used.

Tactics and techniques: [Credential Access](#)

Impact: Blocking legacy authentication may affect clients and devices that rely on these older protocols. It's important to assess the compatibility of your environment and gradually transition to modern authentication mechanisms to minimize potential disruptions.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/block-legacy-authentication>

10. Managed devices SHOULD be required for authentication

Managed devices SHOULD be required for authentication

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.7v1

Description: The security risk of an adversary authenticating to the tenant from their own device is reduced by requiring a managed device to authenticate. Managed devices are under the provisioning and control of the organization. OMB-22-09 (see help links) states, \

Rationale: Create a conditional access policy requiring a user's device to be either Microsoft Entra hybrid joined or compliant during authentication.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: 1. In Entra under Protection and Conditional Access, select Policies.\r\n2. Click on New policy\r\n3. Under New Conditional Access policy, configure the following policy settings in the new conditional access policy, per the values below:\r\n- Users > Include



> All users\r\n- Target resources > Cloud apps > All cloud apps\r\n- Access controls > Grant > Grant Access > Require device to be marked as compliant and Require Microsoft Entra hybrid joined device > For multiple controls > Require one of the selected controls

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad37v1><https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

11. Managed devices SHOULD be required for MFA registration

Managed devices SHOULD be required for MFA registration

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.8v1

Description: Reduce risk of an adversary using stolen user credentials and then registering their own MFA device to access the tenant by requiring a managed device provisioned and controlled by the agency to perform registration actions. This prevents the adversary from using their own unmanaged device to perform the registration.

Rationale: Create a conditional access policy requiring a user to be on a managed device when registering for MFA.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: 1. In Entra under Protection and Conditional Access, select Policies.\r\n2. Click on New policy\r\n3. Under New Conditional Access policy, configure the following policy settings in the new conditional access policy, per the values below:\r\n- Users > Include > All users\r\n- Target resources > User actions > Register security information\r\n- Access controls > Grant > Grant Access > Require device to be marked as compliant and Require Microsoft Entra hybrid joined device > For multiple controls > Require one of the selected controls

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad38v1>

12. Ensure Conditional Access Policy requiring MFA is enabled

Checks if Conditional Access Policy requiring MFA is enabled

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.2v1

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: If phishing-resistant MFA has not been enforced, an alternative MFA method SHALL be enforced for all users.



Rationale: Immediate Action: Create a Conditional Access policy requiring MFA for all users. Use PowerShell: Connect-MgGraph -Scopes 'Policy.ReadWrite.ConditionalAccess'; New-MgIdentityConditionalAccessPolicy with conditions targeting all users and grant controls requiring MFA. Platform Policy: Enable Security Defaults as a baseline if no other CA policies exist, or implement the Microsoft Security Baseline for Entra ID. Holistic Approach: Develop a comprehensive identity protection strategy with risk-based authentication, implement passwordless authentication methods (Windows Hello, FIDO2), and establish emergency access accounts with proper break-glass procedures. Consider implementing Continuous Access Evaluation (CAE) for real-time policy enforcement.

Tactics and techniques: [Credential Access](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad32v1>

13. Phishing-resistant MFA shall be enforced for all users

Phishing-resistant MFA shall be enforced for all users

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.1v1

Description: Weaker forms of MFA do not protect against sophisticated phishing attacks. By enforcing methods resistant to phishing, those risks are minimized.

Rationale: The phishing-resistant methods Microsoft Entra ID certificate-based authentication (CBA), FIDO2 Security Key, Windows Hello for Business, and device-bound passkeys (in the authenticator app of choice) are the recommended authentication options since they offer forms of MFA with the least weaknesses. For federal agencies, Microsoft Entra ID CBA supports federal PIV card authentication directly to Microsoft Entra ID.

