T-MINUS 365

MICROSOFT 365

SECURITY BASELINES

Version 1.0

March 2023

NICK ROSS

Microsoft® MVP Most Valuable Professional

Contents

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 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

Customer checklist can be found in the Appendix section.

Configured	Policy #	Policy	Importance	License	End User Impact	CIS Control	Asset Type	Security Function	IG1	IG2	IG3
Not Selected	7.1	Personal Devices should be restricted from enrolling into the MDM solution	High	Intune	Medium	1.2 Address Unauthoriz	Devices	Repsond	X	X	X
Not Selected	7.2	Devices shall be deleted that haven't checked in for over 30 days	Low	Intune	Low	1.1 Establish and Maint	Devices	Identify	X	X	X
Not Selected	7.3	Devices compliance policies shall be configured for every supported device platform	High	Intune	Medium	4.1 Establish and Maint	Devices	Protect	X	X	X
Not Selected	7.4	Noncompliant devices shall be blocked from accessing corporate resources.	High	Azure AD P1	High	6.2 Establish An Access	Devices	Protect	X	X	X
Not Selected	7.5	MFA Shall be required for Intune Enrollment	Medium	Azure AD P1	Medium	6.4 Require MFA for Rer	Devices	Protect	X	X	X
Not Selected	7.6	Security Baselines should be configured for Windows Devices	Medium	Intune	Medium	4.1 Establish and Maint	Devices	Protect	X	X	X
Not Selected	7.7	Windows Update Rings shall be configured for Windows Devices	High	Intune	Medium	7.3 Perform Automated	Devices	Protect	X	X	X
Not Selected	7.8	Update Policies shall be configured for Apple Devices	High	Intune	Medium	7.3 Perform Automated	Devices	Protect	X	X	X
Not Selected	7.9	App Protection policies should be created for mobile devices	Medium	Intune	Medium	4.12 Separate Enterprise	Devices	Protect			X
Not Selected	7.10	Mobile devices shall only be able to access corporate data through approved client apps	Medium	Azure AD P1	Medium	2.5 Allowlist Authorizec	Devices	Protect		X	X
Not Selected	7.11	Lockout screen and password settings shall be configured for each device	High	Intune	Medium	4.3 Configure Automati	Devices	Protect	X	X	X
Not Selected	7.12	Encryption shall be required on all devices	High	Intune	Medium	3.6 Encrpyt Data on End-	Devices	Protect	X	X	X
Not Selected	7.13	Windows Hello for Business should be configured where applicable	Medium	Intune	Low	6.6 Establish and Maint	Devices	Identify		X	X
Not Selected	7.14	Authorized Applications should be deployed to managed devices	Medium	Intune	Low	2.1 Establish and Maint	Devices	Identify	X	X	X
Not Selected	7.15	Device Use Shall be restricted until required applications are installed	Medium	Intune	Medium	4.1 Establish and Maint	Devices	Protect	X	X	X
Not Selected	7.16	Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device	High	Intune	None	4.11 Enforce Remote Wi	Devices	Protect	X	X	X

If you are looking for a more detailed License Consideration breakdown, check out the free feature matrix here: Feature Matrix | M365 Maps

Updates

I will be reviewing this document on a quarterly basis for updates. Subscribe to my monthly newsletter (right hand nav) if you'd like to receive updates to the documentation.

1.3

Disclaimer

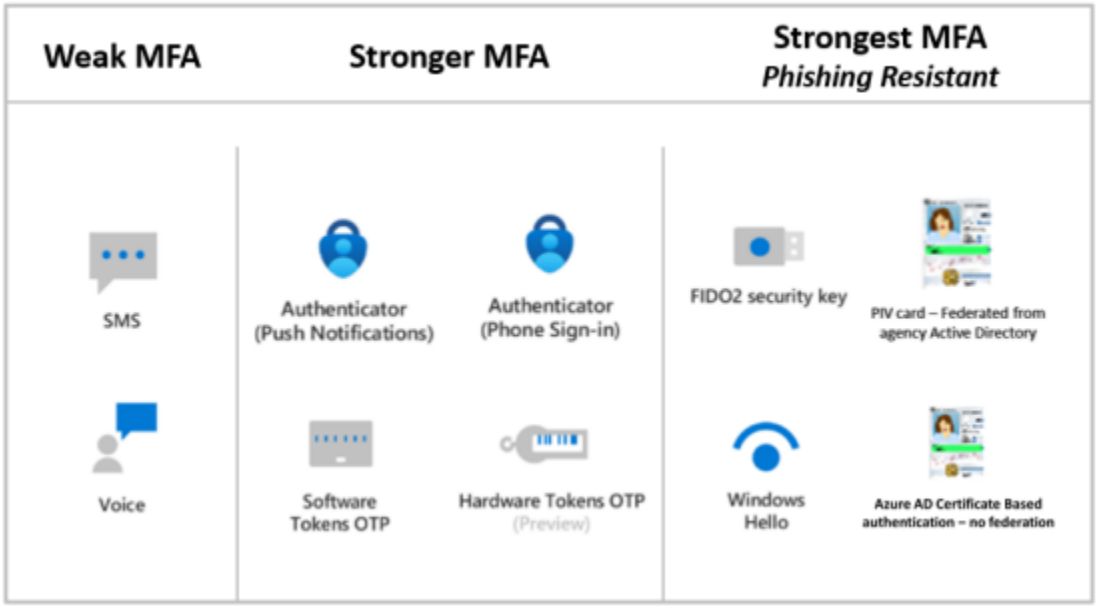
License Compliance and Copyright. This document is expanding off of the Secure Cloud Business applications (SCuBA) project from the Cybersecurity & Infrastructure Security Agency (CISA). Many of the recommendations made from that project are replicated in this document and have additions outlined in 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
- Security Defaults in Azure AD: Providing a default level of security in Azure Active Directory - Microsoft Entra | Microsoft Learn
- Legacy Per user MFA: Enable per-user Multi-Factor Authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Migrating from Legacy Per User Settings: How to migrate to the Authentication methods policy - Azure Active Directory (preview) - Microsoft Entra | Microsoft Learn
- Phishing Resistant MFA:
  - FIDO2 Security Key: Passwordless security key sign-in - Azure Active Directory - Microsoft Entra | Microsoft Learn
  - Certificate Based Authentication: How to configure Azure AD certificate-based authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn
  - Windows Hello for Business: How to configure Azure AD certificate-based authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Password Less Sign In with Microsoft Authenticator: Passwordless sign-in with Microsoft Authenticator - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Using Number matching: Use number matching in multifactor authentication (MFA) notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Using Geolocation: Use additional context in Microsoft Authenticator notifications - Azure Active Directory - Microsoft Entra | Microsoft Learn
- What Authentication methods are available in AAD: Authentication methods and features - Azure Active Directory - Microsoft Entra | Microsoft Learn

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.
    a. For Require number matching, select Enabled.
    b. 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 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**.

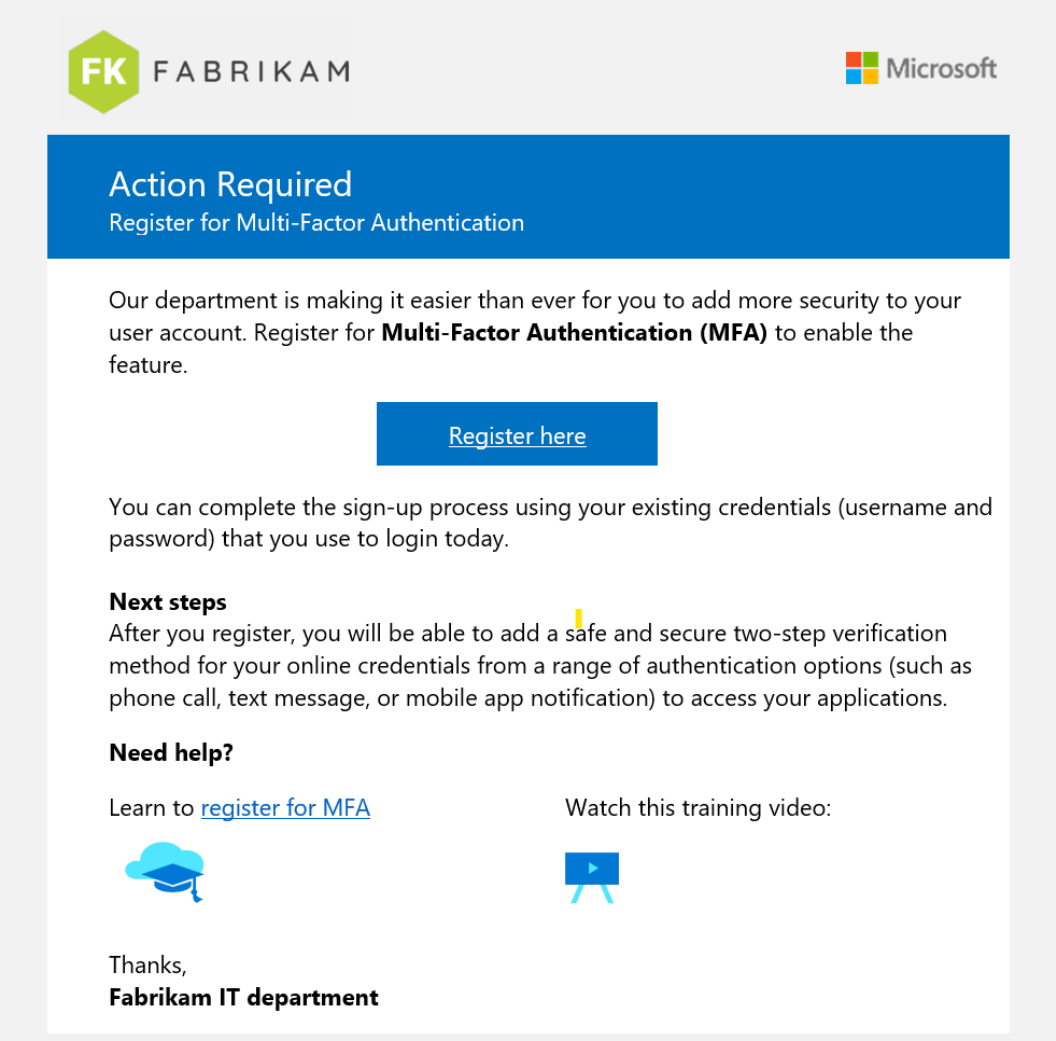
2.1.4

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



FABRIKAM

Microsoft

Action Required

Register for Multi-Factor Authentication

Our department is making it easier than ever for you to add more security to your user account. Register for **Multi-Factor Authentication (MFA)** to enable the feature.

Register here

You can complete the sign-up process using your existing credentials (username and password) that you use to login today.

Next steps

After you register, you will be able to add a safe and secure two-step verification method for your online credentials from a range of authentication options (such as phone call, text message, or mobile app notification) to access your applications.

Need help?

Learn to register for MFA

Watch this training video:

Thanks,

Fabrikam IT department

- 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

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)
- Convert from per-user MFA to Conditional Access MFA: Move from per-user MFA to Conditional Access MFA - ALI TAJRAN
- MFA Status Reporting (Multi-tenant): Security/MFA Status_Custom Control_All Customers.ps1 at master · msp4msps/Security (github.com)
- Monitoring with PowerShell: Monitoring the used MFA type for O365/Azure. (cyberdrain.com)

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
- 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

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

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)
- 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)

2.2.7

Videos

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

2.3 MFA is enforced for Azure Management

Organizations use many Azure services and manage them from Azure Resource Manager based tools like:

- Azure portal
- Azure PowerShell
- Azure CLI

These tools can provide highly privileged access to resources that can make the following changes:

- Alter subscription-wide configurations
- Service settings
- Subscription billing

To protect these privileged resources, Microsoft recommends requiring multifactor authentication for any user accessing these resources. This configuration provides a backup policy to enforce MFA for users accessing Azure Resources in case the main conditional access policy—which requires MFA for all users—is disabled or misconfigured.

2.3.1

Policy

- MFA shall be required for users to access Azure Resources
- One emergency access account shall be excluded from the MFA policy

2.3.2

Licensing Considerations

- Enforcing MFA for Azure Management 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

2.3.3

Set-Up Instructions

1. Create a Conditional Access Policy with the Templates available

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

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

2.3.4

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

2.3.5

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.
- 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.

2.3.6

PowerShell Scripts

- 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)

2.3.7

Videos

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

2.4 MFA registration and usage shall be periodically reviewed

MFA registration should periodically be reviewed to ensure that there are no gaps or misconfigurations of deployment. MFA can be monitored natively within Azure Active Directory or with 3rd party tools.

2.4.1

Policy

- MFA registration details and usage shall be monitored on a defined schedule.

2.4.2

Licensing Considerations

Viewing Authentication Activity in Azure AD 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

MFA reports can also be derived from PowerShell which does not require an Azure AD P1 license and can be used with any Microsoft licensing model

2.4.3

Set-Up Instructions

- To view the Authentication Activity: Authentication Methods Activity - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Using the Azure AD sign-ins report: Sign-in event details for Azure AD Multi-Factor Authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Usage Graph API: List credentialUserRegistrationDetails - Microsoft Graph beta | Microsoft Learn

2.4.4

End-User Impact

Level: None

There is no end-user impact when looking at log information or reports on MFA.

2.4.5

Tips

- Try to review this information at least quarterly
- The registration and reset events of the Authentication methods section can also be used to investigate potential post-breach activity. Attackers sometimes reset MFA registration methods after accessing a compromised account.

2.4.6

PowerShell Scripts

- MFA Status Reporting (Multi-tenant): Security/MFA Status_Custom Control_All Customers.ps1 at master · msp4msps/Security (github.com)
- Find Global Admins without MFA: Security/Customer-Global Admin without MFA.ps1 at master · msp4msps/Security (github.com)

2.4.7

Videos

- MFA Settings in Azure AD: (5) 5 MFA Settings in Azure AD You Probably Don't Know About | Cloud Security - YouTube

2.5 Legacy Authentication shall be blocked

Block legacy authentication protocols using a conditional access policy. Legacy authentication does not support multifactor authentication (MFA), which is required to minimize the impact of user credential theft.

2.5.1

Policy

Legacy Authentication shall be blocked.

2.5.2

Licensing Considerations

Enabling a conditional access policy to block legacy authentication 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

2.5.3

Set-Up Instructions

1. Before enabling the policy, you can review if there is any authentication in use.

2. Create a Conditional Access Policy with the Templates available

3. Chose the “Block Legacy Authentication” setting

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

2.5.4

End-User Impact

Level: Medium

The level of impact here will vary by organization depending on the use of legacy authentication. It is possible there will be no impact at all if no legacy authentication protocols are in use. If there are some in use like IMAP/POP, there would be significant end-user impact. Its best to leverage the sign-in logs as mentioned in 2.4

to identify any legacy authentication present and take proactive steps on remediation.

End User Notification

2.5.5

Tips

- 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.
- Viewing legacy auth sign-ins within Azure AD: Identify legacy authentication use – Practice Protect Support

2.5.6

PowerShell Scripts

- Basic Auth Reporting msp4msps/Basic-Authentication-Reporting (github.com)

2.5.7

Videos

- Blocking Legacy Auth with Conditional Access: https://www.youtube.com/watch?v=mb7At6B_8p0&t
- Automating Basic Auth Reporting: Automating Basic Auth Reporting - YouTube

2.6 High Risk Users Shall Be Blocked

Azure AD Identity Protection uses various signals to detect the risk level for each user and determine if an account has likely been compromised. Users who are determined to be high risk are to be blocked from accessing the system via Conditional Access until an administrator remediates their account.

2.6.1

Policy

- Users detected as high risk shall be blocked.
- Notifications will be sent to admins when high-risk users are detected.

