Azure, Microsoft Entra ID & Microsoft 365 Security Configuration Checklist

> ***Last Updated:*** *January 2026* ***Purpose:*** *Comprehensive security configuration checklist for Azure, Microsoft Entra ID (formerly Azure Active Directory), and Microsoft 365/Office 365 environments.*

Table of Contents

1. Microsoft Entra ID (Identity & Access)

Multi-Factor Authentication (MFA)

- [ ] **Enable MFA for all users** - MFA blocks 99.9% of identity attacks Microsoft Learn: MFA Setup
- [ ] **Prioritize phishing-resistant MFA methods:**
- [ ] FIDO2 security keys
- [ ] Passkeys
- [ ] Windows Hello for Business
- [ ] Certificate-based authentication Microsoft Learn: Phishing-Resistant MFA

- [ ] **Disable SMS and voice call as MFA methods** (low-security options) Microsoft Learn: Authentication Methods
- [ ] **Block legacy authentication protocols** (POP3, IMAP, SMTP AUTH) - these don't support MFA Microsoft Learn: Block Legacy Auth

User & Application Permissions

- [ ] **Restrict non-admin users from creating tenants** - Set to "Yes" Microsoft Learn: Default User Permissions
- [ ] **Configure application consent settings:**
- [ ] Set to "Allow user consent for apps from verified publishers, for selected permissions" OR
- [ ] Set to "Let Microsoft manage your consent settings (Recommended)" Microsoft Learn: App Consent
- [ ] **Restrict device join permissions:**
- [ ] Set "Users may join devices to Microsoft Entra" to "Selected" groups
- [ ] Enable "Require MFA to register or join devices with Microsoft Entra" Microsoft Learn: Device Settings

Password & Credential Security

- [ ] **Enable password hash synchronization** - Even if using federation, configure as backup Microsoft Learn: Password Hash Sync
- [ ] **Configure self-service password reset (SSPR)** with strong authentication methods Microsoft Learn: SSPR
- [ ] **Enable Microsoft Entra Password Protection** - Block common and custom banned passwords Microsoft Learn: Password Protection

Hybrid Identity Security

- [ ] **Do NOT synchronize highly privileged on-premises accounts** to Entra ID Microsoft Learn: Hybrid Security
- [ ] **Ensure Global Administrator accounts are cloud-only** - No ties to on-premises AD Microsoft Learn: Privileged Access

Emergency Access (Break Glass) Accounts

- [ ] **Create at least 2 emergency access accounts** with:
- [ ] Highly protected Global Administrator rights
- [ ] Cloud-only authentication (not federated)
- [ ] Excluded from Conditional Access policies
- [ ] Different authentication methods than regular admins
- [ ] Monitored for any sign-in activity Microsoft Learn: Emergency Access

---

2. Conditional Access Policies

Core Policies

- [ ] **Require MFA for all users accessing all resources** Microsoft Learn: Require MFA
- [ ] **Require MFA for all administrators** (especially for Microsoft admin portals) Microsoft Learn: Admin MFA
- [ ] **Block access for high-risk sign-ins** using Identity Protection Microsoft Learn: Risk-Based Access
- [ ] **Require password change for high-risk users** Microsoft Learn: User Risk Policy
- [ ] **Require compliant or Hybrid Azure AD joined devices** Microsoft Learn: Device Compliance
- [ ] **Block access from unauthorized geographic locations** Microsoft Learn: Named Locations

Policy Configuration Best Practices

- [ ] **Use Conditional Access templates** aligned with Microsoft Zero Trust recommendations Microsoft Learn: CA Templates
- [ ] **Deploy policies in Report-Only mode first** before enforcement Microsoft Learn: Report-Only Mode
- [ ] **Exclude break-glass accounts** from all CA policies Microsoft Learn: CA Best Practices
- [ ] **Stay within 195 policy limit** per tenant Microsoft Learn: CA Limits
- [ ] **Review Microsoft-managed policies** and adopt where appropriate Microsoft Learn: Managed Policies

---

3. Privileged Identity Management (PIM)

Just-in-Time Access

- [ ] **Implement "no standing access"** - No permanent privileged role assignments Microsoft Learn: PIM Overview
- [ ] **Configure just-in-time activation** for all privileged roles Microsoft Learn: PIM Activation
- [ ] **Require MFA for all role activations** Microsoft Learn: PIM Settings
- [ ] **Require approval workflow** for sensitive role activations Microsoft Learn: Approval Workflow
- [ ] **Require justification** for all role activations Microsoft Learn: Role Settings
- [ ] **Set limited activation duration** (e.g., 1-8 hours maximum) Microsoft Learn: Time-Bound Access

