

****

**May 2023**

**NICK ROSS**

**MICROSOFT 365**

**SECURITY BASELINES**

**Version 1.0**

Contents

[1.0 Introduction 6](#_Toc129503052)

[2.0 Azure Active Directory 8](#_Toc129503053)

[2.1 MFA Shall Be Required for All Users 8](#_Toc129503054)

[2.2 MFA is enforced on accounts with Highly Privileged Roles 15](#_Toc129503055)

[2.3 MFA is enforced for Azure Management 17](#_Toc129503056)

[2.4 MFA registration and usage shall be periodically reviewed 19](#_Toc129503057)

[2.5 Legacy Authentication shall be blocked 21](#_Toc129503058)

[2.6 High Risk Users Shall Be Blocked 23](#_Toc129503059)

[2.7 High Risk Sign-Ins Shall Be Blocked 26](#_Toc129503060)

[2.8 Browser Sessions shall not be persistent for privileged users 28](#_Toc129503061)

[2.9 MFA shall be required to enroll devices to Azure AD 30](#_Toc129503062)

[2.10 Managed Devices shall be required for authentication 32](#_Toc129503063)

[2.11 Guest User Access Shall be restricted 34](#_Toc129503064)

[2.12 The number of users with highly privileged roles shall be limited 37](#_Toc129503065)

[2.13 Users assigned highly privileged roles shall not have permanent permissions 39](#_Toc129503066)

[2.14 Activation of privileged roles should be monitored and require approval 41](#_Toc129503067)

[2.15 Highly privileged accounts shall be cloud-only 44](#_Toc129503068)

[2.16 Highly privileged role assignments shall be periodically reviewed 45](#_Toc129503069)

[2.17 Passwords shall not expire 47](#_Toc129503070)

[2.18 Azure AD Logs shall be collected 49](#_Toc129503071)

[2.19 Only Admins shall be allowed to register 3rd party applications 51](#_Toc129503072)

[2.20 Non-admin users shall be prevented from providing consent to 3rd party applications 53](#_Toc129503073)

[2.21 Authorized Applications shall be configured for Single Sign-On 55](#_Toc129503074)

[2.22 Inactive accounts shall be blocked or deleted 57](#_Toc129503075)

[3.0 Microsoft Teams 59](#_Toc129503076)

[3.1 Private Channels shall be utilized to restrict access to sensitive information 59](#_Toc129503077)

[3.2 External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings 61](#_Toc129503078)

[3.3 Anonymous Users SHALL NOT Be Enabled to Start Meetings 63](#_Toc129503079)

[3.4 Automatic Admittance to Meetings SHOULD Be Restricted 65](#_Toc129503080)

[3.5 External User Access SHALL Be Restricted 67](#_Toc129503081)

[3.6 Unmanaged User Access SHALL Be Restricted 69](#_Toc129503082)

[3.7 Contact with Skype Users SHALL Be Blocked 71](#_Toc129503083)

[3.8 Teams Email Integration SHALL Be Disabled 73](#_Toc129503084)

[3.9 Only Approved Apps SHOULD Be Installed 75](#_Toc129503085)

[3.10 File Sharing and File Storage Options shall be blocked 77](#_Toc129503086)

[3.11 Only the Meeting Organizer SHOULD Be Able to Record Live Events 79](#_Toc129503087)

[3.12 Data Loss Prevention Solutions SHALL Be Enabled 81](#_Toc129503088)

[3.13 Attachments SHOULD Be Scanned for Malware 83](#_Toc129503089)

[3.14 Link Protection SHOULD Be Enabled 85](#_Toc129503090)

[3.15 Restrict Users who can Create Teams Channels 87](#_Toc129503091)

[3.16 Teams Channels shall have an expiration policy 89](#_Toc129503092)

[4.0 Microsoft Exchange 91](#_Toc129503093)

[4.1 Automatic Forwarding to External Domains SHALL Be Disabled 91](#_Toc129503094)

[4.2 Sender Policy Framework SHALL Be Enabled 92](#_Toc129503095)

[4.3 DomainKeys Identified Mail SHOULD Be Enabled 94](#_Toc129503096)

[4.4 Domain-Based Message Authentication, Reporting, and Conformance SHALL Be Enabled 96](#_Toc129503097)

[4.5 Enable Email Encryption 98](#_Toc129503098)

[4.6 Simple Mail Transfer Protocol Authentication SHALL Be Disabled 100](#_Toc129503099)

[4.7 Calendar and Contact Sharing SHALL Be Restricted 102](#_Toc129503100)