2.6.2

Licensing Considerations

Azure AD P2. Can be purchased standalone or part of the following bundles:

- EMS + E5
- Microsoft 365 E3
- Microsoft 365 E5

2.6.3

Set-Up Instructions

1. Create a conditional access policy for Sign-In risk: Risk policies - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

2. Under Access Controls> Grant, select Block Access

3. To Create notifications for admins: Azure Active Directory Identity Protection notifications - Microsoft Entra | Microsoft Learn

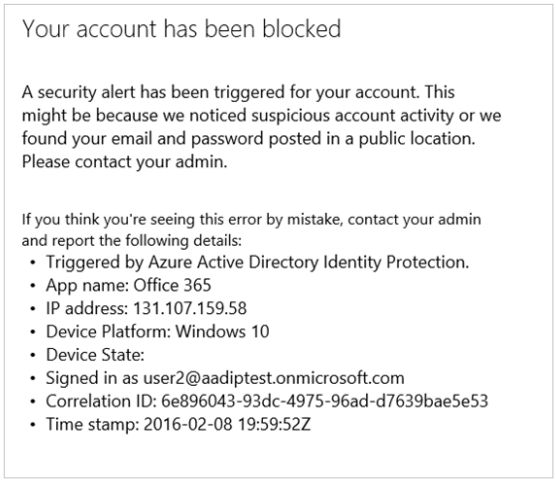
Identity Protection Overview: Azure Active Directory Identity Protection notifications - Microsoft Entra | Microsoft Learn

2.6.4

End-User Impact

Level: High

Once a respective conditional access policy is implemented, if a high-risk user attempts to login, the user will receive an error message with instructions to contact the administrator to re-enable their access.


Your account has been blocked

A security alert has been triggered for your account. This might be because we noticed suspicious account activity or we found your email and password posted in a public location. Please contact your admin.

If you think you're seeing this error by mistake, contact your admin and report the following details:

- Triggered by Azure Active Directory Identity Protection.
- App name: Office 365
- IP address: 131.107.159.58
- Device Platform: Windows 10
- Device State:
- Signed in as user2@aadiptest.onmicrosoft.com
- Correlation ID: 6e896043-93dc-4975-96ad-d7639bae5e53
- Time stamp: 2016-02-08 19:59:52Z

End User Notification Template

2.6.5

Tips

- Integrate the notifications into your ticketing system vs a single administrator.
- Investigate the risk event following these steps: Investigate risk Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

2.6.6

PowerShell Scripts

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)

2.6.7

Videos

- Creating Tickets for Azure AD Risky Users | Power Automate - YouTube
- Identity Protection Deep Dive: Microsoft Azure AD Identity Protection Deep Dive - YouTube
- Azure AD Identity Protection Demo - YouTube

2.7 High Risk Sign-Ins Shall Be Blocked

Azure AD Identity Protection uses various signals to detect the risk level for each user sign-in. Sign-ins detected as high risk are to be blocked via Conditional Access.

2.7.1

Policy

- Sign-Ins detected as high risk shall be blocked.
- Notifications will be sent to admins when high-risk sign-ins are detected.

2.7.2

Licensing Considerations

Azure AD P2. Can be purchased standalone or part of the following bundles:

- EMS + E5
- Microsoft 365 E3
- Microsoft 365 E5

2.7.3

Set-Up Instructions

1. Create a conditional access policy for Sign-In risk: Sign-in risk-based multifactor authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn

2. Under Access Controls> Grant, select Block Access

3. To Create notifications for admins: Azure Active Directory Identity Protection notifications - Microsoft Entra | Microsoft Learn

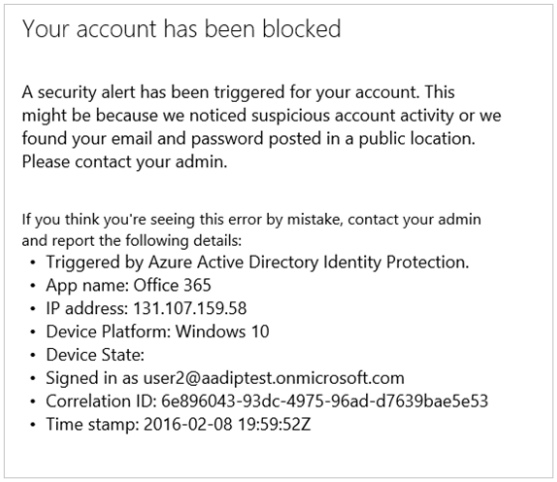
Identity Protection Overview: Azure Active Directory Identity Protection notifications - Microsoft Entra | Microsoft Learn

2.7.4

End-User Impact

Level: High

Once a respective conditional access policy is implemented, if a user attempts to login and their sign-in is seen as high-risk, the user will receive an error message with instructions to contact the administrator to re-enable their access.



End User Notification Template

If after implementing this, it is observed that numerous legitimate user sign-ins are consistently being blocked due to their location being interpreted as suspicious and this creates an operational burden on the agency, then a Trusted Location can be configured in the Conditional Access blade for each of the legitimate sign-in locations. Azure AD Identity Protection considers the Trusted Location data when it calculates sign-in risk, and this may help to prevent users signing in from legitimate locations from being flagged as high risk.

2.7.5

Tips

- Investigate the risk event following these steps: Investigate risk Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn

2.7.6

PowerShell Scripts

- None Currently

2.7.7

Videos

- Identity Protection Deep Dive: Microsoft Azure AD Identity Protection Deep Dive - YouTube

2.8 Browser Sessions shall not be persistent for privileged users

To reduce the risk of credential theft during user sessions, disallow persistent browser sessions for highly privileged users.

2.8.1

Policy

- Highly privileged users shall not have persistent browser sessions.

2.8.2

Licensing Considerations

Azure AD P1. Can be purchased standalone or part of the following bundles:

- Microsoft 365 Business Premium
- EMS +E3/ E5
- Microsoft 365 E3
- Microsoft 365 E5

2.8.3

Set-Up Instructions

1. Create a conditional access policy for Persistent Browser sessions: Configure authentication session management - Azure Active Directory - Microsoft Entra | Microsoft Learn

2. Under Users>Include<Select Users and Groups, choose Directory Roles.

3. Configure highly privileged Directory Roles

2.8.4

End-User Impact

Level: Medium

Since this will be only scoped to privileged roles, the impact will be limited. The severity of impact is increased to medium since it does require the scoped users to reauthenticate once every time the user closes and reopens the browser.

2.8.5

Tips

- This is a policy that you could scope additionally to guest users and for external access on personal devices that are not MDM or MAM enrolled.

2.8.6

PowerShell Scripts

- None currently

2.8.7

Videos

- None currently

2.9 MFA shall be required to enroll devices to Azure AD

It is recommended to enforce MFA before a user can register or join their device to Azure AD. This ensures that compromised accounts cannot be used to add rogue devices to Azure Active Directory.

2.9.1

Policy

- MFA shall be required to enroll devices to Azure AD.

2.9.2

Licensing Considerations

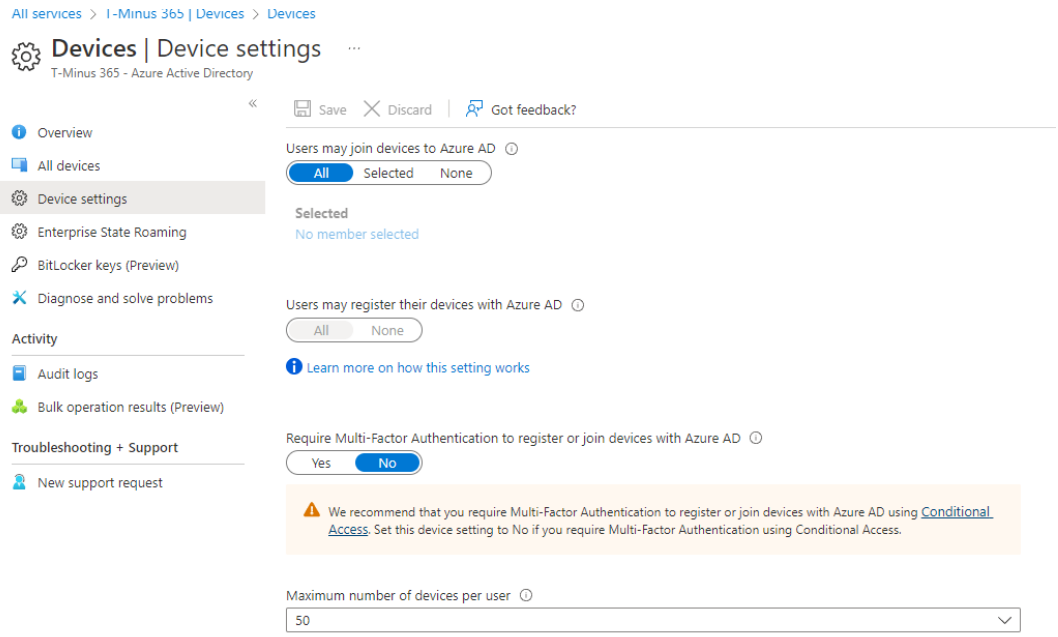
This setting can be configured manually in all tenants via the Azure AD Portal. To enable this setting via Conditional Access, an Azure AD P1 license is required. Can be purchased standalone or part of the following bundles:

  - Microsoft 365 Business Premium
  - EMS +E3/ E5
  - Microsoft 365 E3
  - Microsoft 365 E5

2.9.3

Set-Up Instructions

1. In the Azure AD admin center, go to Devices>Device Settings, and change the “Require Multi-Factor Authentication to register or join devices with Azure AD” to Yes



2. Create a conditional access policy. Under Cloud Apps or actions, select User Actions from the dropdown

3. Checkmark the Register or Join Devices options

4. Under the grant controls, select Require Multifactor Authentication

2.9.4

End-User Impact

Level: Medium

Users will get prompted with MFA when trying to register or join devices to Azure Active Directory. This could be through the out-of-box experience, users signing in via the company portal app, or users registering their devices through the account settings. If the user is brand new, has not set up MFA, and tries to join a device out-

of-the box, a temporary access pass will need to be provided which will allow them to fulfill the MFA requirement.

2.9.5

Tips

- For users trying to join Azure AD devices as part of the out-of-box experience or prior to getting to configure MFA, Temporary Access passes can be leveraged to fulfill the requirement

2.9.6

PowerShell Scripts

- None Currently

2.9.7

Videos

Enabling MFA when Joining a Device to Azure AD - YouTube

2.10 Managed Devices shall be required for authentication

Require that users connect to M365 from a device that is managed using conditional access. Companies that are implementing a hybrid Azure AD environment will likely use the conditional access control option named Hybrid Azure AD joined, whereas companies that are using devices that connect directly to the cloud and do not join an on-premises AD will use the conditional access control option named, Require device to be marked as compliant.

Guest user access note: This conditional access policy will impact guest access to the tenant because guest users will be required to authenticate from a managed device similar to regular Azure AD users. For guest users, the organization that manages their home tenant is responsible for managing their devices and the resource tenant must be configured to trust the device claims from the home tenant, otherwise

guest users will be blocked by the policy. This link describes the detailed authentication flow for guest users and how conditional access related to devices is applied. The implementation section describes the cross-tenant settings that must be configured in both the home and the resource tenants to facilitate guest access with managed devices.

2.10.1

Policy

Managed Devices shall be required for authentication.

2.10.2

Licensing Considerations

Azure AD P1 & Microsoft Intune. Can be purchased standalone or part of the following bundles:

- Microsoft 365 Business Premium
- EMS +E3/ E5
- Microsoft 365 E3
- Microsoft 365 E5

2.10.3

Set-Up Instructions

1. Create a conditional access policy to require devices to be marked as compliant in order to gain access Require compliant, hybrid joined devices, or MFA - Azure Active Directory - Microsoft Entra | Microsoft Learn

2.10.4

End-User Impact

Level: High

Users will not be able to login to their account on devices not enrolled into Intune and in a “Compliant” state.

End-User Notification Template

2.10.5

Tips

- Have a plan for guest users in the organization. Follow the steps as linked in the summary section or exclude guest users from the policy.

2.10.6

PowerShell Scripts

- None Currently

2.10.7

Videos

Conditional Access Policy for Device Compliance - YouTube

2.11 Guest User Access Shall be restricted

Ensure that only users with specific privileges can invite guest users to the tenant and that invites can only be sent to specific external domains. Ensure that guest users have limited access to Azure AD directory objects and that they are required to use MFA.

2.11.1

Policy

- Only users with the Guest Inviter role should be able to invite guest users.
- Guest invites should only be allowed to specific external domains that have been authorized by the agency for legitimate business purposes.
- Guest users should have limited access to Azure AD directory objects
- Guest users shall use MFA
- Guest User Access is periodically reviewed

2.11.2

Licensing Considerations

- All License models support the guest settings
- Azure AD P1 is required to enforce MFA for Guest users via Conditional Access

2.11.3

Set-Up Instructions

1. Configure guest settings in the portal: Enable B2B external collaboration settings - Azure AD - Microsoft Entra | Microsoft Learn

2. Under Guest user access, select Guest users have limited access to properties and memberships of directory objects

3. Under Guest invite settings, select Only users assigned to specific admin roles can invite guest users

4. Under Collaboration restrictions, select Allow invitations only to the specified domains (most restrictive). Select Target domains and enter the names of the external domains that have been authorized by the agency for guest user access.

5. Create a Conditional Access Policy with the Templates available

6. Chose the “Require Multi-Factor authentication for guest access” setting

7. Leverage the sign-in logs to review guest user access

2.11.4

End-User Impact

Level: Medium

Users will not be able to invite guest users to the organization without the Guest Inviter role. A formal process should be put into place to request guest access for certain organizations or users.

End-User Notification Template

2.11.5

Tips

- Use the collaboration settings for external users who are not using Azure AD. Use cross-tenant access settings for external users in another Azure AD environment.

2.11.6

PowerShell Scripts

Assign User as Guest Inviter: Enable B2B external collaboration settings - Azure AD - Microsoft Entra | Microsoft Learn

Allow or Block Domains: Allow or block invites to specific organizations - Azure AD - Microsoft Entra | Microsoft Learn

2.11.7

Videos

- Guest Permissions in Azure AD: A quick look at controlling guest account permissions to Azure AD - YouTube
- Azure AD Cross Tenant Settings: Azure AD Cross-Tenant Access Settings Deep Dive - YouTube

- Azure AD External Identities: What are Azure AD External Identities? - YouTube

2.12 The number of users with highly privileged roles shall be limited

Global Administrator is the highest privileged role in Azure AD because it provides unfettered access to the tenant. Therefore, if a user's credential with these permissions were to be compromised, it would present grave risks to the security of the tenant. Limit the number of users that are assigned the role of Global Administrator. Assign users to finer-grained administrative roles that they need to perform their duties instead of being assigned the Global Administrator role.

2.12.1

Policy

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

2.12.2

Licensing Considerations

All License models support configuration of roles.

2.12.3

Set-Up Instructions

1. In the Azure Portal, navigate to **Azure Active Directory**.

2. Select **Roles and administrators**.

3. Select the **Global administrator role**.

4. Under Manage, select **Assignments**.

5. Validate that between **two to four** users are listed.

a. For those who have Azure AD PIM, they will need to check both the Eligible assignments and Active assignments tabs. There should be a total of two to four users across both of these tabs (not individually).

b. If any groups are listed, need to check how many users are members of each group and include that in the total count.

2.12.4

End-User Impact

Level: Low

Impact is limited to users who have the Global Administrator role. If they do have these roles and you need to reduce the number of admins, you can see what levels of access they require today and give them roles with less permissions.

2.12.5

Tips

- Leverage PIM (need Azure AD P2 licensing) to provide eligible assignments for privileged roles vs permanent assignments.

2.12.6

PowerShell Scripts

- View Global Admins
- PowerShell for PIM: PowerShell for Azure AD roles in PIM - Azure AD - Microsoft Entra | Microsoft Learn
- 365 Admin Report: Export Office 365 Admin Role Report using PowerShell (o365reports.com)

2.12.7

Videos

PIM Overview: Privileged Identity Management (PIM) Demo - YouTube

2.13 Users assigned highly privileged roles shall not have permanent permissions

Do not assign users to highly privileged roles using permanent active role assignments. Instead, assign users to eligible role assignments in a PAM/PIM system and provide an expiration period for active assignments requiring privileged users to reactivate their highly privileged roles upon expiration.

2.13.1

Policy

- Permanent active role assignments shall not be allowed for highly privileged roles. Active assignments shall have an expiration period.
- The only exception to the policy is the break-glass Global Administrator account.

2.13.2

Licensing Considerations

Azure AD P2 if using Azure AD PIM. This can be purchased standalone or is part of the following bundles:

- EMS+E5
- Microsoft 365 E5

2.13.3

Set-Up Instructions

Deploy PIM: Plan a Privileged Identity Management deployment - Azure AD - Microsoft Entra | Microsoft Learn

2.13.4

End-User Impact

Level: Low

Impact is limited to users who are eligible to privileged roles which should be a small amount in the organization. These users will have to enter the Azure AD Admin center to activate their roles when needed.