Monitoring & Review

- [ ] **Enable alerts for privileged role activations** Microsoft Learn: PIM Alerts

- [ ] **Configure regular access reviews** for privileged roles Microsoft Learn: Access Reviews
- [ ] **Monitor all 28 Microsoft-tagged "Privileged" roles** (as of October 2025) Microsoft Learn: Built-in Roles
- [ ] **Limit Global Administrators** to 5 or fewer Microsoft Learn: Best Practices

---

4. Azure Infrastructure Security

Virtual Machine Security

- [ ] **Enable Trusted Launch** for all new Gen2 VMs (default since 2024) Microsoft Learn: Trusted Launch
- [ ] **Consider Confidential VMs** for sensitive workloads (AMD SEV-SNP) Microsoft Learn: Confidential Computing
- [ ] **Enable encryption at host** for end-to-end VM data encryption Microsoft Learn: Encryption at Host
- [ ] **Use Azure Disk Encryption** or Server-Side Encryption with customer-managed keys Microsoft Learn: Disk Encryption
- [ ] **Apply OS security baselines** using Defender for Cloud recommendations Microsoft Learn: Security Baselines
- [ ] **Enable Azure Update Management** for automated patching Microsoft Learn: Update Management
- [ ] **Enable Just-in-Time (JIT) VM access** - Reduce exposure to management ports Microsoft Learn: JIT Access
- [ ] **Use hardened VM images** from Azure Marketplace (CIS benchmarks) Microsoft Learn: Hardened Images

Resource Security

- [ ] **Enable Azure Resource Locks** on critical resources Microsoft Learn: Resource Locks
- [ ] **Implement Azure Policy** for enforcing security standards at scale Microsoft Learn: Azure Policy
- [ ] **Use Azure Blueprints** for consistent security deployment Microsoft Learn: Blueprints

---

5. Azure Network Security

Network Security Groups (NSGs)

- [ ] **Apply NSGs to all subnets and NICs** Microsoft Learn: NSG Overview
- [ ] **Review NSG rules regularly** - Remove overly permissive rules Microsoft Learn: NSG Best Practices
- [ ] **Never allow inbound from 'Any' or 'Internet'** to management ports Microsoft Learn: NSG Rules

- [ ] **Migrate from NSG flow logs to Virtual Network flow logs** (NSG flow logs deprecated after June 30, 2025) Microsoft Learn: VNet Flow Logs

Azure Firewall & Perimeter Security

- [ ] **Deploy Azure Firewall** for centralized network security Microsoft Learn: Azure Firewall
- [ ] **Enable Azure DDoS Protection** for public-facing resources Microsoft Learn: DDoS Protection
- [ ] **Use Private Endpoints** for Azure PaaS services Microsoft Learn: Private Endpoints
- [ ] **Implement Network Security Perimeter** (Preview) for PaaS resources Microsoft Learn: Network Perimeter

2025 Important Changes

- [ ] **Upgrade from Basic to Standard SKU public IPs** (Basic SKU retired September 30, 2025) Microsoft Learn: Public IP SKUs
- [ ] **Plan for removal of default outbound internet access** (September 30, 2025) Microsoft Learn: Default Outbound

---

6. Azure Data Protection & Encryption

Encryption at Rest

- [ ] **Verify Storage Service Encryption (SSE)** is enabled (default with Microsoft-managed keys) Microsoft Learn: Storage Encryption
- [ ] **Consider customer-managed keys (CMK)** for sensitive data using Azure Key Vault Microsoft Learn: CMK
- [ ] **Enable Azure Disk Encryption** for VM OS and data disks Microsoft Learn: ADE

Encryption in Transit

- [ ] **Enforce TLS 1.2 or later** for all connections (required by August 31, 2025) Microsoft Learn: TLS Requirements
- [ ] **Enable HTTPS-only access** for storage accounts Microsoft Learn: Secure Transfer
- [ ] **Use Azure VPN Gateway or ExpressRoute** for hybrid connectivity Microsoft Learn: VPN Gateway