[4.8 External Sender Warnings SHALL Be Implemented 104](#_Toc129503101)

[4.9 Data Loss Prevention Solutions SHALL Be Enabled 106](#_Toc129503102)

[4.10 Emails SHALL Be Filtered by Attachment File Type 108](#_Toc129503103)

[4.11 Zero-Hour Auto Purge for Malware SHOULD Be Enabled 110](#_Toc129503104)

[4.12 Phishing Protections SHOULD Be Enabled 112](#_Toc129503105)

[4.13 Inbound Anti-Spam Protections SHALL Be Enabled 115](#_Toc129503106)

[4.14 Safe Link Policies SHOULD Be Enabled 117](#_Toc129503107)

[4.15 Safe Attachments SHALL Be Enabled 120](#_Toc129503108)

[4.16 IP Allow Lists SHOULD NOT be Implemented 122](#_Toc129503109)

[4.17 Mailbox Auditing SHALL Be Enabled 124](#_Toc129503110)

[4.18 Alerts SHALL Be Enabled 126](#_Toc129503111)

[4.19 Audit Logging SHALL Be Enabled 128](#_Toc129503112)

[4.20 Enhanced Filtering Shall be configured if a 3rd party email filtering tool is being used 130](#_Toc129503113)

[5.0 SharePoint Online 132](#_Toc129503114)

[5.1 File and Folder Links Default Sharing Settings SHALL Be Set to "Specific People (Only the People the User Specifies)" 132](#_Toc129503115)

[5.2 External Sharing SHOULD be Set to “New and Existing Guests” and Managed Through Approved Domains and/or Security Groups Per Interagency Collaboration Needs. 135](#_Toc129503116)

[5.3 Sensitive SharePoint Sites SHOULD Adjust Their Default Sharing Settings to Those Best Aligning to Their Sensitivity Level 137](#_Toc129503117)

[5.4 Expiration Times for Guest Access to a Site or OneDrive, and Reauthentication Expiration Times for People Who Use a Verification Code, SHOULD Be Determined by specific needs or Else Defaulted to 30 Days 139](#_Toc129503118)

[5.5 Users SHALL Be Prevented from Running Custom Scripts 141](#_Toc129503119)

[6.0 OneDrive 143](#_Toc129503120)

[6.1 Anyone Links SHOULD Be Turned Off 143](#_Toc129503121)

[6.2 Expiration Date SHOULD Be Set for Anyone Links 145](#_Toc129503122)

[6.3 Link Permissions SHOULD Be Set to Enabled Anyone Links to View 146](#_Toc129503123)

[6.4 OneDrive Client SHALL Be Restricted to corporate owned devices 148](#_Toc129503124)

[6.5 Legacy Authentication SHALL Be Blocked 150](#_Toc129503125)

[7.0 Intune 152](#_Toc129503126)

[7.1 Personal Devices should be restricted from enrolling into the MDM solution 152](#_Toc129503127)

[7.2 Devices shall be deleted that haven’t checked in for over 30 days 154](#_Toc129503128)

[7.3 Devices compliance policies shall be configured for every supported device platform 156](#_Toc129503129)

[7.4 Noncompliant devices shall be blocked from accessing corporate resources. 159](#_Toc129503130)

[7.5 MFA Shall be required for Intune Enrollment 163](#_Toc129503131)

[7.6 Security Baselines should be configured for Windows Devices 165](#_Toc129503132)

[7.7 Windows Update Rings shall be configured for Windows Devices 167](#_Toc129503133)

[7.8 Update Policies shall be configured for Apple Devices 170](#_Toc129503134)

[7.9 App Protection policies should be created for mobile devices 173](#_Toc129503135)

[7.10 Mobile devices shall only be able to access corporate data through approved client apps 176](#_Toc129503136)

[7.11 Lockout screen and password settings shall be configured for each device 178](#_Toc129503137)

[7.12 Encryption shall be required on all devices 181](#_Toc129503138)

[7.13 Windows Hello for Business should be configured where applicable 184](#_Toc129503139)

[7.14 Authorized Applications should be deployed to managed devices 186](#_Toc129503140)

[7.15 Device Use Shall be restricted until required applications are installed 188](#_Toc129503141)

[7.16 Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device 190](#_Toc129503142)

[Bonus: Review CIS Microsoft Intune Benchmarks 192](#_Toc129503143)

[Appendix 193](#_Toc129503144)

[Customer Checklist 193](#_Toc129503145)

[CIS Control Mappings 193](#_Toc129503146)

# 1.0 Introduction

1.1

About the Author



My name is Nick Ross and I have been publishing educational Microsoft Content for over 3 years now. I have been helping IT Admins architect Microsoft 365 solutions for 6 years and I am a Microsoft MVP. I have a [YouTube channel](https://www.youtube.com/channel/UCePaXDDk5kl3g7FcJ5gH5AQ/) called T-minus365 where I post new educational videos weekly, primarily for Managed Service Providers (MSPs).