End-User Notification Template

2.13.5

Tips

- The emergency break-glass account should be included in the permanent assignments for the Global Administrator role.

2.13.6

PowerShell Scripts

- PowerShell for PIM: PowerShell for Azure AD roles in PIM - Azure AD - Microsoft Entra | Microsoft Learn

2.13.7

Videos

- PIM Overview: Privileged Identity Management (PIM) Demo - YouTube

2.14 Activation of privileged roles should be monitored and require approval

Since many cyberattacks leverage privileged access, it is imperative to closely monitor the assignment and activation of the highest privileged roles for signs of compromise. Create alerts to trigger when a highly privileged role is assigned to a user and when a user activates a highly privileged role

Require approval for a user to activate a highly privileged role, such as Global Administrator. This makes it more challenging for an attacker to leverage the stolen credentials of highly privileged users and ensures that privileged access is monitored closely.

2.14.1

Policy

- Eligible and Permanent privileged role assignments shall trigger an alert
- User activation of the Global Administrator role shall trigger an alert
- Activation of the Global Administrator role should require approval

2.14.2

Licensing Considerations

Azure AD P2 if using Azure AD PIM. This can be purchased standalone or is part of the following bundles:

- EMS+E5
- Microsoft 365 E5

A 3rd party PAM tool could be used as a substitute.

2.14.3

Set-Up Instructions

Monitoring

1. In the Azure Portal, navigate to Azure AD Privileged Identity Management (PIM).
2. Under Manage, select Azure AD roles.
3. Under Manage, select Roles. This should bring up a list of all the Azure AD roles managed by the PIM service.
4. Click the Global Administrator role.
5. Click Settings and then click Edit.
6. Click the Notification tab.
7. Under Send notifications when members are assigned as eligible to this role, in the Role assignment alert -> Additional recipients textbox, enter the email address of the mailbox configured to receive the alerts for this role.
8. Under Send notifications when members are assigned as active to this role, in the Role assignment alert -> Additional recipients textbox, enter the email address of the mailbox configured to receive the alerts for this role.
9. Under Send notifications when eligible members activate this role, in the Role activation alert -> Additional recipients textbox, enter the email address of the mailbox configured to receive the alerts for this role.
10. Click Update.
11. Repeat steps 4 through 10 for each of the other highly privileged roles referenced in the policy section above, with one modification:
    a. When configuring the Send notifications when eligible members activate this role for these other roles, enter an email address of a mailbox that is different from the one used to monitor Global Administrator activations.

Approval

1. In the Azure Portal, navigate to Azure AD and create a new group named “Privileged Escalation Approvers.” This group will contain users that will receive role activation approval requests and approve or deny them. Users in this group must, at least, have the permissions provided to the Privileged Role Administrators role to adjudicate requests.
2. In the Azure Portal, navigate to Azure AD Privileged Identity Management (PIM).
3. Under Manage, select Azure AD roles.

4. Under Manage, select Roles. This should bring up a list of all the Azure AD roles managed by the PIM service.
5. Repeat this step for the Privileged Role Administrator role, User Administrator role, and other roles that the agency has designated as highly privileged.
    a. Click the Global Administrator role in the list.
    b. Click Settings.
    c. Click Edit.
    d. Select the Require approval to activate option.
    e. Click Select approvers, select the group Privileged Escalation Approvers, and then click Select.
    f. Click Update.

2.14.4

End-User Impact

Level: Low

Impact is limited to users who are eligible to privileged roles which should be a small amount in the organization. These users will have to have someone approve their activation.

2.14.5

Tips

- A group of users should be assigned for approval vs a single point of contact.
- More granular settings can be applied to these roles such as requiring MFA upon activation and requiring a justification reason.

2.14.6

PowerShell Scripts

- PowerShell for PIM: [PowerShell for Azure AD roles in PIM - Azure AD - Microsoft Entra | Microsoft Learn]

2.14.7

Videos

- PIM Overview: Privileged Identity Management (PIM) Demo - YouTube

2.15 Highly privileged accounts shall be cloud-only

Assign users that need to perform highly privileged tasks to cloud-only Azure AD accounts to minimize the collateral damage of an on-premises identity compromise.

2.15.1

Policy

- Users that need to be assigned to highly privileged Azure AD roles SHALL be provisioned cloud-only accounts that are separate from the on-premises directory or other federated identity providers.

2.15.2

Licensing Considerations

- All Microsoft Licensing Models support this configuration.

2.15.3

Set-Up Instructions

1. Follow these steps to review the administrative roles like Global Administrator
2. Ensure that these accounts are cloud only

2.15.4

End-User Impact

Level: None

There is no real end user impact here as you are establishing cloud only administrative accounts.

2.15.5

Tips

- Periodically review the privileged roles within the organization to ensure compliance with this policy.

2.15.6

PowerShell Scripts

- Getting Sync Status: Listing Azure AD/Office 365 User Accounts with Directory Sync Status (practical365.com)
- View Microsoft 365 user accounts with PowerShell - Microsoft 365 Enterprise | Microsoft Learn

2.15.7

Videos

- None Currently

2.16 Highly privileged role assignments shall be periodically reviewed

Access reviews should be periodically performed for users with permanent or eligible privileged roles. Users should evaluate whether they still need these permissions and update assignments accordingly. Access reviews can be performed

manually or with a tool like Microsoft Access Reviews which is part of an Azure AD P2 subscription.

2.16.1

Policy

- Access reviews shall be performed for users with permanent or eligible privileged roles.

2.16.2

Licensing Considerations

To leverage the Access Reviews in Microsoft, an Azure AD P2 license is required. This can be purchased standalone or as part of the following bundles:

- EMS+E5
- Microsoft 365 E5

2.16.3

Set-Up Instructions

Follow these steps to create Access Reviews leveraging the native tooling in Microsoft.

2.16.4

End-User Impact

Level: Low

Impact is limited to the users with privileged roles. When an access review is conducted, the user will be notified via email to review their existing roles. They will be able to provide feedback on if they need to continue to have that role with a justification reason.

End-User Notification Template

2.16.5

Tips

- Try to perform access reviews on a semi-annual basis at the minimum.

2.16.6

PowerShell Scripts

- 365 Admin Report: Export Office 365 Admin Role Report using PowerShell (o365reports.com)
- Access Reviews PowerShell samples: microsoft/access-reviews-samples: This repo contains sample code that demonstrates programmatic access to Azure AD Access Reviews. Sample code includes reading and managing Access Reviews, as well as working on decisions and results of Access Reviews. (github.com)

2.16.7

Videos

Access Review Demo - YouTube

2.17 Passwords shall not expire

Ensure that user passwords do not expire. Both the National Institute of Standards and Technology (NIST) and Microsoft emphasize MFA because they indicate that mandated password changes make user accounts less secure.

2.17.1

Policy

User passwords shall not expire.

2.17.2

Licensing Considerations

Configuring this setting is available in any Microsoft 365 offering.

2.17.3

Set-Up Instructions

1. Follow these steps to set passwords to never expire

Microsoft Password Guidance Microsoft_Password_Guidance-1.pdf

2.17.4

End-User Impact

Level: Medium

Impact is low as users do not have to reset their passwords on a periodic basis but will have to set up passwordless methods of authentication.

End-User Notification Template

2.17.5

Tips

- Ensure that weak passwords are not being used Password protection in Azure Active Directory - Microsoft Entra | Microsoft Learn
- If possible, think about going passwordless: Passwordless authentication | Microsoft Security

2.17.6

PowerShell Scripts

Automating with PowerShell: Deploying passwordless Authentication (cyberdrain.com)

2.17.7

Videos

- I used passwordless first day on the job - YouTube
- How can Passwordless make new hire onboarding even easier...? - YouTube
- Passwordless: Using Microsoft Authenticator for app login (phone sign-in preview) - YouTube

2.18 Azure AD Logs shall be collected

Azure AD logs should be a collected and periodically reviewed to detect any anomalies. Log information should be centralized in a SIEM tool, like Microsoft Sentinel, so that it can be audited and queried. Audit logs should be retained in a storage account for a minimum of 90 days.

Log events that can be collected are as follows: AuditLogs, SignInLogs, RiskyUsers, UserRiskEvents, NonInteractiveUserSignInLogs, ServicePrincipalSignInLogs, ADFSSignInLogs, RiskyServicePrincipals, and ServicePrincipalRiskEvents.

2.18.1

Policy

- Azure AD Log data is sent to a SIEM and/or external storage
- Log data is periodically reviewed.
- Log data is sent to an internal or external SOC for monitoring

2.18.2

Licensing Considerations

To retain Azure AD log data more than 7 days, an Azure AD P1 License is required. This license retains data for 30 days and is available to purchase standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- EMS+E3/E5
- Microsoft 365 E3
- Microsoft 365 E5

2.18.3

Set-Up Instructions

Analyzing Sign-Ins Analyze sign-ins with the Azure AD sign-ins log - Microsoft Entra | Microsoft Learn

Route logs to a storage account: Tutorial - Archive directory logs to a storage account - Microsoft Entra | Microsoft Learn

Everything you want to know about Security and Audit logging in Office 365 Everything you wanted to know about Security and Audit Logging in Office 365 | The Cloud Technologist

Sign In logs in Azure AD: Sign-in logs (preview) in Azure Active Directory - Microsoft Entra | Microsoft Learn

Connect AD data to Microsoft Sentinel: Connect Azure Active Directory data to Microsoft Sentinel | Microsoft Learn

2.18.4

End-User Impact

Level: None

There is no end user impact to review and collect Azure AD logs.

2.18.5

Tips

- N/A

2.18.6

PowerShell Scripts

- Documenting with PowerShell: Downloading and storing the Office 365 Audit logs (With search!) (cyberdrain.com)
- Automating with PowerShell: Storing Office 365 audit logs longer than 90 days (cyberdrain.com)
- Monitoring with PowerShell: Monitoring failed logins for Office365 (cyberdrain.com)
- Azure AD PowerShell cmdlets for reporting - Microsoft Entra | Microsoft Learn

2.18.7

Videos

Audit Logs and Sign in logs in AAD | A deep-dive session on Azure AD Audit Logs and Sign-in Logs - YouTube

2.19 Only Admins shall be allowed to register 3rd party applications

Ensure that only administrators can register third-party applications that can access the tenant.

2.19.1

Policy

- Only administrators SHALL be allowed to register third-party applications.

2.19.2

Licensing Considerations

This setting can be configured with any Microsoft licensing.

2.19.3

Set-Up Instructions

1. In the Azure Portal, navigate to Azure Active Directory.
2. Under Manage, select Users.
3. Select User settings.
4. Under App Registrations -> Users can register applications, select No.
5. Click Save.

2.19.4

End-User Impact

Level: Low

The number of times a user should be trying to register a 3rd part application should be low but when they do, they will be blocked. This setting is not generally something that requires any communication before turning on.

2.19.5

Tips

- N/A

2.19.76

PowerShell Scripts

- Automating with PowerShell: Setting up application consent (cyberdrain.com)
- Monitoring with PowerShell: Monitoring oAuth application changes (cyberdrain.com)

2.19.7

Videos

Azure AD App Registrations, Enterprise Apps and Service Principals - YouTube

2.20 Non-admin users shall be prevented from providing consent to 3rd party applications

Ensure that only administrators can consent to third-party applications and only administrators can control which permissions are granted. An admin consent workflow can be configured in Azure AD; otherwise, users will be blocked when they try to access an application that requires permissions to access organizational data. Develop a process for approving and managing third-party applications.

2.20.1

Policy

- Only administrators SHALL be allowed to consent to third-party applications.
- An admin consent workflow SHALL be configured.
- Group owners SHALL NOT be allowed to consent to third-party applications.

2.20.2

Licensing Considerations

This setting can be configured with any Microsoft licensing.

2.20.3

Set-Up Instructions

1. In the Azure Portal, navigate to Azure Active Directory.
2. Create a new Azure AD Group that contains admin users responsible for reviewing and adjudicating app requests.
3. Under Manage, select Enterprise Applications.
4. Under Security, select Consent and permissions
5. Under User consent for applications, select Do not allow user consent.
6. Under Group owner consent for apps accessing data, select Do not allow group owner
7. consent.
8. In the menu, navigate back to Enterprise Applications.
9. Under Manage, select User Settings.
10. Under Admin consent requests -> Users can request admin consent to apps they are unable to consent to, select Yes.
11. Under Who can review admin consent requests, select the group created in step two that is responsible for reviewing and adjudicating app requests.
12. Click Save.

2.20.4

End-User Impact

Level: Low

The number of times a user should be trying to consent a 3rd part application should be low but when they do, they will be blocked. If you have configured the admin consent flow, they will be notified accordingly. This setting is not generally something that requires any communication before turning on.

2.20.5

Tips

- N/A

2.20.6

PowerShell Scripts

- Automating with PowerShell: Setting up application consent (cyberdrain.com)
- Monitoring with PowerShell: Monitoring oAuth application changes (cyberdrain.com)

2.20.7

Videos

Azure AD App Registrations, Enterprise Apps and Service Principals - YouTube

2.21 Authorized Applications shall be configured for Single Sign-On

If available, all authorized applications should be configured for single sign-on to extend authentication security to 3rd party applications.

2.21.1

Policy

- Authorized applications shall be configured for single sign-on if available.

2.21.2

Licensing Considerations

To configure Enterprise applications for SSO, an Azure AD P1 license is required. This can be purchased standalone or is available as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5
- EMS+E3/E5

2.21.3

Set-Up Instructions

The configuration settings will be application specific but all applications will be configured in the Enterprise application section of Azure AD: Enable single sign-on for an enterprise application - Microsoft Entra | Microsoft Learn

Example SSO with Dropbox: Tutorial: Azure Active Directory integration with Dropbox Business - Microsoft Entra | Microsoft Learn

2.21.4

End-User Impact

Level: Medium

After applications are set up for single sign-on, users will be able to leverage their Azure Active Directory credentials to access the application. It is important to alert users before turning on SSO for an application so they are not caught off-guard from a redirection to Microsoft when trying to sign-in. Be careful with some applications as you can get locked out if settings are not configured properly.

End-User Notification Template

2.21.5

Tips

- Establish a communication plan prior to setting up SSO for an application.
- Leverage Azure AD groups to grant and revoke access to applications.
- Leverage SCIM provisioning if it is available from the application provider.

2.21.6

PowerShell Scripts

- N/A

2.21.7

Videos

- Configuring an Enterprise Application for Single Sign-on - YouTube
- Single Sign On | What it is How it works Why you need it - YouTube
- Configuring Dropbox for SSO - YouTube

2.22 Inactive accounts shall be blocked or deleted

Deleting or blocking accounts that haven't been used for over 30 days helps prevent unauthorized use of inactive accounts. These accounts can be targets for attackers who are looking to find ways to access your data or move laterally throughout an organization without being noticed.

2.22.1

Policy

- Inactive accounts shall be blocked or deleted.
- Users who leave the organization shall have their account switched to a blocked state immediately.