Azure Key Vault Security

- [ ] **Use Azure Key Vault Premium or Managed HSM** for encryption key management Microsoft Learn: Key Vault Best Practices
- [ ] **Enable soft-delete and purge protection** on Key Vault Microsoft Learn: Soft Delete
- [ ] **Configure key rotation policies** Microsoft Learn: Key Rotation
- [ ] **Enable Key Vault access logging** Microsoft Learn: KV Logging

- [ ] **Use RBAC for Key Vault access control** (instead of access policies) Microsoft Learn: KV RBAC
- [ ] **Backup Key Vault secrets/keys** that cannot be recreated Microsoft Learn: Backup

---

7. Microsoft Defender for Cloud

Enable Protection Plans

- [ ] **Enable Defender for Cloud** on all subscriptions Microsoft Learn: Enable Defender
- [ ] **Enable Defender CSPM** (Cloud Security Posture Management) Microsoft Learn: Defender CSPM
- [ ] **Enable Defender for Servers** (Plan 1 or Plan 2) Microsoft Learn: Defender for Servers
- [ ] **Enable Defender for Storage** Microsoft Learn: Defender for Storage
- [ ] **Enable Defender for Containers** Microsoft Learn: Defender for Containers
- [ ] **Enable Defender for Key Vault** Microsoft Learn: Defender for KV
- [ ] **Enable Defender for SQL** Microsoft Learn: Defender for SQL

Configuration

- [ ] **Apply Microsoft Cloud Security Benchmark (MCSB)** as default standard Microsoft Learn: MCSB
- [ ] **Configure auto-provisioning** for agents and extensions Microsoft Learn: Auto-Provisioning
- [ ] **Enable Attack Disruption** with "Full - remediate threats automatically" Microsoft Learn: Attack Disruption
- [ ] **Review and remediate security recommendations** by risk priority Microsoft Learn: Recommendations
- [ ] **Configure security alerts and notifications** Microsoft Learn: Alerts

---

8. Microsoft 365 Email Security

Email Authentication (SPF, DKIM, DMARC)

- [ ] **Configure SPF record** for your domain with `-all` (hard fail) Microsoft Learn: SPF Setup
- [ ] **Enable DKIM signing** for all domains (disabled by default) Microsoft Learn: DKIM Setup
- [ ] **Implement DMARC** - Start with `p=none`, progress to `p=quarantine` then `p=reject` Microsoft Learn: DMARC Setup
- [ ] **Configure DKIM and SPF for third-party email services** (Mailchimp, Salesforce, etc.) Microsoft Learn: Third-Party Email
- [ ] **Use subdomains for bulk email services** to protect main domain reputation Microsoft Learn: Email Best Practices

Microsoft Defender for Office 365

- [ ] **Enable Safe Attachments** - Scan email attachments for malware Microsoft Learn: Safe Attachments
- [ ] **Enable Safe Links** - Scan URLs at time of click Microsoft Learn: Safe Links
- [ ] **Configure anti-phishing policies** with:
- [ ] Mailbox intelligence
- [ ] Impersonation protection
- [ ] Spoof intelligence Microsoft Learn: Anti-Phishing
- [ ] **Enable Zero-hour Auto Purge (ZAP)** for spam and malware Microsoft Learn: ZAP
- [ ] **Configure preset security policies** (Standard or Strict) Microsoft Learn: Preset Policies

Exchange Online Security

- [ ] **Disable automatic email forwarding** to external addresses Microsoft Learn: Mail Flow Rules
- [ ] **Enable mailbox auditing** (enabled by default since 2019) Microsoft Learn: Mailbox Auditing
- [ ] **Configure connection filtering** to block known malicious IPs Microsoft Learn: Connection Filtering

---

9. SharePoint & OneDrive Security

External Sharing Controls

- [ ] **Limit SharePoint external sharing** to:
- [ ] "Only people in your organization" OR
- [ ] "Existing guests" Microsoft Learn: Sharing Settings
- [ ] **Limit OneDrive external sharing** to same or more restrictive than SharePoint Microsoft Learn: OneDrive Sharing
- [ ] **Block sharing with specific domains** (competitors, high-risk countries) Microsoft Learn: Domain Restrictions
- [ ] **Set expiration dates** for guest access and sharing links Microsoft Learn: Guest Expiration
- [ ] **Disable anonymous sharing links** for sensitive sites Microsoft Learn: Anonymous Links