1.2

Format

The document contains sections for each of the key Microsoft 365 Product offerings. Each section contains the following format:

* Control Summary
* Policy Definition
* Licensing Considerations
* Set up instructions.
* End-User Impact/Notifications
* Tips
* PowerShell Scripts
* Video Demonstrations

Compliance Mappings and Customer checklist can be found in the Appendix section.



If you are looking for a more detailed License Consideration breakdown, check out the free feature matrix here: [Feature Matrix | M365 Maps](https://m365maps.com/matrix.htm)

**Updates**

I will be reviewing this document on a quarterly basis for updates. [Subscribe to my monthly newsletter](https://tminus365.com/) (right hand nav) if you’d like to receive updates to the documentation.

1.3

Disclaimer

License Compliance and Copyright. This document is expanding off of the [Secure Cloud Business applications (SCuBA)](https://www.cisa.gov/sites/default/files/publications/FINAL-CSSO_SCuBA_Fact_Sheet.pdf) project from the Cybersecurity & Infrastructure Security Agency (CISA). Many of the recommendations made from that project are replicated in this document and have additions outlined in the format section (1.2). Portions of this document are adapted from documents in Microsoft 365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The recommendations and mapping of compliance controls provided in this article are for informational purposes only and should not be considered legal advice or a substitute for professional judgment.



# 2.0 Azure Active Directory

## 2.1 MFA Shall Be Required for All Users

MFA, or multi-factor authentication, is a security measure that requires users to provide multiple forms of identification to gain access to a system or network. By enforcing MFA within an organization, companies can better protect themselves against cyber threats, such as hacking and identity theft.

At a minimum, users with **privileged roles** such as Global Administrators should have MFA enforced. Where possible, **phishing-resistant MFA** should be required for all users. Phishing-resistant multifactor authentication protects against sophisticated phishing attacks. Phishing-resistant MFA may not always be immediately available, especially on mobile devices. Where phishing-resistant MFA is not yet available, organization should adopt an MFA method from the list below.



Microsoft also encourages a **break-glass account** to ensure that you are not accidently locked out of your organization. These accounts are referred to as emergency access accounts and should be excluded from MFA enforcement.

MFA can be enforced with per user settings, Conditional Access Policies, or Security Defaults. **Per user settings will be deprecated in January of 2024**. Since February of 2022, Security Defaults are enabled on all new tenants which requires MFA for all users. Security defaults are NOT a hard requirement for non-partner tenants but are recommended. If you have a tenant licensed with conditional access, it is recommended that you enforce conditional access policies instead of security defaults.

**2.1.1**

**Policy**

* MFA is enforced for all users
* Phishing Resistant MFA is enforced for all users
* If phishing Resistant MFA cannot be used, and MFA method from the list below shall be used temporarily:
	+ Microsoft Authenticator (Push Notifications)
	+ Microsoft Authenticator (Passwordless-SignIn)
		- While using Microsoft Authenticator:
			* Number Matching shall be enabled
			* Geolocation shall be enabled
	+ Software Tokens One-Time Password (OTP) – This option is commonly implemented using mobile phone authenticator apps.
	+ Hardware tokens OTP
* SMS and Voice shall not be used as the MFA method
* One emergency, break-glass account shall be created and excluded from MFA enforcement
* Accounts excluded from MFA shall be documented and include a justification reason

**2.1.2**

**Licensing Considerations**

Enforcing MFA through conditional access requires an Azure AD P1 license which can be purchased standalone or through the following common plans:

* + Microsoft 365 Business Premium
	+ EMS + E3 or EMS + E5
	+ Microsoft 365 E3
	+ Microsoft 365 E5
* OATH Hardware Tokens require Azure AD P1 or P2 Licensing
* Enforcing MFA per user or through Security Defaults is available through all Microsoft Licensing Plans