2.22.2

Licensing Considerations

To gather the user's last sign in from the Audit logs, you will need an Azure AD P1 subscription which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5
- EMS+E3/E5

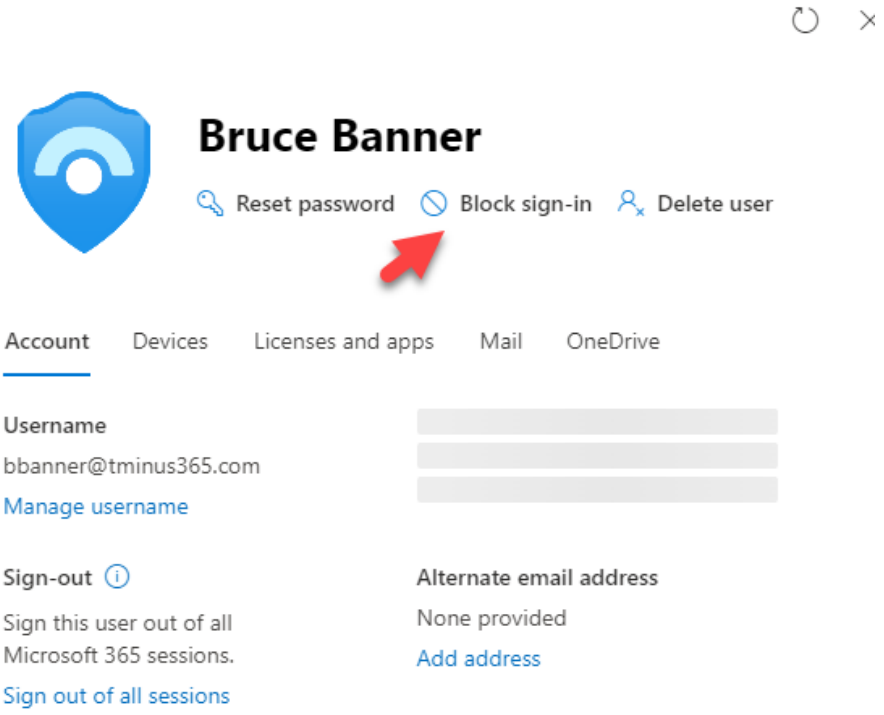
2.22.3

Set-Up Instructions

Manage inactive user accounts in Azure AD: How to manage inactive user accounts in Azure AD - Microsoft Entra | Microsoft Learn

Blocking Sign-In

1. Go to https://admin.microsoft.com/
2. Click Users>Active Users
3. Select the account you want to block
4. Click Block sign-in at underneath the account name



2.22.4

End-User Impact

Level: None

If accounts are truly dormant, there should be no impact to end-users. Proper validation is required before blocking or deleting accounts.

2.22.5

Tips

- Block user accounts after someone leaves the organization. Develop a retention policy that defines how long you will keep the account before removing completely.

2.22.6

PowerShell Scripts

Leveraging Graph API: How to manage inactive user accounts in Azure AD - Microsoft Entra | Microsoft Learn.

Find Azure AD Inactive Users using Powershell and Graph - Azure365Pro.com

2.22.7

Videos

None Currently

3.0 Microsoft Teams

3.1 Private Channels shall be utilized to restrict access to sensitive information

Access controls are a fundamental part of any compliance regulation. Giving access to certain Teams channels where users are collaborating on sensitive topics or sharing critical documents should follow a model of least privilege. Microsoft Teams allows you to create private channels where users can request access to the owners and all other users are prohibited from seeing the content.

3.1.1

Policy

- When creating new Teams channels, a proper evaluation should be done to determine if a private channel should be selected.

3.1.2

Licensing Considerations

Creating Private channels does not require any premium licensing. Any base plan with Teams included will have access to create a Teams Private Channel.

3.1.3

Set-Up Instructions

Follow these steps to create a private channel in Teams

Overview of Private Channels: Private channels in Microsoft Teams - Microsoft Teams | Microsoft Learn

3.1.4

End-User Impact

Level: Medium

Content within a private channel is restricted to the owners and members of that channel. Users will not be able to share any documents part of the channel with any members of the org not part of the channel.

3.1.5

Tips

Best practices for organizing teams in Microsoft Teams: Best practices for organizing teams - Microsoft Teams | Microsoft Learn

3.1.6

PowerShell Scripts

Create Private channel in Microsoft Teams using PowerShell (morgantechspace.com)

New-TeamChannel (MicrosoftTeamsPowerShell) | Microsoft Learn

3.1.7

Videos

- Best Practices for Organizing Microsoft Teams
- How to make a Private Channel in Teams

3.2 External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings

This setting controls whether external meeting participants can request control of the shared desktop or window during the meeting. In this instance, the term “external participants” includes external users, B2B guest users, unmanaged users, and anonymous users.

While there is some inherent risk in granting an external participant control of a shared screen, legitimate use cases for this exist. Furthermore, the risk is minimal as users cannot gain control of another user’s screen unless the user giving control explicitly accepts a control request. As such, while enabling external participants to request control is discouraged, it may be done, depending on organizational need.

3.2.1

Policy

External participants SHOULD NOT be enabled to request control of shared desktops or windows in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

3.2.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.2.3

Set-Up Instructions

Follow these steps to configure desktop sharing settings in the Teams admin center.

To ensure external participants do not have the ability to request control of the shared desktop or window in the meeting

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings** -> **Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Content sharing** section, set **Allow an external participant** to give or request control to **Off.**
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3

3.2.4

End-User Impact

Level: Low

The number of occurrences where an external participant should need to control the screen is limited. If this is something that is required for a long-term engagement,

you could set up a policy to temporarily enable it for certain users within the organization.

3.2.5

Tips

- N/A

3.2.6

PowerShell Scripts

Configure Meeting Policy Set-CsTeamsMeetingPolicy (SkypeForBusiness) | Microsoft Learn

3.2.7

Videos

Giving or Requesting Control of Screens

3.3 Anonymous Users SHALL NOT Be Enabled to Start Meetings

This setting controls which meeting participants can start a meeting. In this instance, the term “anonymous users” refers to any Teams users joining calls that are not authenticated through the company’s tenant.

3.3.1

Policy

Anonymous users SHALL NOT be enabled to start meetings in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

3.3.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.3.3

Set-Up Instructions

Microsoft Resources: Control who can bypass the meeting lobby in Microsoft Teams - Microsoft Teams | Microsoft Learn

To configure settings for anonymous users:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Meetings** -> **Meeting policies.**
3. Select the **Global** (Org-wide default) policy.
4. Under the **Participants & guests** section, set **Let anonymous people start a meeting** to **Off**.
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3

3.3.4

End-User Impact

Level: Low

This is only affecting external users who enter a meeting as anonymous.

3.3.5

Tips

- N/A

3.3.6

PowerShell Scripts

- Configure Meeting Policy Set-CsTeamsMeetingPolicy (SkypeForBusiness) | Microsoft Learn

3.3.7

Videos

- None Currently

3.4 Automatic Admittance to Meetings SHOULD Be Restricted

This setting controls which meeting participants wait in the lobby before they are admitted to the meeting

3.4.1

Policy

- Anonymous users, including dial-in users, SHOULD NOT be admitted automatically.
- Internal users SHOULD be admitted automatically.
- B2B guest users MAY be admitted automatically.
- The above settings SHOULD be set in the Global (Org-wide default) meeting policy.
- Custom meeting policies MAY be created that allow more flexibility for specific users.

3.4.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.4.3

Set-Up Instructions

Microsoft Resources: Manage meeting policies for participants and guests - Microsoft Teams | Microsoft Learn

To configure settings for automatic meeting admittance:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Meetings** -> **Meeting policies.**
3. Select the **Global** (Org-wide default) policy.
4. Under the **Participants & guests section**, ensure **Automatically admit people** is **not set** to **Everyone**.
5. In the same section, set **Dial-in users can bypass the lobby** to **Off**.
6. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3

3.4.4

End-User Impact

Level: Low

Internal Users will need to manually admit anonymous and/or external users to meetings when they enter the lobby.

3.4.5

Tips

- N/A

3.4.6

PowerShell Scripts

- Configure Meeting Policy Set-CsTeamsMeetingPolicy (SkypeForBusiness) | Microsoft Learn

3.4.7

Videos

- None Currently

3.5 External User Access SHALL Be Restricted

External access allows external users to look up internal users by their email address to initiate chats and calls entirely within Teams. Blocking external access prevents external users from using Teams as an avenue for reconnaissance or phishing. Even with external access disabled, external users will still be able to join Teams calls, assuming anonymous join is enabled. Depending on organizational need, if both external access and anonymous join need to be blocked— neither required nor recommended by this baseline—external collaborators would only be able to attend meetings if added as a B2B guest user. External access may be granted on a per-domain basis. This may be desirable in some cases, e.g., for agency-to-agency collaboration.

3.5.1

Policy

- External access SHALL only be enabled on a per-domain basis.
- Anonymous users SHOULD be enabled to join meetings.

3.5.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.5.3

Set-Up Instructions

Microsoft Resources:

- Manage external meetings and chat - Microsoft Teams | Microsoft Learn
- Manage meeting settings - Microsoft Teams | Microsoft Learn
- Use guest access and external access to collaborate with people outside your organization - Microsoft Teams | Microsoft Learn

To enable external access for only specific domains:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users** -> **External access**.
3. Under Choose which external domains your users have access to, select **Allow only specific external domains.**
4. Click **Allow domains** to add allowed external domains. All domains not added in this step will be blocked.
5. Click Save

To enable anonymous users to join meetings:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings** -> **Meeting settings.**
3. Under **Participant**s, set **Anonymous users can join a meeting** to **On.**
4. Click Save

Anonymous users can also be enabled/blocked on a per-policy basis.

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Meetings** -> **Meeting policies.**
3. Select the **Global** (Org-wide default), or other policy as needed.
4. Under **Participants & guests**, set **Let anonymous people join a meeting** to **On**.
5. Click Save.

3.5.4

End-User Impact

Level: Low

This will vary depending on the organization and need for external collaboration. A formal process for adding external domains for collaboration should be established so that end users have a place to request new external participants.

3.5.5

Tips

- Make sure its clear how end-users request external collaboration participants

3.5.6

PowerShell Scripts

- Set External Access Policy: Set-CsExternalAccessPolicy (SkypeForBusiness) | Microsoft Learn
- Manage external meetings and chat - Microsoft Teams | Microsoft Learn

3.5.7

Videos

- None Currently

3.6 Unmanaged User Access SHALL Be Restricted

Blocking contact with unmanaged Teams users prevents these users from looking up internal users by their email address and initiating chats and calls within Teams. These users would still be able to join calls, assuming anonymous join is enabled. Additionally, unmanaged users may be added to Teams chats if the internal user initiates the contact. Unmanaged accounts are ones not managed by an organization, typically Teams personal accounts.

3.6.1

Policy

- Unmanaged users SHALL NOT be enabled to initiate contact with internal users.
- Internal users SHOULD NOT be enabled to initiate contact with unmanaged users.

3.6.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.6.3

Set-Up Instructions

Microsoft Resources:

Manage external meetings and chat - Microsoft Teams | Microsoft Learn

To block unmanaged users for initiating contact:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Users** -> **External access.**
3. To completely block contact with unmanaged users, under T**eams accounts not managed by an organizatio**n, set **People in my organization can communicate with Teams users whose accounts aren't managed by an organization** to **Off.**
4. To allow contact with unmanaged users **only if the internal user initiates** the contact:
    a. Under Teams accounts not managed by an organization, set People in my organization can communicate with Teams users whose accounts aren't managed by an organization to On.
    b. **Clear the check** next **to External users with Teams accounts not managed by an organization can contact users in my organization.**

3.6.4

End-User Impact

Level: Low

This will vary depending on the organization and need for external collaboration with users not managed by an organization. A formal process for adding external domains for collaboration should be established so that end users have a place to request new external participants.

3.6.5

Tips

- Make sure its clear how end-users request external collaboration participants

3.6.6

PowerShell Scripts

- Set External Access Policy: Set-CsExternalAccessPolicy (SkypeForBusiness) | Microsoft Learn

3.6.7

Videos

- None Currently

3.7 Contact with Skype Users SHALL Be Blocked

Microsoft officially retired Skype for Business Online on July 31, 2021, and it is no longer supported.

3.7.1

Policy

Contact with Skype users SHALL be blocked.

3.7.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.7.3

Set-Up Instructions

Microsoft Resources:

Manage external meetings and chat - Microsoft Teams | Microsoft Learn

Instructions for enabling communications with Skype users are outlined in Communicate with Skype users.

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Users** -> **External access**.
3. Under **Skype user**s, set **Allow users in my organization to communicate with Skype users** to **Off.**
4. Click **Save.**

3.7.4

End-User Impact

Level: Low

The frequency of which someone is asking to communicate via skype should be low.

3.7.5

Tips

- N/A

3.7.6

PowerShell Scripts

- Set External Access Policy: Set-CsExternalAccessPolicy (SkypeForBusiness) | Microsoft Learn

3.7.7

Videos

- None Currently

3.8 Teams Email Integration SHALL Be Disabled

Teams provides an optional feature that allows channels to have an email address and receive email. These channel email addresses are not under the tenant's domain; rather, they are associated with a Microsoft-owned domain, teams.ms. As such, although some basic checks are performed, companies do not have control over the security settings associated with this email. For this reason, email channel integration should be disabled.

3.8.1

Policy

Teams email integration SHALL be disabled.

3.8.2

Licensing Considerations

Teams email integration is only available with E3/E5 licenses. It is not available in GCC or DoD tenants.

3.8.3

Set-Up Instructions

Resources:

How to Control Sending Email to Teams Channels | Practical365

To ensure that teams email integration is disabled:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Teams** -> **Teams Settings.**
3. Under the **Email integration** section, set **Allow users to send emails to a channel email address** to **Off**.

3.8.4

End-User Impact

Level: Low

Adoption of the Teams email integration should be low or nonexistent. Make sure to review and active Teams emails in use and notify users accordingly before disabling this feature.

3.8.5

Tips

- N/A

3.8.6

PowerShell Scripts

- None Currently

3.8.7

Videos

How to enable or disable email integration in Microsoft Teams Admin #Office365 - YouTube

3.9 Only Approved Apps SHOULD Be Installed

Teams can integrate with the following classes of apps:

- Microsoft apps: apps published by Microsoft.
- Third-party apps: apps not authored by Microsoft, published to the Teams store.
- Custom apps: apps not published to the Teams store, such as apps under development, that users "sideload" into Teams

Only authorized and approved applications should be available to end-users to manage exfiltration of corporate data. Additionally, unmanaged applications may have certain vulnerabilities that exploit users, devices, or data.

3.9.1

Policy

- Organizations SHOULD allow all apps published by Microsoft, but MAY block specific Microsoft apps as needed.
- Organizations SHOULD NOT allow installation of all third-party apps or custom apps, but MAY allow specific apps as needed.
- Organizations shall establish policy dictating the app review and approval process to be used by the company.

3.9.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.9.3

Set-Up Instructions

Resources:

Manage app permission policies in Microsoft Teams - Microsoft Teams | Microsoft Learn

To restrict which Team apps can be installed:

1. Sign in to the **Microsoft Teams admin center.**
2. Select **Teams apps** -> **Permission policies.**
3. Select **Global** (Org-wide default).
4. Under **Microsoft apps**, select **Allow all apps, unless specific apps need to be disallowed**, in which case select **Block specific apps and allow all others.**
5. Set **Third-party apps** to **Block all apps, unless specific apps have been approved by the agenc**y, in which case select Allow specific apps and block all others.
6. Set **Custom apps** to **Block all apps, unless specific apps have been approved by the agency**, in which case select Allow specific apps and block all others.
7. Click **Save**.
8. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

3.9.4

End-User Impact

Level: Medium

This will vary depending on the organization but users will not be able to add applications from the Apps section of team unless preapproved in the Teams admin

center. A formal process for requesting new Teams apps should be properly documented and communicated.

3.9.5

Tips

- May sure users understand how to request a new applications for Microsoft Teams.

3.9.6

PowerShell Scripts

How to manage Microsoft Teams app permission policy – PARAS DODHIA BLOG

New-CsTeamsAppPermissionPolicy (SkypeForBusiness) | Microsoft Learn

Set-CsTeamsAppPermissionPolicy (SkypeForBusiness) | Microsoft Learn

3.9.7

Videos

- None Currently

3.10 File Sharing and File Storage Options shall be blocked

By default, users can add external third-party storage providers like Google and Drobox to their Teams channels for file storage. Only managed, trusted providers should be allowed for data loss prevention purposes.

3.10.1

Policy

File Sharing and File Storage Options are disabled.

3.10.2

Licensing Considerations

Any Teams licensing supports this configuration.

3.10.3

Set-Up Instructions

Resources:

Controlling Third Party Cloud Storage Access for Microsoft Teams | Practical365

To restrict file sharing and file storage options:

1. Go to the **Microsoft Teams Admin Center**
2. Choose **Teams -> Teams Settings.**
3. Under **Files** turn off all 3rd part file storage applications
4. Click **Save**

3.10.4

End-User Impact

Level: Low

This will very depending on the organization but in most cases, end-users should be leveraging native file storage options such as SharePoint or OneDrive. Ensure that end-users are not uploading files to 3rd parties before configuring this setting.