Tactics and techniques: [Initial Access](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad31v1>

14. Phishing-resistant MFA shall be enforced for all highly privileged roles

Phishing-resistant MFA shall be enforced for all highly privileged roles

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.3.6v1

Essential 8 (Australia ACSC) - Multi-Factor Authentication

Description: This is a backup security policy to help protect privileged access to the tenant if the conditional access policy, which requires MFA for all users, is disabled or misconfigured.

Rationale: The following roles are considered highly privileged according to CISA: Global Administrator, Privileged Role Administrator, User Administrator, SharePoint Administrator,



Exchange Administrator, Hybrid Identity Administrator, Application Administrator, Cloud Application Administrator

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad36v1>

15. Block High Risk User in Entra ID Conditional Access Policies

A notification SHOULD be sent to the administrator when high-risk users are detected.

Cloud Service Type: Entra Id Conditional Access Policy

Score: 5

Compliance controls:

CISA SCuBA - MS.AAD.2.2v1

Description: Notification enables the admin to monitor the event and remediate the risk. This helps the organization proactively respond to cyber intrusions as they occur.

Rationale: Blocking high-risk users may prevent compromised accounts from accessing the tenant. This requires the Tenant to be licensed for P2. If the tenant is not, then this might be a false-positive.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:<https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/ad.md#msaad22v1>

Entra ID Applications

1. Entra ID Application has dangerously extensive permissions

Ensure Entra ID Application only has required permissions

Cloud Service Type: Entra Id Applications

Score: 8

Compliance controls:

ARGOS Entra ID - 1.2

Description: This rule checks for Entra ID applications that are granted permissions which exceed the minimum necessary for their operation. Specifically, it identifies applications with permissions that could potentially allow them to escalate privileges or perform actions on behalf of other entities within the organization.

Rationale: Permissions within Entra ID should follow the principle of least privilege, ensuring applications have no more access than they need. This rule identifies applications with permissions that could be abused for privilege escalation, including but not limited to RoleManagement.ReadWrite.Directory, AppRoleAssignment.ReadWrite.All, and Application.ReadWrite.All. These permissions can allow applications to modify roles, assign app roles, and act as other entities, respectively, which might lead to unauthorized access or actions within the organization's digital environment.



Impact: Applications with extensive permissions pose a significant security risk. They could be leveraged by malicious actors to gain elevated access or control over organizational resources, potentially leading to data breaches, unauthorized data access, or further compromise of organizational security. Identifying and mitigating such permissions is crucial for maintaining the integrity and security of the organization's digital assets.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions?pivots=ms-graph>

2. Entra ID Graph CLI Service Principal should not have permanent permissions consented to

Ensure the 'Microsoft Graph Command Line Tools' service principal has no permissions consented to.

Cloud Service Type: Entra Id Applications

Score: 8

Compliance controls:

ARGOS Entra ID - 1.3

Description: This rule checks if the Entra ID 'Microsoft Graph Command Line Tools' Service Principal has any permissions consented to it.

Rationale: This rule identifies if the 'Microsoft Graph Command Line Tools' Service Principal has permissions consented to it. These should be regularly reviewed and ideally removed as they can allow a user to escalate their privileges within Entra ID. While some use cases (like an ARGOS assessment) might require permissions on this application it is highly recommended to review this application regularly and remove permissions when not required anymore.

Tactics and techniques: [Persistence](#)

Impact: Privilege-escalation path to read/write directory data across the tenant.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions?pivots=ms-graph>

3. Entra ID Service Principal has dangerously extensive permissions

Ensure Entra ID Service Principal only has required permissions

Cloud Service Type: Entra Id Applications

Score: 8

Compliance controls:

ARGOS Entra ID - 1.2

Description: This rule checks for Entra ID Service Principals that are granted permissions which exceed the minimum necessary for their operation. Specifically, it identifies service principals with permissions that could potentially allow them to escalate privileges or perform actions on behalf of other entities within the organization.