**2.1.3**

**Set-Up Instructions**

* Requiring All users to have MFA through conditional Access: [Require MFA for all users with Conditional Access - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa)
* Security Defaults in Azure AD: [Providing a default level of security in Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults)
* Legacy Per user MFA: [Enable per-user Multi-Factor Authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates)
* Migrating from Legacy Per User Settings: [How to migrate to the Authentication methods policy - Azure Active Directory (preview) - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-authentication-methods-manage)
* Phishing Resistant MFA:
	+ FIDO2 Security Key: [Passwordless security key sign-in - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key#fido-security-key-optional-settings)
	+ Certificate Based Authentication: [How to configure Azure AD certificate-based authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-certificate-based-authentication#steps-to-configure-and-test-azure-ad-cba)
	+ Windows Hello for Business: [How to configure Azure AD certificate-based authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-certificate-based-authentication#steps-to-configure-and-test-azure-ad-cba)
* Password Less Sign In with Microsoft Authenticator: [Passwordless sign-in with Microsoft Authenticator - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone)
* Using Number matching: [Use number matching in multifactor authentication (MFA) notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match)
* Using Geolocation: [Use additional context in Microsoft Authenticator notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context)
* What Authentication methods are available in AAD: [Authentication methods and features - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods)

**Enable Microsoft Authenticator**

1. In the Azure Portal navigate to **Azure Active Directory**.
2. Select **Security**.
3. Select **Manage** -> **MFA**.
4. Under Configure, select **Additional cloud-based MFA settings**.
5. Under verification options, select **Notification through mobile app**.
6. If desired, to enforce Microsoft Authenticator app usage and disable third party authenticator apps usage, make sure that Verification code from mobile app or hardware token is not selected.
7. Click **Save**.
8. Go back to the Azure Active Directory home tab and select **Security**.
9. Select **Authentication Methods**.
10. In the Policies window, select **Microsoft Authenticator**.
11. For Enable, select **Yes.**
12. For Target, select **All users**.
13. In the row for the All users, click the … -> Configure.
14. If configuring Phone Sign-in (aka Passwordless Sign-in), for Authentication mode, select Passwordless. If configuring Push Notifications, for Authentication mode, select Push. If configuring the usage of both, for Authentication mode, select Any.
	1. For Require number matching, select Enabled.
	2. For Show additional context in notifications, select Enabled.
15. Select Done.
16. Click Save

**Software Tokens OTP or Hardware Tokens OTP**

1. In the Azure Portal, navigate to **Azure Active Directory**.
2. Select **Security**.
3. Select Manage -> **MFA**.
4. Under Configure, select **Additional cloud-based MFA settings**.
5. Under verification options, select **Verification code from mobile app or hardware token**.
6. If configuring Hardware Tokens OTP, follow the additional steps at [this link](https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens#oath-hardware-tokens-preview) when provisioning a user.

**Disabling SMS and Voice**

1. In the Azure Portal, navigate to **Azure Active Directory**.
2. Select **Security**.
3. Select Manage -> **MFA**.
4. Under Configure, select **Additional cloud-based MFA settings**.
5. Under verification options, make sure that **Text message to phone and Call to phone are disabled**.

**2.1.4**

**End-User Impact**

Level: High

End-User impact is high due to the necessary configuration steps along and prompts to fulfill MFA request. The user experience will vary depending on which MFA methods you have set up. Below you will find links to end-user communication templates that help for various rollout scenarios.

[End-User Notifications](https://tminus365com.sharepoint.com/%3Af%3A/s/M365/Egp_e1bCckxMp_PvcdSZRqEBGCH-1Tjq3n17OTRrkwVjCQ?e=zIA13S)



* Included in the End-User Notifications:
	+ Authenticator Setup
	+ Passwordless Updates
	+ MFA drip:
		- MFA Coming Soon
		- MFA Action Required
		- MFA is Here
		- MFA Reminder
	+ MFA Number Match
		- Overview
		- Nudge
		- Helpdesk
	+ MFA + Self-Service Password Reset
	+ FIDO2 Security Key
	+ FIDO2 Security Key + Temporary access pass
	+ Enabling Registration Campaign: [Nudge users to set up Microsoft Authenticator - Azure Active Directory - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign#user-experience)

**2.1.5**

**Tips**

* Create a group in Azure Active Directory used to place all accounts excluded from MFA. This would be your emergency break-glass account and service accounts such as the Azure AD Connect sync service account (if you are running a hybrid environment).
* If you are not able to enforce phishing-resistant MFA across all users, at minimum try to enable it for accounts with privileged roles (Global Admins, User Admins, etc.)