3.10.5

Tips

- N/A

3.10.6

PowerShell Scripts

Get-CsTeamsClientConfiguration (SkypeForBusiness) | Microsoft Learn

Set-CsTeamsClientConfiguration (SkypeForBusiness) | Microsoft Learn

3.10.7

Videos

Security & Compliance in Microsoft Teams: Cloud App Security & 3rd Party Storage - YouTube

How to add third-party cloud services to Microsoft Teams - YouTube

3.11 Only the Meeting Organizer SHOULD Be Able to Record Live Events

Live events are recorded by default. Organizations should increase their privacy by changing the policy so that events are only recorded at the organizer's discretion.

3.11.1

Policy

Record an event SHOULD be set to Organizer can record.

3.11.2

Licensing Considerations

Enterprise licensing is required to host live events.

3.11.3

Set-Up Instructions

Resources:

Live events recording policies - Microsoft Teams | Microsoft Learn

1. Sign in to the Microsoft Teams admin center.
2. Select Meetings -> Live events policies.
3. Select Global (Org-wide default).
4. Set Record an event to Organizer can record.
5. Click Save.

3.11.4

End-User Impact

Level: Low

Ensure users are aware that only the meeting organizer can record the live event.

3.11.5

Tips

- N/A

3.11.6

PowerShell Scripts

- None Currently

3.11.7

Videos

- None Currently

3.12 Data Loss Prevention Solutions SHALL Be Enabled

Data loss prevention (DLP) helps prevent both accidental leakage of sensitive information as well as intentional exfiltration of data. DLP forms an integral part of securing Microsoft Teams. There a several commercial DLP solutions available that document support for Microsoft Teams. Agencies may select any service that fits their needs and meets the requirements outlined in this baseline control.

3.12.1

Policy

- A DLP solution SHALL be enabled.
- Organizations SHOULD use either the native DLP solution offered by Microsoft or a DLP solution that offers comparable services.
- The DLP solution SHALL protect Personally Identifiable Information (PII) and sensitive information, as defined by the agency. At a minimum, the sharing of credit card numbers, taxpayer Identification Numbers (TIN), and Social Security Numbers (SSN) via email SHALL be restricted.

3.12.2

Licensing Considerations

Data loss prevention policies can be configured with the following plans:

- Microsoft 365 Business Premium
- Office 365 E5/A5/G5
- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/G5 Information Protection and Governance
- Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance

3.12.3

Set-Up Instructions

Resources:

Data loss prevention and Microsoft Teams - Microsoft Purview (compliance) | Microsoft Learn

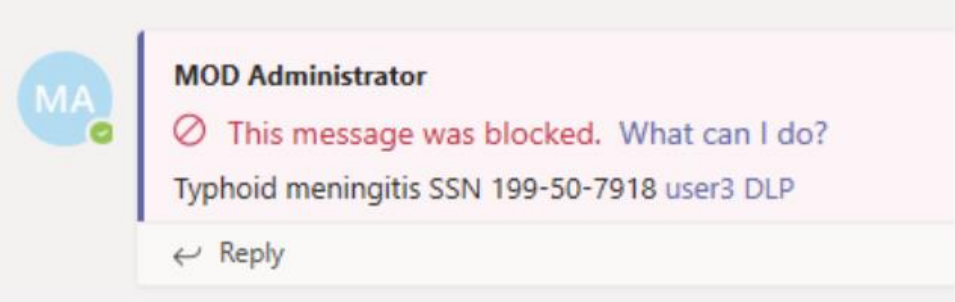
To create a DLP policy for Teams follow the steps listed here

3.12.4

End-User Impact

Level: Medium

When DLP policies are in place any user trying to share sensitive information as defined by the policy will be blocked.



Teams messages about data loss prevention (DLP) and communication compliance policies - Microsoft Support

3.12.5

Tips

- To ensure organizational compliance, its recommended send end-user communications before turning the policy on. Educate users on how to properly share sensitive information.

3.12.6

PowerShell Scripts

How to Create and Manage DLP policies using PowerShell » Jorge Bernhardt

New-DlpCompliancePolicy (ExchangePowerShell) | Microsoft Learn

3.12.7

Videos

How to add third-party cloud services to Microsoft Teams - YouTube

Microsoft 365 DLP (Data Loss Prevention Policies) How they work & Why YOU need them NOW! - YouTube

Microsoft Teams DLP - Create a Teams DLP Policy - YouTube

3.13 Attachments SHOULD Be Scanned for Malware

Safe attachment protection policies from Defender for Office 365 should be enabled and configured for Teams. Attachments should be scanned in a sandbox for malware upon opening or downloading.

3.13.1

Policy

- Attachments included with Teams messages SHOULD be scanned for malware. Users SHOULD be prevented from opening or downloading files detected as malware.

3.13.2

Licensing Considerations

Safe Attachments can be configured with the Following plans

- Defender for Office 365 Plan 1/2
- Microsoft 365 Business Premium
- Office 365 E5/A5/G5
- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/G5 Information Protection and Governance
- Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance

3.13.3

Set-Up Instructions

Resources:

Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams - Office 365 | Microsoft Learn

To enable Safe Attachments for Teams follow the steps listed here

3.13.4

End-User Impact

Level: Low

When safe attachments are enabled in Teams users will experience more latency for files to open as they are scanned. Users will get a prompt in Teams that lets them know the file is being scanned for malicious content.

3.13.5

Tips

- N/A

3.13.6

PowerShell Scripts

Turn on Safe Attachments for SharePoint, OneDrive, and Microsoft Teams - Office 365 | Microsoft Learn

3.13.7

Videos

MS-700 \\ Safe Attachments & Safe Links (Ep 13) - YouTube

Teams Meetings - Safe Attachments - YouTube

3.14 Link Protection SHOULD Be Enabled

Microsoft Defender protects users from malicious links included in Teams messages by prependinghttps://*.safelinks.protection.outlook.com/?url= to URLs included in the messages.

By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy performs the following checks:

- Compares the URL with a block list
- Compares the URL with a list of know malicious sites
- If the URL points to a downloadable file, applies real-time file scanning

If all checks pass, the user is redirected to the original URL.

3.14.1

Policy

- URL comparison with a block-list SHOULD be enabled.
- Direct download links SHOULD be scanned for malware.
- User click tracking SHOULD be enabled.

3.14.2

Licensing Considerations

Safe Links can be configured with the Following plans

- Defender for Office 365 Plan 1/2
- Microsoft 365 Business Premium
- Office 365 E5/A5/G5
- Microsoft 365 E5/A5/G5
- Microsoft 365 E5/A5/G5 Information Protection and Governance
- Microsoft 365 E5/A5/G5/F5 Compliance and F5 Security & Compliance

3.14.3

Set-Up Instructions

Resources:

Set up Safe Links policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

To enable Safe Links for Teams follow the steps listed here

3.14.4

End-User Impact

Level: Low

When safe links is enabled in Teams users will experience more latency for webpages to open while the URL is being scanned. If a link is detected as malicious the user will see a warning message. Depending on how the policy is configured, the user will/will not be able to proceed to the webpage.

3.14.5

Tips

- N/A

3.14.6

PowerShell Scripts

Set up Safe Links policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

3.14.7

Videos

MS-700 \\ Safe Attachments & Safe Links (Ep 13) - YouTube

3.15 Restrict Users who can Create Teams Channels

Users within a tenant have the ability to create a public or private Teams channel by default. Behind the scenes, creating a Teams channel also creates a Microsoft 365 or Office 365 Group and a SharePoint site with a document library that stores all documents shared within the Teams channel. Over time, if this is not managed, the environment could quickly get out of hand with the number of Teams channels being created. This could lead to data loss, insecure sharing of documentation, and overall confusion across the organization. We recommend limiting the creation of Teams channels to certain members within the organization and creating a formal request process for new channels. To configure this setting, you will be restricting access for who can create a group as that is the backend to a Teams channel.

3.15.1

Policy

- Creating Teams Channels should be restricted to a limited group of users

3.15.2

Licensing Considerations

To manage who creates groups, an Azure AD Premium license is required

Manage who can create Microsoft 365 Groups | Microsoft Learn

This license can be purchased standalone or as part of the following bundles:

- EMS + E3/E5
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

3.15.3

Set-Up Instructions

Resources:

To restrict who can create Teams channels (groups) follow the steps listed here

3.15.4

End-User Impact

Level: Medium

It is very important that you properly plan and communicate any changes here before rolling them out. The goal is not to inhibit productivity and force users to go to outside channels to collaborate, causing shadow IT. It is imperative that you make the request for creating a new Teams channel as seamless as possible. Restricting the creation of Teams channels also restricts who can create Groups. The setting is all or nothing in this regard.

3.15.5

Tips

- N/A

3.15.6

PowerShell Scripts

Manage who can create Microsoft 365 Groups | Microsoft Learn

3.15.7

Videos

Restricting who can create Microsoft Teams Channels - YouTube

3.16 Teams Channels shall have an expiration policy

Organizations with a large number of Teams often have Teams channels that are never actually used. This can happen because of several reasons including product experimentation, short-term team collaboration, or team owners leaving the organization. Over time, such teams can accumulate and create a burden on tenant resources. To curb the number of unused teams, as an admin, you can use group expiration policy to automatically clean up unused teams. Because teams are backed by groups, group expiration policies automatically apply to teams as well.

3.16.1 Policy

- Teams channels shall have an expiration policy for inactivity

3.16.2 Licensing Considerations

There are no licensing considerations for modifying the group expiration policy.

3.16.3 Set-Up Instructions

Resources:

Microsoft 365 group expiration policy | Microsoft Learn

To define group expiration policies, follow the steps listed here

3.16.4 End-User Impact

Level: Medium

When you apply an expiration policy to a team, a team owner receives a notification for team renewal 30 days, 15 days and 1 day before the team's expiration date. When the team owner receives the notification, they can click Renew now in team settings to renew the team. To prevent accidental deletion, auto-renewal is automatically enabled for a Team in the group expiration policy. When the group expiration policy is set up, any team that has at least one channel visit from any team member before its expiration date is automatically renewed without any manual intervention from the team owner.

3.16.5

Tips

- N/A

3.16.6

PowerShell Scripts

New-AzureADMSGroupLifecyclePolicy (AzureAD) | Microsoft Learn

Set-AzureADMSGroup (AzureAD) | Microsoft Learn

3.16.7

Videos

Setting Expiration Policies for Teams - YouTube

4.0 Microsoft Exchange

4.1 Automatic Forwarding to External Domains SHALL Be Disabled

This control is intended to prevent bad actors from using client-side forwarding rules to exfiltrate data to external recipients.

4.1.1 Policy

Automatic forwarding to external domains SHALL be disabled

4.1.2 Licensing Considerations

Any tenant with an Exchange Online license can configure this setting.

4.1.3 Set-Up Instructions

To disallow automatic forwarding to external domains:

1. Sign in to the **Exchange admin center.**
2. Select **Mail flow**, then **Remote domains**.
3. Select **Default**.
4. Under **Email reply types**, select **Edit reply types**.
5. **Clear the checkbox** next to Allow automatic forwarding, then click Save.

4.1.4

End-User Impact

Level: Low

With this setting enabled, users will be prevented from setting up any auto-forwarding rules to external domains.

4.1.5

Tips

- N/A

4.1.6

PowerShell Scripts

- Block Auto FW: https://github.com/msp4msps/Security/blob/master/Block%20Auto-FW.ps1
- Block Auto FW Multi-Tenant: https://github.com/msp4msps/Security/blob/master/Block%20Auto-FW_All%20Customers.ps1

4.1.7

Videos

- Block Auto FW with Microsoft 365 BP: https://www.youtube.com/watch?v=kskBq4b2rqo

4.2 Sender Policy Framework SHALL Be Enabled

The Sender Policy Framework (SPF) is a mechanism that allows domain administrators to specify which Internet Protocol (IP) addresses are explicitly approved to send email on behalf of the domain, facilitating detection of spoofed

emails. SPF is not configured through the Exchange admin center, but rather via the Domain Name Service (DNS) records hosted by the organization's domain.

4.2.1

Policy

- A list of approved IP addresses for sending mail SHALL be maintained
- An SPF policy(s) that designates only these addresses as approved senders SHALL be published.

4.2.2

Licensing Considerations

Any tenant can configure this setting.

4.2.3

Set-Up Instructions

Set up SPF to help prevent spoofing - Office 365 | Microsoft Learn

How Sender Policy Framework (SPF) prevents spoofing - Office 365 | Microsoft Learn

Adding SPF records to a domain will vary depending on where the domain is hosted. Follow these steps for configuring an SPF record for Exchange Online.

4.2.4

End-User Impact

Level: Low

Without proper SPF configuration, is possible that users will have their email rejected or marked as spam when sending outbound messages.

4.2.5

Tips

- Optimize SPF Record: How To Optimize SPF Record? v spf1 a mx (easydmarc.com)

4.2.6

PowerShell Scripts

- N/A

4.2.7

Videos

Intro to SPF, DKIM, and DMARC - YouTube

4.3 DomainKeys Identified Mail SHOULD Be Enabled

DomainKeys Identified Mail (DKIM) allows digital signatures to be added to email messages in the message header, providing a layer of both authenticity and integrity to emails. As with SPF, DKIM relies on DNS records; thus, its deployment depends on how an organization manages its DNS. DKIM is enabled for the tenant's default domain (e.g., on microsoft.com domains), but it must be manually enabled for custom domains.

4.3.1

Policy

DKIM SHOULD be enabled for any custom domain.

4.3.2

Licensing Considerations

DKIM signing is included with Exchange Online Protection (EOP), which is included in all Microsoft 365 subscriptions that contain Exchange Online mailboxes.

4.3.3

Set-Up Instructions

How to use DKIM for email in your custom domain - Office 365 | Microsoft Learn

How Sender Policy Framework (SPF) prevents spoofing - Office 365 | Microsoft Learn

Support for validation of Domain Keys Identified Mail (DKIM) signed messages - Office 365 | Microsoft Learn

To enable DKIM, follow the instructions listed on Steps to Create, enable and disable DKIM from Microsoft 365 Defender portal | Microsoft Docs.

1. Navigate to the **Microsoft 365 Defender admin center**.
    a. Go to Policies & Rules.
        i. Go to Threat Policies.
2. Select **DKIM**.
3. Select your domain.
4. Switch **Sign messages for this domain with DKIM signatures** to Enabled.
5. If you are enabling DKIM for the first time, a pop-up window listing Canonical Name (CNAME) records displays. Publish these records to your DNS service provider.
6. Return to the DKIM page on the Defender admin center to finish enabling DKIM.

4.3.4

End-User Impact

Level: Low

While there is no direct impact to end-users, they should experience better outbound mail flow delivery with DKIM in place.

4.3.65

Tips

- N/A

4.3.6

PowerShell Scripts

- N/A

4.3.7

Videos

Intro to SPF, DKIM, and DMARC - YouTube

4.4 Domain-Based Message Authentication, Reporting, and Conformance SHALL Be Enabled

Domain-based Message Authentication, Reporting, and Conformance (DMARC) works with SPF and DKIM to authenticate mail senders and ensure that destination email systems can validate messages sent from your domain. DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF or DKIM checks

4.4.1

Policy

- A DMARC policy SHALL be published for every custom domain.
- The DMARC message rejection option SHALL be “p=reject.”

4.4.2

Licensing Considerations

Any tenant can perform this configuration

4.4.3

Set-Up Instructions

Use DMARC to validate email, setup steps - Office 365 | Microsoft Learn

Use DMARC to validate email, setup steps - Office 365 | Microsoft Learn

DMARC implementation varies depending on how an agency manages its DNS records. See Form the DMARC TXT record for your domain | Microsoft Docs for Microsoft guidance. DMARC records can be requested using the PowerShell tool Resolve-DnsName. For example:

Resolve-DnsName _dmarc.example.com txt

Replace “example.com” in the example with the domain(s) used for your agency’s emails. Ensure that (1) the DNS record exists, (2) “p=reject;” is included in the policy returned from the query

4.4.4

End-User Impact

Level: Low

While there is no direct impact to end-users, they should experience better outbound mail flow delivery with DMARC in place,

4.4.5

Tips

- N/A

4.4.6

PowerShell Scripts

- N/A

4.4.7

Videos

Intro to SPF, DKIM, and DMARC - YouTube

4.5 Enable Email Encryption

Email encryption rules can be added to encrypt a message with defined rules such as having a particular keyword in the subject line or body. Most common is to add “Secure” as the key word in the subject to encrypt the message. M365/O365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.