Rationale: Permissions within Entra ID should follow the principle of least privilege, ensuring Service Principals have no more access than they need. This rule identifies Service Principals with permissions that could be abused for privilege escalation, including but not limited to RoleManagement.ReadWrite.Directory, AppRoleAssignment.ReadWrite.All, and



Application.ReadWrite.All. These permissions can allow applications to modify roles, assign app roles, and act as other entities, respectively, which might lead to unauthorized access or actions within the organization's digital environment.

Impact: Service Principals with extensive permissions pose a significant security risk. They could be leveraged by malicious actors to gain elevated access or control over organizational resources, potentially leading to data breaches, unauthorized data access, or further compromise of organizational security. Identifying and mitigating such permissions is crucial for maintaining the integrity and security of the organization's digital assets.

Help Link: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions?pivots=ms-graph>

4. Entra ID Application redirects to insecure URI

Ensure Entra ID Application does not redirect to insecure URI

Cloud Service Type: Entra Id Applications

Score: 6

Compliance controls:

ARGOS Entra ID - 1.3

Description: This rule checks if Entra ID Applications are configured to redirect to URIs that do not use secure protocols. Redirecting to insecure URIs can expose applications to various security risks, such as man-in-the-middle attacks.

Rationale: When an application redirects to a URI that is not secured by HTTPS, the data transmitted between the client and the server can be intercepted, read, or modified by attackers. This rule identifies such insecure configurations to prevent potential security breaches.

Impact: If an Entra ID Application redirects to an insecure URI, sensitive data could be exposed during the redirect process, leading to potential data breaches and compromise of user security.

Help Link: <https://learn.microsoft.com/en-us/entra/identity-platform/security-best-practices-for-app-registration#redirect-uri>

5. Entra ID Application has no Owner configured

Ensure Entra ID Application has Owner configured

Cloud Service Type: Entra Id Applications

Score: 6

Compliance controls:

ARGOS Entra ID - 1.4

Description: This rule checks if Entra ID Applications are configured with at least one Owner.

Rationale: Applications without an owner may not be properly managed or maintained, leading to potential security risks. Assigning an owner ensures accountability and proper management of the application.\n\n

Impact: Applications without an owner may be neglected, leading to potential security vulnerabilities and lack of maintenance. However, Low privilege users that are owners of high privilege Applications can use that ownership for privilege escalation.



Help Link:<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/assign-app-owners?pivot=portalhttps://learn.microsoft.com/en-us/entra/identity/enterprise-apps/overview-assign-app-owners>

6. Entra ID Application uses password credentials

Ensure Entra ID Application uses certificate credentials

Cloud Service Type: Entra Id Applications

Score: 5

Compliance controls:

ARGOS Entra ID - 1.4

Description: This rule checks if Entra ID Applications use password credentials instead of certificates for authentication. Always use certificate credentials whenever possible and avoid password credentials, also known as secrets. A detection is created if an Application uses password credentials and does not use certificate credentials.

Rationale: Certificates offer stronger security than passwords by using cryptographic techniques, reducing the risk of compromise. They support advanced features like automatic rotation, aligning with best practices for secure authentication.

Impact: Using password credentials can lead to increased security risks, including unauthorized access and potential compliance failures. Certificates reduce these risks by providing more secure authentication methods.

Help Link:<https://learn.microsoft.com/en-us/entra/identity-platform/security-best-practices-for-app-registration#certificates-and-secretshttps://learn.microsoft.com/en-us/entra/identity-platform/certificate-credentials>

7. Entra ID Application has expired secret

Ensure Entra ID Application does not have expired secret

Cloud Service Type: Entra Id Applications

Score: 4

Compliance controls:

ARGOS Entra ID - 1.1

Description: This rule checks if Entra ID Applications have expired secrets. Secrets are used to authenticate and authorize applications to access resources. Expired secrets can lead to unexpected application outages.

Rationale: Application secrets are crucial for the security and operational integrity of applications, acting as passwords that allow applications to authenticate with services securely. When these secrets expire, the application may lose access to critical services and resources, disrupting its functionality. This rule identifies applications with expired secrets to ensure that all applications maintain continuous access to their resources and operate securely.