**2.1.6**

**PowerShell Scripts**

* Per User MFA: [Security/Enable MFA.ps1 at master · msp4msps/Security (github.com)](https://github.com/msp4msps/Security/blob/master/Enable%20MFA.ps1)
* Convert from per-user MFA to Conditional Access MFA: [Move from per-user MFA to Conditional Access MFA - ALI TAJRAN](https://www.alitajran.com/move-from-per-user-mfa-to-conditional-access-mfa/#:~:text=Convert%20per-user%20MFA%20to%20Conditional%20Access%20based%20MFA,script%20and%20place%20it%20in%20the%20C%3Ascripts%20folder.)
* MFA Status Reporting (Multi-tenant): [Security/MFA Status\_Custom Control\_All Customers.ps1 at master · msp4msps/Security (github.com)](https://github.com/msp4msps/Security/blob/master/MFA%20Status_Custom%20Control_All%20Customers.ps1)
* [Monitoring with PowerShell: Monitoring the used MFA type for O365/Azure. (cyberdrain.com)](https://www.cyberdrain.com/monitoring-with-powershell-monitoring-the-used-mfa-type-for-o365-azure/)

**2.1.7**

**Videos**

* MFA Settings in Azure AD: [(5) 5 MFA Settings in Azure AD You Probably Don't Know About | Cloud Security - YouTube](https://www.youtube.com/watch?v=k0uHPT7pBRs)
* Creating CAP For MFA: <https://www.youtube.com/watch?v=lU6OfJT57l8&t>
* Stronger Azure AD Authentication: <https://www.youtube.com/watch?v=ns_94ZXrbPI&t>

## 2.2 MFA is enforced on accounts with Highly Privileged Roles

Require users to perform MFA to access highly privileged roles. This configuration provides a backup policy to enforce MFA for highly privileged users in case the main conditional access policy—which requires MFA for all users—is disabled or misconfigured.

**2.2.1**

**Policy**

* MFA shall be required for users to access highly privileged roles
* Highly Privileged roles include the following:
	+ Global Administrator
	+ Privileged Role Administrator
	+ User Administrator
	+ SharePoint Administrator
	+ Exchange Administrator
	+ Hybrid Identity Administrator
	+ Application Administrator
	+ Teams Administrator
* One emergency access account shall be excluded from the MFA policy

**2.2.2**

**Licensing Considerations**

* Enforcing MFA for privileged roles through conditional access requires an Azure AD P1 license which can be purchased standalone or through the following common plans:
	+ Microsoft 365 Business Premium
	+ EMS + E3 or EMS + E5
	+ Microsoft 365 E3
	+ Microsoft 365 E5

**2.2.3**

**Set-Up Instructions**

1. Create a Conditional Access Policy with the [Templates available](https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common#conditional-access-templates-preview)

2. Chose the “Require Multi-Factor authentication for Admins” setting

3. Modify the policy to ensure your emergency access user/group is excluded

**2.2.4**

**End-User Impact**

Level: Low

End-User impact is low due to this policy scoped to a small set of users. The end-user experience is the same as the previous section (2.1.4). The user experience will vary depending on which MFA methods you have set up. Below you will find links to end-user communication templates that help for various rollout scenarios.

[End-User Notifications](https://tminus365com.sharepoint.com/%3Af%3A/s/M365/Egp_e1bCckxMp_PvcdSZRqEBGCH-1Tjq3n17OTRrkwVjCQ?e=zIA13S)

**2.2.5**

**Tips**

* Create a group in Azure Active Directory used to place all accounts excluded from MFA. This would be your emergency break-glass account and a service accounts such as the Azure AD Connect sync service account.
* If you are able to enforce phishing-resistant MFA across all users, at minimum try to enable it for accounts with privileged roles (Global Admins, User Admins, etc.)
* Turn the Conditional Access Policy to “Report-Only” mode to get information around how many users in the organization this will impact before turning the policy on.

**2.2.6**

**PowerShell Scripts**

* Viewing Global Admins without MFA: [Security/Customer-Global Admin without MFA.ps1 at master · msp4msps/Security (github.com)](https://github.com/msp4msps/Security/blob/master/Customer-Global%20Admin%20without%20MFA.ps1)
* Conditional Access Policies as Code: [Azure-Samples/azure-ad-conditional-access-apis: Use Conditional Access Graph APIs to manage policies like code. Automate approvals to promote policies from preproduction environments, backup and restore, monitor change, and plan ahead for emergencies. (github.com)](https://github.com/Azure-Samples/azure-ad-conditional-access-apis)

**2.2.7**

**Videos**

* Creating CAP For MFA: <https://www.youtube.com/watch?v=lU6OfJT57l8&t>