4.5.1

Policy

- An email encryption policy Shall be configured

4.5.2

Licensing Considerations

To enable this feature, an Azure Information Protection Plan 1 subscription is required which can either be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3

- Microsoft 365 E5

Azure Information Protection service description - Service Descriptions | Microsoft Learn

4.5.3

Set-Up Instructions

Set up Microsoft Purview Message Encryption - Microsoft Purview (compliance) | Microsoft Learn

Add your brand to encrypted messages - Microsoft Purview (compliance) | Microsoft Learn

Follow these steps to configure a transport rule for email encryption.

4.5.4

End-User Impact

Level: Low

End-Users will likely need some instructions on how to use email encryption within the organization. Depending on how you role it out, they may have to type a specific subject line or leverage a built in plug-in that allows them to encrypt the message on demand. Users will need to open encrypted messages in Outlook on the web vs the email client on the desktop.

4.5.5

Tips

- N/A

4.5.6

PowerShell Scripts

- Set up an email encryption rule: https://github.com/msp4msps/Security/blob/master/Email%20Encryption%20Rule.ps1

- Set up an email encryption rule (Multi-Tenant): https://github.com/msp4msps/Security/blob/master/Email%20Encryption%20Rule-All%20Customers.ps1
- Verify Message Encryption: https://learn.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide#verify-microsoft-purview-message-encryption-configuration-in-exchange-online-powershell

4.5.7

Videos

Office 365 Email Encryption - YouTube

Office 365 Email Encryption-Custom Branding - YouTube

4.6 Simple Mail Transfer Protocol Authentication SHALL Be Disabled

Modern email clients that connect to Exchange Online mailboxes—including Outlook, Outlook on the web, iOS Mail, and Outlook for iOS and Android—do not use Simple Mail Transfer Protocol Authentication (SMTP AUTH) to send email messages. SMTP AUTH is only needed for applications outside of Outlook that send email message,

4.6.1

Policy

- SMTP AUTH SHALL be disabled in Exchange Online
- SMTP AUTH MAY be enabled on a per-mailbox basis

4.6.2

Licensing Considerations

This setting can be configured in any Microsoft tenant.

4.6.3

Set-Up Instructions

SMTP AUTH can only be disabled tenant-wide using Exchange Online PowerShell. To do so, follow the instructions listed at Disable SMTP AUTH in your organization | Microsoft Docs.

To enable SMTP AUTH on a per-mailbox basis, follow the instructions listed at Use the Microsoft 365 admin center to enable or disable SMTP AUTH on specific mailboxes | Microsoft Docs.

4.6.4

End-User Impact

Level: Low

This will vary depending on the organization and what existing mail infrastructure looks like. This can be impactful if you have scanners, printers, or Line-of-business (LOB) applications leveraging SMTP auth for message relay. To avoid any issues here, follow these steps.

4.6.5

Tips

- Use the following for configuring SMTP relay for printers, scanners, etc: How to set up a multifunction device or application to send email using Microsoft 365 or Office 365 | Microsoft Learn

4.6.6

PowerShell Scripts

- Changing Modern Auth Settings: https://www.cyberdrain.com/automating-with-powershell-changing-modern-and-basic-authentication-settings/
- Basic Auth Reporting: https://github.com/msp4msps/Basic-Authentication-Reporting

4.6.7

Videos

Enable or Disable SMTP Auth: How to Enable SMTP Authentication in Microsoft 365 | Enable or disable SMTP AUTH in Exchange Online

4.7 Calendar and Contact Sharing SHALL Be Restricted

Exchange Online allows the creation of sharing polices that ease default restrictions on contact and calendar details sharing. These policies should only be enabled with caution and must comply with the following policies.

4.7.1

Policy

- Contact folders SHALL NOT be shared with all domains, although they MAY be shared with specific domains.
- Calendar details SHALL NOT be shared with all domains, although they MAY be shared with specific domains

4.7.2

Licensing Considerations

This setting can be configured in any Microsoft tenant.

4.7.3

Set-Up Instructions

Sharing policies in Exchange Online | Microsoft Learn

Sharing in Exchange Online | Microsoft Learn

To restrict sharing with all domains:

1. Sign in to the **Exchange admin center.**
2. Under Organization, select **Sharing**.
3. Under **Individual Sharing**, for all existing policies, ensure that for all sharing rules, **Sharing with all domains** is not selected.

4.7.4

End-User Impact

Level: Low

With this setting in place, users will not be able to share calendar or contacts to any external domains unless they are whitelisted. A formal request process should be put into place and evaluated when a user needs to share their calendar details.

4.7.5

Tips

- N/A

4.7.6

PowerShell Scripts

- Free/Busy Sharing Settings: https://github.com/msp4msps/Security/blob/master/Free_Busy%20Calendar%20Settings-Single%20Tenant.ps1

- Free/Busy Sharing Settings (Multi-Tenant): https://github.com/msp4msps/Security/blob/master/Free_Busy%20Calendar%20Settings%20Multitenant.ps1

4.7.7

Videos

- None Currently

4.8 External Sender Warnings SHALL Be Implemented

Mail flow rules allow the modification of incoming mail such that mail from external users can be easily identified, for example, by prepending the subject line with "[External]." Seeing this message can help users identify email messages that might be spoofed and mark them as malicious.

4.8.1

Policy

- External sender warnings SHALL be implemented.

4.8.2

Licensing Considerations

This setting can be configured in any Microsoft tenant with Exchange Online.

4.8.3

Set-Up Instructions

Mail flow rules (transport rules) in Exchange Online | Microsoft Learn

To enable external sender warnings:

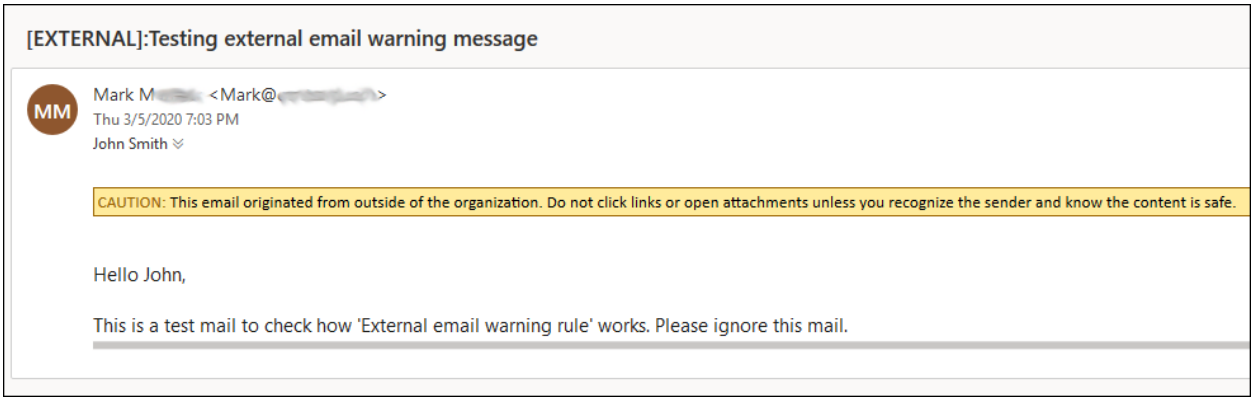
1. Sign in to the **Exchange admin center.**
2. Under **Mail flow**, select **Rules.**
3. Click the plus (+) button to create a new rule.
4. Select **Modify** messages....
5. Give the rule an appropriate name.
6. Under Apply this rule if..., select **The sender is located**....
7. Under select sender location, select **Outside the organization**, then click OK.
8. Under Do the following..., select **Prepend the subject of the message with**....
9. Under specify subject prefix, enter a message such as **"[External]"** (without the quotation marks), then click OK.
10. Under Choose a mode for this rule, select **Enforce**.
11. Click Save

4.8.4

End-User Impact

Level: Low

With this setting in place, users will see a prepended message with each email they get originating outside the organization. Users should be trained to spot these messages in a combination of the from address to identify if the from address is being spoofed.



4.8.5

Tips

- N/A

4.8.6

PowerShell Scripts

- https://adamtheautomator.com/external-email-warning/
- https://lazyadmin.nl/it/add-external-email-warning-to-office-365-and-outlook/
- https://learn.microsoft.com/en-us/powershell/module/exchange/set-externalinoutlook?view=exchange-ps

4.8.7

Videos

- https://www.youtube.com/watch?v=HkQ17gfvltw
- https://www.youtube.com/watch?v=KFWKG_vi13Q

4.9 Data Loss Prevention Solutions SHALL Be Enabled

Data loss prevention (DLP) helps prevent both accidental leakage of sensitive information, as well as intentional exfiltration of data. DLP forms an integral part of securing Microsoft Exchange Online. Microsoft offers DLP services, controlled within the Microsoft 365 compliance admin center.

4.9.1

Policy

- A data loss prevention policy shall be configured that applies to Exchange Online.

4.9.2

Licensing Considerations

To configure data loss prevention policies, one of the following licenses is needed:

- Microsoft 365 Business Premium
- Microsoft 365 E3/E5
- Office 365 E3/E5

4.9.3

Set-Up Instructions

Data loss prevention in Exchange Online | Microsoft Learn

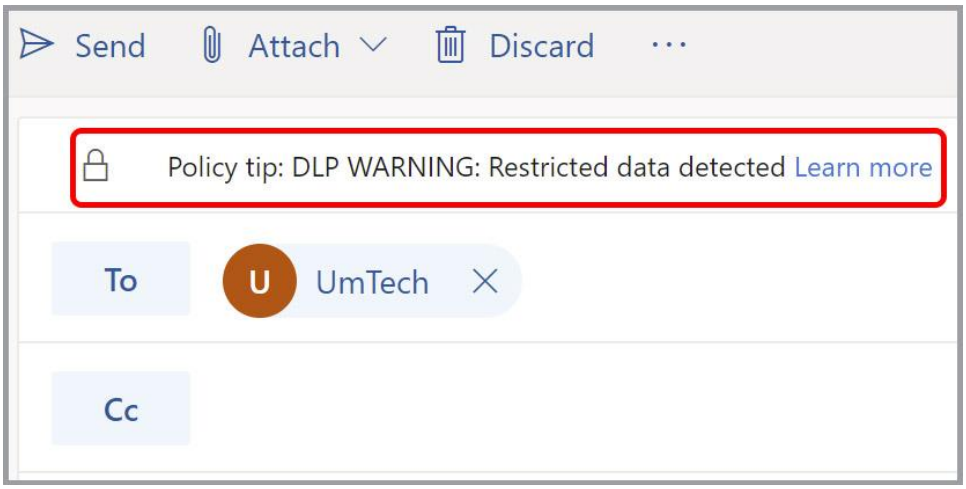
To create a DLP policy for Exchange follow the steps listed here

4.9.4

End-User Impact

Level: Low

With this setting in place, users could have their email rejected depending on the policy definition. For example, if a user is trying to send sensitive information such as credit card info to an external domain, a DLP policy could kick in and block the message from being sent. The user would get a rejection email telling them why the message was blocked. They can also get messaging with policy tips before sending the email if that is configured.



4.9.5

Tips

- N/A

4.9.6

PowerShell Scripts

- https://learn.microsoft.com/en-us/powershell/module/exchange/new-dlpcompliancepolicy?view=exchange-ps

4.9.7

Videos

- https://www.youtube.com/watch?v=q3MhTFLYNAc
- https://www.youtube.com/watch?v=APq399z8YGo

4.10 Emails SHALL Be Filtered by Attachment File Type

For some types of files (e.g., executable files), the dangers of allowing them to be sent over email outweigh any potential benefits. Some services, such as the Common Attachment Filter of Microsoft Defender, filter emails based on the attachment file types. Use of Microsoft Defender for this purpose is not strictly required; instead, equivalent products that fulfill the requirements outlined in this baseline setting may be used

4.10.1

Policy

- Emails SHALL be filtered by the file types of included attachments
- Disallowed file types SHALL be determined and set. At a minimum, click-to-run files SHOULD be blocked (e.g., .exe, .cmd, and .vbe).

4.10.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.10.3

Set-Up Instructions

Configure anti-malware policies - Office 365 | Microsoft Learn

Anti-malware protection - Office 365 | Microsoft Learn

To enable common attachments filter in the default policy:

1. Sign in to **Microsoft 365 Defender.**

2. Under Email & collaboration, select **Policies & rules.**
3. Select **Threat policies**.
4. Under Policies, select **Anti-malware.**
5. Select the Default (Default) policy.
6. Click **Edit protection settings**.
7. Check Enable the **common attachments filter**.
8. Click Customize file types as needed.
9. Click Save.

4.10.4

End-User Impact

Level: Low

With this setting in place, users will not be able to receive attachments specified in the policy.

4.10.5

Tips

- N/A

4.10.6

PowerShell Scripts

- https://learn.microsoft.com/en-us/powershell/module/exchange/set-malwarefilterpolicy?view=exchange-ps

4.10.7

Videos

- https://www.youtube.com/watch?v=R-0YVW6pNt4

4.11 Zero-Hour Auto Purge for Malware SHOULD Be Enabled

This setting determines whether emails can be quarantined automatically after delivery to a user's mailbox (e.g., in the case of a match with an updated malware classification rule).

4.11.1

Policy

Zero-hour auto purge (ZAP) for malware SHOULD be enabled in the default antimalware policy and in all existing custom policies.

4.11.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.11.3

Set-Up Instructions

Configure anti-malware policies - Office 365 | Microsoft Learn

To enable ZAP:

1. Sign in to **Microsoft 365 Defender**.
2. Under Email & collaboration, select **Policies & rules.**
3. Select **Threat policies.**
4. Under **Policies, select Anti-malware.**

5. Select the Default (Default) policy.
6. Click Edit **protection settings**.
7. Check **Enable zero-hour** auto purge for malware (Recommended).
8. Click Save.

4.11.4

End-User Impact

Level: Low

With this setting in place, users will have certain email messages removed from their mailbox if they are detected as malware.

4.11.5

Tips

- N/A

4.11.6

PowerShell Scripts

- https://learn.microsoft.com/en-us/powershell/module/exchange/set-malwarefilterpolicy?view=exchange-ps

4.11.7

Videos

- https://www.youtube.com/watch?v=R-0YVW6pNt4

4.12 Phishing Protections SHOULD Be Enabled

There are multiple ways to protect against phishing, including impersonation protection, mailbox intelligence and safety tips. Impersonation protection checks incoming emails to see if the sender address is similar to the users or domains on an agency-defined list. If the sender address is significantly similar, as to indicate an impersonation attempt, the email is quarantined. Mailbox intelligence is an artificial intelligence (AI)-based tool for identifying potential impersonation attempts

4.12.1

Policy

- User impersonation protection SHOULD be enabled for key agency leaders.
- Domain impersonation protection SHOULD be enabled for domains owned by the agency.
- Domain impersonation protection SHOULD be added for frequent partners.
- Trusted senders and domains MAY be added in the event of false positives.
- Intelligence for impersonation protection SHALL be enabled.
- Message action SHALL be set to quarantine if the message is detected as impersonated.
- Mail classified as spoofed SHALL be quarantined.
- All safety tips SHALL be enabled, including:
    - – first contact.
    - – user impersonation.
    - – domain impersonation.
    - – user impersonation unusual characters.
    - – “?” for unauthenticated senders for spoof.
    - – “via” tag.
- The above configurations SHALL be set in the default policy and SHOULD be set in all existing custom policies.

4.12.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.12.3

Set-Up Instructions

Configure anti-phishing policies in EOP - Office 365 | Microsoft Learn

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies**.
4. Under Policies, select **Anti-phishing.**
5. Select the Office365 **AntiPhish Default** (Default) policy.
6. Click Edit **protection settings.**
7. Check **Enable users to protect.**
8. Click Manage sender(s), then add users that merit impersonation protection.
9. Check **Enable domains** to protect.
10. Check Include domains I own.
11. Check Include custom domains.
12. Click **Manage custom domains(s)** to add the domains of frequent partners.
13. Check Enable mailbox intelligence (Recommended).
14. Check Enable Intelligence for impersonation protection (Recommended).

4.12.4

End-User Impact

Level: Medium

With this setting in place, users will better protection against spoofing attempts against their email. With additional protections, there is a higher chance of false

positives that could negatively impact the user in which they do not receive legitimate mail.