Impact: Having an expired secret in an Entra ID Application can result in authentication failures, leading to application downtime or restricted functionality. This not only affects the availability of the application but can also compromise the security posture by forcing the use of less secure fallback mechanisms.



Help Link:<https://learn.microsoft.com/en-us/entra/identity-platform/security-best-practices-for-app-registration#certificates-and-secrets>

Entra ID Consent Settings

1. Block User Consent for Risky Applications

Block User Consent on Detection of Risky Application Requests

Cloud Service Type: Entra Id Consent Settings

Score: 7

Compliance controls:

ARGOS Entra ID - 4.1

Description: Defines whether user consent will be blocked when a risky request is detected.

Rationale: This rule prevents users from giving consent to applications when those applications are determined to be risky. Risk assessment is performed based on various indicators such as unusual request patterns, untrusted sources, or other security red flags. By blocking consent in these scenarios, the rule helps to mitigate potential security risks that could lead to data leaks or other exploits.

Tactics and techniques: [Initial Access Persistence Defense Evasion Lateral Movement Credential Access](#)

Impact: Implementing this rule reduces the likelihood of security breaches by preventing unauthorized or risky applications from gaining access to sensitive or critical resources. It protects both user data and organizational assets from potential threats posed by compromised or malicious third-party applications.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-risk-based-step-up-consent>

2. Ensure only Admins can consent to 3rd party applications

Users can request admin consent to apps they are unable to consent to.

Cloud Service Type: Entra Id Consent Settings

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.5.2v1

Description: CISA SCuBA MS.AAD.5.2v1: Non-Admin Users SHALL Be Prevented From Providing Consent To Third-Party Applications.

Rationale: If this option is set to enabled, then users request admin consent to any app that requires access to data they do not have the permission to grant. If this option is set to disabled, then users must contact their admin to request to consent in order to use the apps they need.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/Admin



[minConsentSettingshttps://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overviewhttps://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad52v1](https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview)

3. Prevent Non-Admin User Consent to Third-Party Apps

Ensure email validated users cannot self join the Entra ID tenant.

Cloud Service Type: Entra Id Consent Settings

Score: 7

Compliance controls:

CISA SCuBA - MS.AAD.5.4v1

Description: CISA SCuBA 2.7: Non-Admin Users SHALL Be Prevented From Providing Consent To Third-Party Applications.

Rationale: Group and team owners can authorize applications, such as applications published by third-party vendors, to access your organization's data associated with a group. For example, a team owner in Microsoft Teams can allow an app to read all Teams messages in the team, or list the basic profile of a group's members.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Impact: Allowing non-admin users to provide consent to third-party applications can lead to unauthorized access to sensitive organizational data and potential data breaches, undermining the security of the Entra ID tenant.

Help

Link:[https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettingshttps://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad54v1](https://portal.azure.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings)

Entra ID Hybrid Management

1. Entra ID Connect Synchronisation is unhealthy

Entra ID Synchronisation is unhealthy.

Cloud Service Type: Entra Id Hybrid Management

Score: 5

Compliance controls:

ARGOS Entra ID - 6.0

Description: This rule checks the health status of Entra ID Connect Synchronisation to ensure it is functioning correctly.

Rationale: Entra ID Connect Synchronisation is responsible for synchronizing on-premises directories with Entra ID. If the synchronization is unhealthy, it can lead to outdated or incorrect directory information in Entra ID.

Impact: Unhealthy synchronization can result in security risks, such as outdated user information, incorrect group memberships, and potential access issues.

Help

Link:https://entra.microsoft.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncM



[enuBlade/~ /CloudSyncConfigurationshttps://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-synchttps://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-health-synchhttps://microsoft.github.io/zerotrustassessment/docs/workshop-guidance/identity/RMI_077](https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync)

2. Entra ID Synchronization Check

Check if synchronization between Entra ID and Active Directory exists.