Access Controls

- [ ] **Configure restricted access control** to limit access to specific security groups Microsoft Learn: Restrict Access
- [ ] **Enable idle session sign-out** for SharePoint and OneDrive Microsoft Learn: Idle Timeout
- [ ] **Require managed devices** for access to sensitive data Microsoft Learn: Device Access

- [ ] **Configure Information Barriers** if needed for compliance Microsoft Learn: Info Barriers

Site Security

- [ ] **Apply sensitivity labels** to sites for automatic protection Microsoft Learn: Site Labels
- [ ] **Enable versioning** to protect against ransomware Microsoft Learn: Versioning
- [ ] **Configure site access requests** and approvals Microsoft Learn: Access Requests

---

10. Microsoft Teams Security

External & Guest Access

- [ ] **Review and configure external access settings** - Control federation with other organizations Microsoft Learn: External Access
- [ ] **Configure guest access policies** - Limit what guests can do Microsoft Learn: Guest Access
- [ ] **Block guest access** if not required by business Microsoft Learn: Guest Settings

Meeting Security

- [ ] **Configure meeting policies** to control who can present, record, etc. Microsoft Learn: Meeting Policies
- [ ] **Enable lobby** for external participants Microsoft Learn: Lobby
- [ ] **Disable anonymous meeting join** if not needed Microsoft Learn: Anonymous Join
- [ ] **Configure watermarking** for sensitive meetings (E5) Microsoft Learn: Watermarks

App & Bot Security

- [ ] **Control which apps can be installed** in Teams Microsoft Learn: App Policies
- [ ] **Block specific third-party apps** that pose security risks Microsoft Learn: Block Apps

---

11. Data Loss Prevention (DLP)

Policy Configuration

- [ ] **Create DLP policies** for sensitive information types:
- [ ] Credit card numbers
- [ ] Social Security Numbers
- [ ] Health records (HIPAA)
- [ ] Financial data
- [ ] Custom sensitive data Microsoft Learn: DLP Overview

- [ ] **Apply DLP to all locations:**
- [ ] Exchange Online
- [ ] SharePoint Online
- [ ] OneDrive
- [ ] Teams
- [ ] Endpoints (Windows/macOS)
- [ ] Microsoft 365 Copilot (new in 2025) Microsoft Learn: DLP Locations
- [ ] **Deploy policies in simulation mode first** before enforcement Microsoft Learn: Test Mode
- [ ] **Configure policy tips** to educate users Microsoft Learn: Policy Tips

Advanced DLP Features

- [ ] **Enable Adaptive Protection** integration with Insider Risk Management Microsoft Learn: Adaptive Protection
- [ ] **Configure DLP for Microsoft 365 Copilot** (new in 2025) Microsoft Learn: DLP for Copilot
- [ ] **Enable DLP for Windows Recall** on Copilot+ PCs Microsoft Learn: DLP for Recall

Sensitivity Labels

- [ ] **Create and publish sensitivity labels** for document classification Microsoft Learn: Sensitivity Labels
- [ ] **Configure automatic labeling** for sensitive content Microsoft Learn: Auto-Labeling
- [ ] **Enable label encryption** for highly confidential data Microsoft Learn: Label Encryption

---

12. Audit & Monitoring

Unified Audit Logging

- [ ] **Verify Unified Audit Logging is enabled** (default for most tenants) PowerShell: `Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled` Microsoft Learn: Enable Auditing
- [ ] **Understand retention periods:**
- [ ] E3/Business Premium: 180 days (changed from 90 days in Oct 2023)
- [ ] E5: 1 year default, extendable with retention policies Microsoft Learn: Audit Retention
- [ ] **Create custom audit log retention policies** for critical activities Microsoft Learn: Retention Policies
- [ ] **Monitor for audit logging being disabled** (indicator of compromise) Microsoft Learn: Search Audit Log

SIEM Integration

- [ ] **Forward logs to Azure Monitor / Log Analytics** Microsoft Learn: Azure Monitor
- [ ] **Configure Microsoft Sentinel** for advanced threat detection Microsoft Learn: Sentinel
- [ ] **Enable Office 365 connector** in Sentinel for M365 log ingestion Microsoft Learn: O365 Connector
- [ ] **Create detection rules** for suspicious activities Microsoft Learn: Analytics Rules