4.12.5

Tips

- N/A

4.12.6

PowerShell Scripts

- https://learn.microsoft.com/en-us/powershell/module/exchange/set-antiphishpolicy?view=exchange-ps

4.12.7

Videos

- https://www.youtube.com/watch?v=UYRkY0eRmGc

4.13 Inbound Anti-Spam Protections SHALL Be Enabled

There are several features that protect against inbound spam: bulk compliant level, quarantines, safety tips, and zero hour auto purge.

4.13.1

Policy

- The bulk complaint level (BCL) threshold SHOULD be set to six or lower.
- Spam and high confidence spam SHALL be moved to either the junk email folder or the quarantine folder.

- Phishing and high confidence phishing SHALL be quarantined.
- Bulk email SHOULD be moved to either the junk email folder or the quarantine folder.
- Spam in quarantine SHOULD be retained for at least 30 days.
- Spam safety tips SHOULD be turned on.
- Zero-hour auto purge (ZAP) SHALL be enabled for both phishing and spam messages.
- Allowed senders MAY be added, but allowed domains SHALL NOT be added.
- The previously listed configurations SHALL be set in the default policy and SHOULD be set in all existing custom policies.

4.13.2

Licensing Considerations

This setting can be configured with any tenant that has Exchange Online.

4.13.3

Set-Up Instructions

Configure spam filter policies - Office 365 | Microsoft Learn

Microsoft recommendations for EOP and Defender for Office 365 security settings - Office 365 | Microsoft Learn

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules**.
3. Select **Threat policies.**
4. Under **Policies, select Anti-spam**.
5. Select **Anti-spam inbound policy** (Default).
6. Under Bulk email threshold & spam properties, click **Edit spam threshold** and properties.
7. Set **Bulk email threshold** to six or lower.
8. Click Save.
9. Under Actions, click **Edit actions.**
10. In the Message actions section:
    a. For Spam, High confidence spam, and Bulk, set the action to either Move message to Junk Email folder or Quarantine message.

b. Set the action for both Phishing and High confidence phishing to Quarantine message.
c. Set Retain spam in quarantine for this many days to “30.”
d. Check Enable spam safety tips.
e. Check Enable zero-hour auto purge (ZAP), Enable for phishing messages, and Enable for spam messages.

11. Click Save.

.4.13.4

End-User Impact

Level: Medium

With this setting in place, its possible that false positives will be generated and users will need to look either in their junk folder or have an admin release a message from quarantine that is legitimate.

4.13.5

Tips

- Educate users on how to make request for quarantined messages to be released

4.13.6

PowerShell Scripts

Configure spam filter policies - Office 365 | Microsoft Learn

4.13.7

Videos

Anti Spam Policies - Microsoft Defender for Office 365 | Configure Inbound & Outbound Spam policies. - YouTube

4.14 Safe Link Policies SHOULD Be Enabled

When enabled, URLs in emails are rewritten by prepending:

https://*.safelinks.protection.outlook.com/?url=

to the original URL. This change can only be seen by either clicking the URL or copying and pasting it; the end-user, even when hovering over the URL in their email, will still only see the original URL. By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy can perform the following:

- Compare the URL with a block list.
- Compare the URL with a list of know malicious sites.
- If the URL points to a downloadable file, apply real-time file scanning.

If all checks pass, the user is redirected to the original URL

4.14.1

Policy

- The Safe Links Policy SHALL include all agency domains—and by extension—all users.
- URL rewriting and malicious link click checking SHALL be enabled.
- Malicious link click checking SHALL be enabled with Microsoft Teams.
- Real-time suspicious URL and file-link scanning SHALL be enabled.
- URLs SHALL be scanned completely before message delivery.
- Internal agency email messages SHALL have safe links enabled.
- User click tracking SHALL be enabled.
- Safe Links in Office 365 apps SHALL be turned on.
- Users SHALL NOT be enabled to click through to the original URL.

4.14.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.14.3

Set-Up Instructions

Complete Safe Links overview for Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

Set up Safe Links policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

1. Sign in to **Microsoft 365 Defender**.
2. Under **Email & collaboration**, select **Policies & rules.**
3. Select **Threat policies.**
4. Under Policies, select **Safe Links.**
5. Create a Safe Links Policy.
    a. Assign the new policy an appropriate name and description.
    b. Include all tenant domains. All users under those domains will be added.
    c. On the **URL & click protection** settings page:
        i. Select **On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.**
        ii. Select **Apply Safe Links to email messages sent within the organization.**
        iii. Select **Apply real-time URL scanning for suspicious links and links that point to files**.
        iv. Select **Wait for URL scanning to complete before delivering the message.**
    d. On the **URL & click protection settings** page, under Teams, select **On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten**.

e. On the **URL & click protection settings page**, under Office 365 Apps, select On: Safe Links checks a list of known, malicious links when users click links in Microsoft Office Apps. **URLs are not rewritten.**
f. On the URL & click protection settings page, under **Click protection settings**:
    i. Select **Track User Clicks.**
    ii. Do not select **Let users click through to the original URL**.
g. Review the new policy, then click Submit.

.4.14.4

End-User Impact

Level: Medium

With this setting in place, there may be some latency in email flow while the URL is being scanned before delivery. When users click on a link and the link is found to be malicious, users will get a page describing the malicious link and will not be able to proceed to the webpage.

4.14.5

Tips

- N/A

4.14.6

PowerShell Scripts

Set up Safe Links policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

Security/ATP Implementation.ps1 at master · msp4msps/Security (github.com)

4.14.7

Videos

Best Practices for Safe Links and Safe Attachments - YouTube

Protect against malicious links with Safe Links in Microsoft Defender for Office 365 - YouTube

4.15 Safe Attachments SHALL Be Enabled

The Safe Attachments will scan messages for attachments with malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment. The process then uses machine learning and analysis techniques to detect malicious intent. Enabling this feature may slow down message delivery to the user due to the scanning.

4.15.1

Policy

- At least one Safe Attachments Policy SHALL include all agency domains—and by extension—all users.
- The action for malware in email attachments SHALL be set to block.
- Redirect emails with detected attachments to an agency-specified email SHOULD be enabled.

4.15.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.15.3

Set-Up Instructions

Safe Attachments - Office 365 | Microsoft Learn

Set up Safe Attachments policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

To configure safe attachments for Exchange Online, follow the instructions listed on Use the Microsoft 365 Defender portal to create Safe Attachments policies.

1. Sign in to **Microsoft 365 Defender.**
2. Under **Email & collaboration**, select **Policies & rules.**
3. Select **Threat policies.**
4. Under Policies, select **Safe Attachments**.
5. Click **Create** to start a new policy.
6. Give the new policy an appropriate name and description.
7. Under domains, enter all organization tenant domains. All users under these domains will be added to the policy.
8. Under Safe Attachments unknown malware response, select **Block.**
9. Set the Quarantine policy to **AdminOnlyAccessPolicy.**
10. Click Next, then Submit.

.4.15.4

End-User Impact

Level: Low

With this setting in place, there may be some latency in email flow while the attachment is being scanned before delivery. If the attachment is found to be malicious, the email will be blocked from sending.

4.15.5

Tips

- N/A

4.15.6

PowerShell Scripts

Set up Safe Attachments policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Learn

Security/ATP Implementation.ps1 at master · msp4msps/Security (github.com)

4.15.7

Videos

Best Practices for Safe Links and Safe Attachments - YouTube

Creating Safe Attachment Policies - YouTube

How to set up ATP safe attachments in Microsoft 365 for business - YouTube

4.16 IP Allow Lists SHOULD NOT be Implemented

Microsoft Defender supports the creations of IP “allow lists,” which are intended to ensure that emails from specific senders are not blocked. However, as a result, emails from these senders bypass important security mechanisms, such as spam filtering, SPF, DKIM, DMARC, and FROM address enforcement.

IP “block lists” ensure that mail from these IP addresses is always blocked. Although we have no specific guidance on which IP addresses to add, block lists can be used to block mail from known spammers. The IP “safe lists” group is a dynamic list of “known, good senders,” which Microsoft sources from various third-party subscriptions. As with senders in the allow list, emails from these senders bypass important security mechanisms.

4.16.1

Policy

- IP allow lists SHOULD NOT be created.
- Safe lists SHOULD NOT be enabled.
- A connection filter MAY be implemented to create an IP “block list.”

4.16.2

Licensing Considerations

- Exchange Online Protection

4.16.3

Set-Up Instructions

Create safe sender lists - Office 365 | Microsoft Learn

Configure the default connection filter policy - Office 365 | Microsoft Learn

To modify the connection filters, follow the instructions found on Use the Microsoft 365 Defender portal to modify the default connection filter policy.

1. Sign in to **Microsoft 365 Defender.**
2. Under **Email & collaboration**, select **Policies & rules**.
3. Under **Policies**, select **Anti-spam**.
4. Select **Connection filter policy** (Default).
5. Click Edit connection filter policy.
6. Ensure no addresses are specified under **Always allow messages from the following IP addresses or address range.**
7. Enter addresses under **Always block messages from the following IP addresses or address range as needed.**
8. Ensure **Turn on safe list** is not selected.

4.16.4

End-User Impact

Level: Low

With this setting in place, there may be some false positives from IP addresses that are seen as malicious.

4.16.5

Tips

- N/A

4.16.6

PowerShell Scripts

Configure the default connection filter policy - Office 365 | Microsoft Learn

4.16.7

Videos

What is Connection Filter | Microsoft Defender for Office 365 | Exchange Online Protection (EOP) - YouTube

4.17 Mailbox Auditing SHALL Be Enabled

Mailbox auditing helps users investigate compromised accounts or discover illicit access to Exchange Online. Some actions performed by administrators, delegates, and owners are logged automatically. While mailbox auditing is enabled by default, organizations should ensure that it has not been inadvertently disabled.

4.17.1

Policy

Mailbox auditing SHALL be enabled

4.17.2

Licensing Considerations

- Exchange Online Protection

4.17.3

Set-Up Instructions

Mailbox auditing can be enabled from the Exchange Online PowerShell. Follow the instructions listed on Manage mailbox auditing in Office 365.

4.17.4

End-User Impact

Level: None

There is no end-user impact for this setting

4.17.5

Tips

- N/A

4.17.6

PowerShell Scripts

https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide

To check the current mailbox auditing status via PowerShell:

1. Connect to the Exchange Online PowerShell.

2. Run the following command:
    a. Get-OrganizationConfig | Format-List AuditDisabled.

To enable mailbox auditing via PowerShell:

1. Connect to the Exchange Online PowerShell
2. Run the following command:
    a. Set-OrganizationConfig –AuditDisabled $false.

4.17.7

Videos

Enable Mailbox Auditing - YouTube

4.18 Alerts SHALL Be Enabled

Microsoft Defender includes several prebuilt alert policies, many of which pertain to Exchange Online. These alerts give admins better real-time insight into possible security incidents.

4.18.1

Policy

At a minimum, the following alerts SHALL be enabled:

- Suspicious email sending patterns detected.
- Suspicious connector activity
- Suspicious email forwarding activity.
- Unusual increase in email reported as phish.
- Messages have been delayed.
- Tenant restricted from sending unprovisioned email.
- Tenant restricted from sending email.
- Malware campaign detected after delivery.
- A potentially malicious URL click was detected.

The alerts SHOULD be sent to a monitored address or incorporated into a security incident and event management (SIEM) tool.

4.18.2

Licensing Considerations

This setting requires Defender for Office 365 Plan 1 or Plan 2 which can be purchased standalone or as part of the following bundles:

- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

4.18.3

Set-Up Instructions

Microsoft 365 alert policies - Microsoft Purview (compliance) | Microsoft Learn

1. Sign in to **Microsoft 365 Defender.**
2. Under **Email & collaboration**, select **Policies & rules.**
3. Select **Alert Policy.**
4. Click the policy name.
    a. Ensure Status is set to **On**.
    b. Ensure Email recipients includes **at least one monitored address**

4.18.4

End-User Impact

Level: None

There is no end-user impact for this setting

4.18.5

Tips

- N/A

4.18.6

PowerShell Scripts

New-ProtectionAlert (ExchangePowerShell) | Microsoft Learn

4.18.7

Videos

How To Create Alert Policy In Exchange Online In Office 365 Step By Step Full Information - YouTube

4.19 Audit Logging SHALL Be Enabled

To view data in threat protection reports, email security reports, and Explorer, audit logging must be turned on. By default, Microsoft retains the audit logs for only 90 days.

4.19.1

Policy

Audit logging SHALL be enabled.

4.19.2

Licensing Considerations

By default, Microsoft retains the audit logs for only 90 days for every Microsoft Tenant

Advanced audit capabilities, including the creation of a custom audit log retention policy, requires E5/G5 licenses or E3/G3 licenses with add-on compliance licenses. Additionally, maintaining logs in the Microsoft 365 environment for longer than one year requires an add-on license. For more information, see Licensing requirements | Microsoft Docs.

4.19.3

Set-Up Instructions

Auditing can be enabled from the Microsoft 365 compliance admin center and the Exchange Online PowerShell. Follow the instructions listed on Turn on auditing.

1. Sign in to the Microsoft 365 compliance admin center.
2. Under Solutions, select Audit.
3. If auditing is not enabled, a banner displays and prompts that the user and admin activity start being recorded.
4. Click the Start recording user and admin activity banner.

To set up advanced audit, see Set up Advanced Audit in Microsoft 365 | Microsoft Docs.

To create an audit retention policy, follow the instructions listed on Create an audit log retention policy.

4.19.4

End-User Impact

Level: None

There is no end-user impact for this setting.

4.19.5

Tips

- N/A

4.19.6

PowerShell Scripts

To check the current logging status via PowerShell:

1. Connect to the Exchange Online PowerShell.
2. Run the following command:
    a. Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled.

To enable logging via PowerShell:

1. Connect to the Exchange Online PowerShell.
2. Run the following command:
    a. Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true.

4.19.7

Videos

Microsoft 365 audit logging and monitoring - YouTube

How to use audit log search in office 365 - YouTube

4.20 Enhanced Filtering Shall be configured if a 3rd party email filtering tool is being used

Enhanced email filtering can be set up if you have a connector in 365 (3rd party email filtering service or hybrid configuration) and your MX record does not point to Microsoft 365 or Office 365. This new feature allows you to filter email based on the actual source of messages that arrive over the connector. This is also known as skip listing and this feature will allow you to overlook, or skip, any IP addresses that are considered internal to you in order to get the last known external IP address, which should be the actual source IP address.

If you are using Defender for Office 365, this will enhance its machine learning capabilities and security around safe links/safe attachments/anti-spoofing from Microsoft's known malicious list based off IP. In a way, you are getting a secondary

layer of protection by allowing Microsoft to view the IPs of the original email and check against their database.

4.20.1

Policy

Enhanced Filtering Shall be configured if a 3rd party email filtering tool is being used

4.20.2

Licensing Considerations

Exchange Online Protection

4.20.3

Set-Up Instructions

Enhanced filtering for connectors in Exchange Online | Microsoft Learn

Follow these steps to configure Enhanced Filtering for Connectors on an inbound connector.

4.20.4

End-User Impact

Level: Low

There is no end-user impact for this setting. Depending on the providers, there may be some false positives that restrict legitimate mail to end-users.

4.20.5

Tips

- N/A

4.20.6

PowerShell Scripts

Enhanced filtering for connectors in Exchange Online | Microsoft Learn

4.20.7

Videos

None Currently

5.0 SharePoint Online

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

This policy ensures that when sharing files in SharePoint, there are several possible scopes, including agency-wide or “anyone with the link.”

5.1.1

Policy

File and folder links default sharing setting SHALL be set to “Specific People (Only the People the User Specifies).”

5.1.2

Licensing Considerations

Any tenant with SharePoint online licensing can access this setting.