Cloud Service Type: Entra Id Hybrid Management

Score: 1

Compliance controls:

ARGOS Entra ID - 6.1

Description: This rule checks if synchronization is configured between Entra ID and Active Directory.

Rationale: This is not a security issue, but something to be aware of in one's tenant.

Help

Link:https://entra.microsoft.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncM
[enuBlade/~ /CloudSyncConfigurationshttps://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-synchttps://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-health-synchhttps://microsoft.github.io/zerotrustassessment/docs/workshop-guidance/identity/RMI_077](https://entra.microsoft.com/#view/Microsoft_AAD_Connect_Provisioning/CloudSyncM)

Entra ID Password Setting

1. Activate Banned Password Enforcement

Enforce Banned Password List to Prevent Weak Passwords

Cloud Service Type: Entra Id Password Setting

Score: 7

Compliance controls:

ARGOS Entra ID - 5.8

Description: When enabled, the words in the list found in the Microsoft documentation are used in the banned password system to prevent easy-to-guess passwords.

Rationale: This rule checks the banned password check system, which uses a predefined list of commonly used, predictable, or compromised passwords. When enabled, any attempt to set a password that appears on this list is automatically rejected. This measure significantly enhances security by ensuring that all passwords are sufficiently strong and less likely to be breached.

Tactics and techniques: [Credential Access](#)

Impact: By enabling this setting in Entra ID, the organization mitigates the risk of password-related security breaches. It prevents the use of weak, common, or previously compromised passwords, thereby reducing the overall vulnerability to credential-based attacks. This is critical for maintaining the integrity and security of user accounts and sensitive data.



Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtectionhttps://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#global-banned-password-list

2. Smart Lockout - Lockout duration in seconds

Configure Lockout Duration to Prevent Brute Force Attacks

Cloud Service Type: Entra Id Password Setting

Score: 7

Compliance controls:

ARGOS Entra ID - 5.8

Description: The minimum length in seconds of each lockout. If an account locks repeatedly, this duration increases.

Rationale: This rule checks the minimum duration for which an account is locked out after a specified number of failed login attempts. The lockout duration acts as a critical deterrent against brute force attacks, where attackers try multiple password combinations. The smart lockout feature increases this duration with each subsequent lockout within a given time frame, thus enhancing security by preventing rapid repeat attempts on the same account.

Tactics and techniques: [Credential Access](#)

Impact: Implementing a smart lockout policy with dynamically increasing lockout durations significantly enhances security by reducing the risk of unauthorized access through brute force attacks. It prevents attackers from continuously attempting password guesses, thus protecting user accounts from compromise and maintaining the integrity of the system.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtectionhttps://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

3. Smart Lockout - Lockout threshold

Define Lockout Threshold for User Accounts to Prevent Unauthorized Access

Cloud Service Type: Entra Id Password Setting

Score: 7

Compliance controls:

ARGOS Entra ID - 5.8

Description: How many failed sign-ins are allowed on an account before its first lockout. If the first sign-in after a lockout also fails, the account locks out again.

Rationale: This rule checks the number of unsuccessful sign-in attempts allowed before a user account is locked out for the first time, enhancing security against unauthorized access attempts. Following a lockout, if the account's first subsequent sign-in attempt fails, the account is locked again. This smart lockout mechanism helps to strike a balance between securing accounts from brute force attacks and maintaining user accessibility by adjusting sensitivity based on recent sign-in activity and failures.

Tactics and techniques: [Credential Access](#)



Impact: Implementing a defined lockout threshold reduces the risk of unauthorized access through repeated password attempts. It serves as an effective deterrent against brute force attacks, securing sensitive data while ensuring that user accounts are only temporarily disabled to minimize inconvenience. This security measure is crucial for maintaining the integrity and confidentiality of user data and protecting the network from potential intrusions.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtectionhttps://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout

4. Manage Banned Password Check Modes

Control Mode for On-Premises Banned Password Check

Cloud Service Type: Entra Id Password Setting

Score: 6

Compliance controls:

ARGOS Entra ID - 5.8

Description: If set to Enforce, users will be prevented from setting banned passwords and the attempt will be logged. If set to Audit, the attempt will only be logged.