Alert Policies

- [ ] **Review and customize default alert policies** Microsoft Learn: Alert Policies
- [ ] **Create custom alerts** for organization-specific risks Microsoft Learn: Custom Alerts
- [ ] **Configure email notifications** for critical alerts Microsoft Learn: Notifications

---

13. Microsoft Secure Score

Monitoring

- [ ] **Access Secure Score** in Microsoft Defender portal Microsoft Secure Score
- [ ] **Target score above 80%** for strong security posture Microsoft Learn: Secure Score
- [ ] **Review score trends** over time using new trend chart feature (2025) Microsoft Learn: Track History

Focus Areas (2025 Categorization)

- [ ] **Identity** - MFA, Conditional Access, PIM
- [ ] **Device** - Compliance policies, Intune baselines, updates
- [ ] **Apps** - App protection, consent controls
- [ ] **Data** - DLP, sensitivity labels, encryption Microsoft Learn: Improvement Actions

High-Impact Actions

- [ ] **Implement all "High Impact" recommendations first** Microsoft Learn: Prioritization
- [ ] **Address identity-related recommendations** - Most impactful category Microsoft Learn: Identity Actions
- [ ] **Document score for cyber insurance** requirements (increasingly important in 2025) CoreView: Secure Score Playbook

---

14. CISA SCuBA Compliance

Overview

The Secure Cloud Business Applications (SCuBA) project provides secure configuration baselines for Microsoft 365. While mandatory for US federal agencies (BOD 25-01), all organizations can benefit from these baselines.

Compliance Deadlines (Federal Agencies): - February 21, 2025: Identify all Microsoft 365 cloud tenants - June 20, 2025: Implement SCuBA secure configuration baselines

SCuBA Baselines by Service

- [ ] **Microsoft Entra ID baseline** - Identity and access controls CISA: Entra ID Baseline
- [ ] **Microsoft Defender for Office 365 baseline** - Email protection CISA: Defender Baseline
- [ ] **Exchange Online baseline** - Mail flow and mailbox security CISA: Exchange Baseline
- [ ] **Microsoft Teams baseline** - Collaboration security CISA: Teams Baseline
- [ ] **SharePoint Online / OneDrive baseline** - File sharing security CISA: SharePoint Baseline
- [ ] **Power Platform baseline** - Low-code app security CISA: Power Platform Baseline

ScubaGear Assessment Tool

- [ ] **Install ScubaGear** from PowerShell Gallery: `powershell Install-Module -Name ScubaGear` GitHub: ScubaGear
- [ ] **Run assessment** against your tenant CISA: SCuBA Project
- [ ] **Review HTML/JSON/CSV reports** for compliance gaps CISA: Using ScubaGear
- [ ] **Remediate findings** based on priority and risk CISA: Baselines

---

Quick Reference: Key Resources

Resource	Link
Microsoft Entra Admin Center	https://entra.microsoft.com
Microsoft Defender Portal	https://security.microsoft.com
Microsoft Purview Portal	https://purview.microsoft.com
Azure Portal	https://portal.azure.com
Microsoft Secure Score	https://security.microsoft.com/securescore
CISA SCuBA Project	https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project

Resource	Link
ScubaGear GitHub	https://github.com/cisagov/ScubaGear
Microsoft Cloud Security Benchmark	https://learn.microsoft.com/en-us/security/benchmark/azure/overview
Microsoft Security Best Practices	https://learn.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns

Sources

This checklist was compiled from the following authoritative sources:

- Microsoft Learn - Security Best Practices and Patterns
- Microsoft Learn - Azure Identity & Access Security Best Practices
- Microsoft Learn - Best Practices to Secure with Microsoft Entra ID
- Microsoft Learn - Data Encryption Best Practices
- Microsoft Learn - Network Security Best Practices
- Microsoft Learn - Microsoft Defender for Cloud
- Microsoft Learn - Conditional Access
- Microsoft Learn - Email Authentication
- CISA - Secure Cloud Business Applications (SCuBA)
- CISA - Microsoft 365 Secure Configuration Baselines
- SentinelOne - Azure Security Best Practices 2026
- Netrix Global - Microsoft 365 Security Hardening Checklist
- CoreView - 2025 Microsoft Secure Score Playbook
- LA NET Azure - Microsoft Entra ID Security Baseline 2025
- Paradigm Security - Top 10 Conditional Access Policies 2025
- Jeffrey Appel - 2025 Microsoft Defender Optimization Cheat Sheet