Rationale: This rule governs the operational mode of the banned password check for on-premises systems. When set to 'Enforce', the system actively prevents users from setting passwords that are deemed weak or commonly used (banned), and logs the attempt for audit purposes. If set to 'Audit' mode, the system does not block the use of banned passwords but records the attempt, allowing administrators to monitor compliance without enforcing restrictions.

Tactics and techniques: [Credential Access](#)

Impact: Setting this policy to 'Enforce' greatly enhances security by actively preventing the use of weak passwords, reducing the likelihood of successful credential-based attacks. On the other hand, setting it to 'Audit' provides insights into user behavior without immediate disruption, which can be useful during policy transition phases or for less critical systems.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtectionhttps://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

5. Configure custom banned list

Implement Custom Banned Password List for Enhanced Security

Cloud Service Type: Entra Id Password Setting

Score: 6

Compliance controls:

ARGOS Entra ID - 5.8

Description: A list of words, one per line, to prevent your users from using in their passwords. You should include words specific to your organization, such as your products,



trademarks, industries, local cities and towns, and local sports teams. Your list can contain up to 1000 words. These are case insensitive, and common character substitutions (o for 0, etc) are automatically considered.

Rationale: This rule checks the configuration of a custom banned password list, which prohibits users from selecting passwords containing any of the specified words. It is designed to include terms closely related to the organization, such as product names, industry-specific jargon, and locally significant names, enhancing security by avoiding predictable passwords. The system automatically extends these restrictions to common substitutions (e.g., replacing 'o' with '0'), making it more robust against common workarounds.

Tactics and techniques: [Credential Access](#)

Impact: Enforcing a custom banned password list significantly lowers the risk of password-related security breaches. By preventing the use of easily guessable passwords related to the organization, it enhances protection against brute-force and dictionary attacks. This proactive measure is crucial in safeguarding user accounts and sensitive information against external threats and insider vulnerabilities.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtectionhttps://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#custom-banned-password-list

6. Enable Banned Password Check for On-Premises Active Directory

Password Protection - Enable password protection on Windows Server Active Directory

Cloud Service Type: Entra Id Password Setting

Score: 6

Compliance controls:

ARGOS Entra ID - 5.8

Description: If set to Yes, password protection is turned on for Active Directory domain controllers when the appropriate agent is installed.

Rationale: This rule enforces the use of password protection on Windows Server Active Directory by checking passwords against a list of known weak or common passwords. When enabled, this setting requires the installation of an agent on domain controllers that ensures passwords are evaluated against this banned password list. This helps to prevent the use of easily guessable or commonly breached passwords, significantly enhancing the security of user credentials.

Tactics and techniques: [Credential Access](#)

Impact: Activating this rule helps secure the organizational network by reducing the risk of password-related breaches. By preventing the use of common or predictable passwords, the rule protects against unauthorized access and potential security incidents, thus strengthening the overall security posture of the organization.

Help

Link:https://portal.azure.com/#view/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/~/PasswordProtection

7. User passwords SHALL NOT expire



Ensure User passwords SHALL NOT expire

Cloud Service Type: Entra Id Password Setting

Score: 6

Compliance controls:

CISA SCuBA - MS.AAD.6.1v1

Description: The National Institute of Standards and Technology (NIST), OMB, and Microsoft have published guidance indicating mandated periodic password changes make user accounts less secure. For example, OMB-22-09 states, \

Rationale: This rule checks the configuration of a custom banned password list, which prohibits users from selecting passwords containing any of the specified words. It is designed to include terms closely related to the organization, such as product names, industry-specific jargon, and locally significant names, enhancing security by avoiding predictable passwords. The system automatically extends these restrictions to common substitutions (e.g., replacing 'o' with '0'), making it more robust against common workarounds.

Impact: Enforcing a custom banned password list significantly lowers the risk of password-related security breaches. By preventing the use of easily guessable passwords related to the organization, it enhances protection against brute-force and dictionary attacks. This proactive measure is crucial in safeguarding user accounts and sensitive information against external threats and insider vulnerabilities.

Help

Link:<https://admin.cloud.microsoft/?#/Settings/SecurityPrivacy/Settings/L1/PasswordPolicy><https://github.com/cisagov/ScubaGear/blob/main/PowerShell/ScubaGear/baselines/aad.md#msaad61v1>

Entra ID Device Registration Policy

1. Global Administrators are added to Device Local Administrators Group

Ensure Global Administrators are not added to Device Local Administrators Group

Cloud Service Type: Entra Id Device Registration Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 2.7

Description: By default, Global Administrators in Microsoft Entra ID are added to the Local Administrators group on devices, which can lead to elevated privileges and potential security risks. Only the users that were members of the Global Administrators role at the time of joining the device are added to the Local Administrators group.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/DeviceSettings/menuld/Overview<https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin><https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units>



2. Registering User is added to Device Local Administrators Group

Ensure Registering User is not added to Device Local Administrators Group

Cloud Service Type: Entra Id Device Registration Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 2.7

Description: By default, the user who registers a device in Microsoft Entra ID is added to the Local Administrators Group on that device, which can lead to elevated privileges and potential security risks. If this detection is found that means the registering user or a set of predefined users (independent of their Entra ID roles) will become local administrators on joined devices. Only the users defined at the time of joining the device are added to the Local Administrators group.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/_DeviciceSettings/menuld/Overview<https://learn.microsoft.com/en-us/entra/identity/devices/assign-local-admin><https://learn.microsoft.com/en-us/azure/active-directory/roles/admin-units>

3. User should not be allowed to join device to Entra ID

Ensure users cannot join devices to Entra ID

Cloud Service Type: Entra Id Device Registration Policy

Score: 6

Compliance controls:

ARGOS Entra ID - 2.7

Description: By default, Microsoft Entra ID allows all users to join their devices. Anyone with an Entra ID account can link their personal devices to Entra ID.

Tactics and techniques: [Initial Access Persistence Defense Evasion](#)

Help

Link:https://entra.microsoft.com/#view/Microsoft_AAD_Devices/DevicesMenuBlade/~/_DeviciceSettings/menuld/Overview<https://learn.microsoft.com/en-us/autopilot/tutorial/user-driven/azure-ad-join-allow-users-to-join><https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot>

Entra ID License Settings

1. Entra ID Premium P2 licenses should be purchased.

Entra ID Premium P2 licenses should be purchased.

Cloud Service Type: Entra Id License Settings

Score: 4

Compliance controls:



ARGOS Entra ID - 5.9

Description: This rule checks if the tenant has purchased Entra ID Premium P2 licenses.

Rationale: Entra ID Premium P2 licenses provide advanced security features, including Privileged Identity Management (PIM). Without these licenses, the tenant may be at risk of privilege escalation attacks.

Tactics and techniques: [Privilege Escalation](#)

Impact: Without Entra ID Premium P2 licenses, the tenant lacks advanced security features, increasing the risk of privilege escalation and other security threats.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Entra ID Privileged Identity Management

1. Entra ID Privileged Identity Management should be used.

Entra ID Privileged Identity Management should be used.

Cloud Service Type: Entra Id Pim

Score: 6

Compliance controls:

ARGOS Entra ID - 6.0

Description: This rule checks if there are any Privileged Identity Management (PIM) assignments in the tenant.

Rationale: Privileged Identity Management (PIM) helps manage, control, and monitor access within your organization. Without PIM assignments, there is a risk of unmanaged privileged access.

Tactics and techniques: [Privilege Escalation](#)

Impact: Without PIM assignments, the tenant may have unmanaged privileged access, increasing the risk of security breaches and privilege escalation.

Help Link: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