5.1.3

Set-Up Instructions

Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Learn

In the SharePoint admin center:

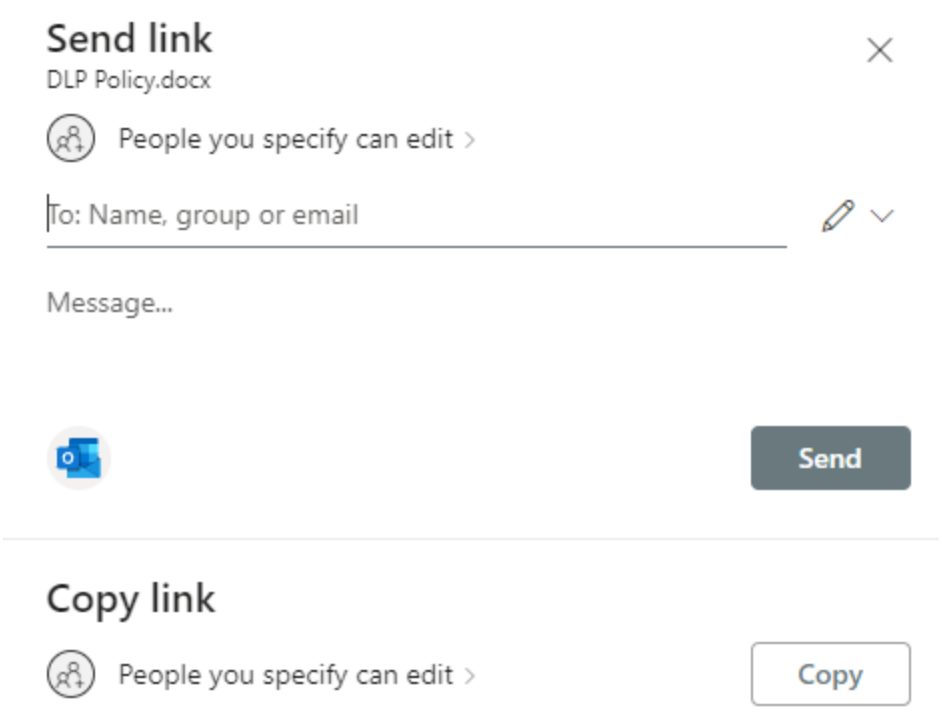
1. In the left-hand navigation bar, click **Policies** -> **Sharing** to display sharing settings.
2. Under File and folder links, ensure that the default link type is set to **Specific people (only the people the user specifies).**

5.1.4

End-User Impact

Level: Low

With this setting enabled, users will have to specify users that can access the link. If the link is forwarded to other users internally or externally, those users will not be able to access the link.



5.1.5

Tips

- N/A

5.1.6

PowerShell Scripts

Set-SPOTenant (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

5.1.7

Videos

Direct Access vs. Sharing Link in SharePoint Online - YouTube

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.

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends allowlisting by domains and security groups per interagency collaboration needs. Note: Adjusting this setting will adjust external sharing for OneDrive and Teams to the same, selected level. OneDrive and Teams can be less permissive (not more permissive) than SharePoint Online. Adding approved domains and/or security groups will also be reflected in One Drive external sharing settings.

5.2.1

Policy

External sharing SHOULD be limited to approved domains and security groups per interagency collaboration needs.

5.2.2

Licensing Considerations

Any tenant with SharePoint online licensing can access this setting.

5.2.3

Set-Up Instructions

Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Learn

To adjust sharing settings, in the SharePoint admin center:

1. Select **Policies** -> **Sharing.**
2. Adjust external sharing slider to **New and Existing Guests**.
3. Expand More external sharing settings.
4. Select **Limit external sharing by domain**.
5. Select **Add domains.**

6. Add domains.
7. Select Save.
8. Select **Allow only users in specific security groups to share externally.**
9. Select **Manage security groups**.
10. Add security groups.
11. Select Save.

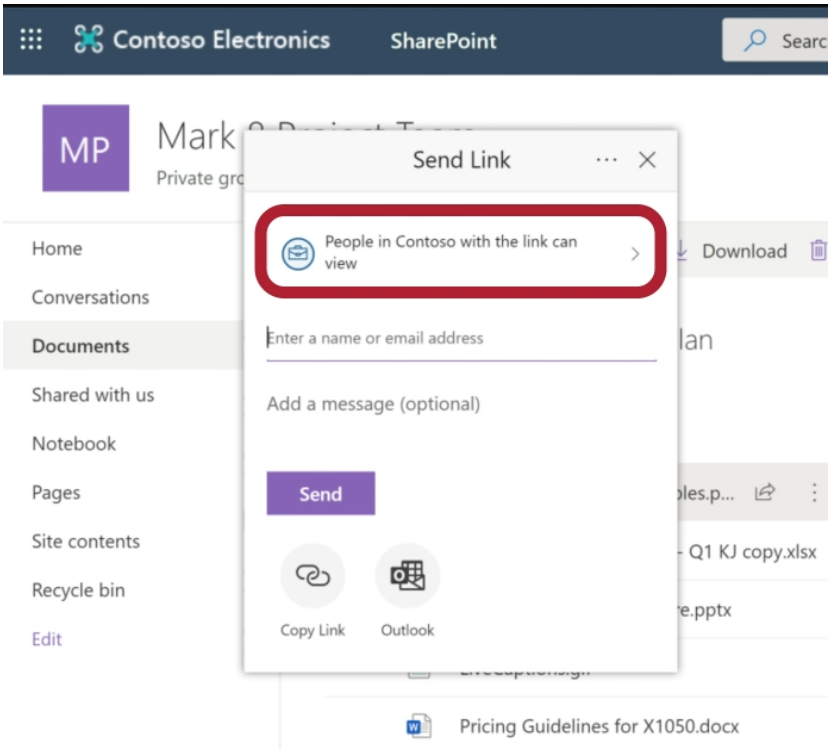
5.2.4

End-User Impact

Level: High

With this setting enabled, users will not be able to share external links unless:

- External users are added as guest to the organization
- External user domains are added to the SharePoint setting
- Users are added to the specified security groups so they can send to external users



5.2.5

Tips

- There should be a formal request process for adding domains and being added to a security group.

5.2.6

PowerShell Scripts

Set-SPOTenant (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

5.2.7

Videos

Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Learn

5.3 Sensitive SharePoint Sites SHOULD Adjust Their Default Sharing Settings to Those Best Aligning to Their Sensitivity Level

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends outside of the default organizational settings agencies should evaluate each created site and adjust sharing settings best aligned to their respective sensitivity level.

5.3.1

Policy

Sharing settings for specific SharePoint sites SHOULD align to their sensitivity level

5.3.2

Licensing Considerations

Any tenant with SharePoint online licensing can access this setting.

5.3.3

Set-Up Instructions

Managing SharePoint Online Security: A Team Effort | Microsoft Learn

To limit external sharing by domain, in the SharePoint admin center:

1. Select **Sites**.
2. Select **Active sites**.
3. Select **Site name.**
4. Select **Add domains**.
5. Select **Policies**.
6. Under **external sharing**, select Edit.
7. Select permissions aligning to the risk posture associated with the sensitivity of the SharePoint site.
8. Select **Save.**

5.3.4

End-User Impact

Level: Medium

Depending on the selection here, users will be restricted in sharing links of documents within the SharePoint Site.

5.3.5

Tips

- There should be guidance provided on document repository structure.
- Leverage some type of form for when users want to create a new SharePoint site to see if it will contain sensitive information.

5.3.6

PowerShell Scripts

Set-SPOSite (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

5.3.7

Videos

Unlock the Secret to SharePoint External Sharing! - YouTube

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

SharePoint allows sharing with users who are outside the agency, which is convenient but may pose a data loss or other information security risk. This working group recommends setting an expiration time for guest access to the site or OneDrive

5.4.1

Policy

- Expiration timers for 'guest access to a site or OneDrive' and 'people who use a verification code' SHOULD be set.
- Expiration timers SHOULD be set to 30 days.

5.4.2

Licensing Considerations

Any tenant with SharePoint online licensing can access this setting.

5.4.3

Set-Up Instructions

Managing SharePoint Online Security: A Team Effort | Microsoft Learn

To limit external sharing by domain, in the SharePoint admin center:

1. Select **Policies** -> **Sharing.**
2. Expand More **external sharing settings**.
3. Select **Guest access to a site or OneDrive will expire automatically after this many days.**
4. Enter “30” days.
5. Select **People who use a verification code must reauthenticate after this many days.**
6. Enter “30” days.

5.4.4

End-User Impact

Level: Low

- Users may have to reshare new links if the existing ones expire before the interaction with external users is complete.

5.4.5

Tips

- N/A

5.4.6

PowerShell Scripts

Set-SPOSite (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

Best practices for unauthenticated sharing | Microsoft Learn

5.4.7

Videos

- None Currently

5.5 Users SHALL Be Prevented from Running Custom Scripts

Allowing users to run custom scripts can potentially allow malicious scripts to run in a trusted environment. For this reason, running custom scripts should not be allowed

5.5.1

Policy

Users SHALL be prevented from running custom scripts

5.5.2

Licensing Considerations

Any tenant with SharePoint online licensing can access this setting.

5.5.3

Set-Up Instructions

Allow or prevent custom script - SharePoint in Microsoft 365 | Microsoft Learn

In the SharePoint Classic admin center:

1. Scroll to the **Custom Script setting** and select both of the following:
    a. Prevent users from running custom script on personal sites.
    b. Prevent users from running custom script on self-service created sites.

5.5.4

End-User Impact

Level: Low

There shouldn't be many users looking to run custom scripts in SharePoint

5.5.5

Tips

- N/A

5.5.6

PowerShell Scripts

Allow or prevent custom script - SharePoint in Microsoft 365 | Microsoft Learn

5.5.7

Videos

- None Currently

6.0 OneDrive

6.1 Anyone Links SHOULD Be Turned Off

Unauthenticated sharing (Anyone links) is used to share data without authentication and users are free to pass it on to others outside the agency. To prevent users from unauthenticated sharing of content, turn off Anyone sharing for users outside the tenant when accessing content in SharePoint, Groups, or Teams

6.1.1 Policy

Anyone links SHOULD be disabled.

6.1.2 Licensing Considerations

Any tenant with OneDrive for Business licensing can access this setting.

6.1.3 Set-Up Instructions

Limit accidental exposure | Microsoft Learn

Note: OneDrive settings can be more restrictive than the SharePoint setting, but not more permissive.

To turn off Anyone links for the agency:

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, expand **Policies**, then select **Sharing**.

3. Set the SharePoint **external sharing settings** to New and existing guests, then set **OneDrive to New and existing guests**.
4. Click Save.

6.1.4

End-User Impact

Level: Medium

With this setting enabled, users will have to specify users that can access the link. If the link is forwarded to other users internally or externally, those users will not be able to access the link.

End-User Notification Template

6.1.5

Tips

- A formal process should be put into place for requesting guest users and sharing company data.

6.1.6

PowerShell Scripts

Set-SPOSite (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

6.1.7

Videos

- None Currently

6.2 Expiration Date SHOULD Be Set for Anyone Links

Files that are stored in SharePoint sites, Groups, and Teams for months and years could lead to unexpected modifications to files if shared with unauthenticated people. Configuring expiration times for Anyone links can help avoid unwanted changes. If Anyone links are enabled, the expiration date SHOULD be set to thirty days or as determined by mission needs or agency policy.

6.2.1 Policy

- An expiration date SHOULD be set for Anyone links.
- Expiration date SHOULD be set to thirty days.

6.2.2 Licensing Considerations

Any tenant with OneDrive for Business licensing can access this setting.

6.2.3 Set-Up Instructions

Best practices for unauthenticated sharing | Microsoft Learn

To set an expiration date for Anyone links across the agency (Note: Anyone links must be enabled).

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, expand **Policies**, and then select **Sharing**.
3. Under **Choose expiration and permissions options for Anyone links**, select the These **links must expire within this many days check box**.
4. Enter the **number of days in the box**, and then click Save.

6.2.4

End-User Impact

Level: Low

Users may have to reshare new links if the existing ones expire before the interaction with external users is complete.

6.2.5

Tips

- N/A

6.2.6

PowerShell Scripts

Set-SPOSite (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

6.2.7

Videos

- None Currently

6.3 Link Permissions SHOULD Be Set to Enabled Anyone Links to View

The Anyone links default to allow people to edit files, as well as edit and view files and upload new files to folders. To allow unauthenticated sharing but keep unauthenticated people from modifying the agency's content, consider setting the file and folder permissions to View

6.3.1

Policy

Anyone link permissions SHOULD be limited to View.

6.3.2

Licensing Considerations

Any tenant with OneDrive for Business licensing can access this setting.

6.3.3

Set-Up Instructions

Best practices for unauthenticated sharing | Microsoft Learn

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, expand **Policies,** then select **Sharing**.
3. Under **Advanced settings** for Anyone links, set the file and folder permissions to **View**.

6.3.4

End-User Impact

Level: Low

Users may have to request additional permissions to share editable documents with Anyone links.

6.3.5

Tips

- N/A

6.3.6

PowerShell Scripts

Set-SPOSite (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

6.3.7

Videos

- None Currently

6.4 OneDrive Client SHALL Be Restricted to corporate owned devices

Windows and MacOS devices should be prevented from syncing the OneDrive Client on devices that are personally owned. These devices may not be joined to the corporate domain and have a highly likelihood of being compromised without the corporations security implemented.

6.4.1

Policy

OneDrive Client Sync for Windows and MacOS SHALL be restricted to corporate owned devices.

6.4.2

Licensing Considerations

Any tenant with OneDrive for Business licensing can access this setting.

6.4.3

Set-Up Instructions

Allow syncing only on computers joined to specific domains - SharePoint in Microsoft 365 | Microsoft Learn

SharePoint and OneDrive unmanaged device access controls for administrators - SharePoint in Microsoft 365 | Microsoft Learn

1. Open the **SharePoint admin center.**
2. In the left-hand navigation pane, select **Settings** and sign in with an account that has admin permissions for the agency.
3. Select **Sync.**
4. Select the **Allow syncing only on computers joined to specific domains** check box.
5. Add the Globally Unique Identifier (GUID) of each domain for the member computers that the agency wants to be able to sync.
    a. Note: Add the domain GUID of the computer domain membership. If users are in a separate domain, only the domain GUID that the computer account is joined to is required.
    b. Important: This setting is only applicable to Active Directory domains. It does not apply to Azure Active Directory (AAD) domains. If agency devices are only Azure AD joined, consider using a Conditional Access Policy instead.
6. Click **Save**

6.4.4

End-User Impact

Level: Low

Users will be prevented from syncing OneDrive or a SharePoint site to their local device if that device is not corporate owned.

6.4.5

Tips

- N/A

6.4.6

PowerShell Scripts

Set-SPOTenantSyncClientRestriction (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

6.4.7

Videos

How to Restrict OneDrive & SharePoint to PC's Joined to Specific Domains - YouTube

6.5 Legacy Authentication SHALL Be Blocked

Modern authentication, based on Active Directory Authentication Library (ADAL) and Open Authorization 2 (OAuth2), is a critical component of security in Office 365. It provides the device authentication and authorization capability of Office 365, which is a foundational security component. If modern authentication is not required, this creates a loophole that could allow unauthorized devices to connect to OneDrive and download/exfiltrate enterprise data. For this reason, it is important to make sure that only apps that support modern authentication are allowed to connect, assuring that only authorized devices are allowed to access enterprise data.

6.5.1

Policy

Legacy Authentication SHALL be blocked for OneDrive and SharePoint

6.5.2

Licensing Considerations

Any tenant with OneDrive for Business licensing can access this setting.

6.5.3

Set-Up Instructions

1. Open the **SharePoint admin center**.
2. In the left-hand navigation pane, click **Policies** > Access Control > **Device access**.
3. Click **Apps that don't use modern authentication** to display the device access settings.
4. On the Apps that don't use modern authentication page, select the **Block access option**

Note to this can be accomplished through a Conditional Access Policy as well

6.5.4

End-User Impact

Level: Low

There should not be many users trying to access OneDrive or SharePoint documents with apps that do not use modern authentication

6.5.5

Tips

- If you have a Conditional Access Policy set up to block legacy authentication, this setting is not necessary

6.5.6

PowerShell Scripts

Set-SPOTenantSyncClientRestriction (Microsoft.Online.SharePoint.PowerShell) | Microsoft Learn

6.5.7

Videos

Securing the Remote Workforce- SharePoint and OneDrive - YouTube

7.0 Intune

7.1 Personal Devices should be restricted from enrolling into the MDM solution

By default, any device can enroll into Intune whether or not it is classified as corporate or personal. To prevent device users from accidently enrolling their personal device, device restrictions should be configured. Users should only be enrolling corporate owned devices that have specifications that meet corporate standards.

7.1.1 Policy

- Device restrictions should be configured to restrict personal devices from enrolling in the MDM solution
- Only device types (i.e. Windows, Linux, macOS, etc.) defined by the corporation shall be supported for Intune enrollment

7.1.2 Licensing Considerations

Any tenant with Intune licensing can access this setting.

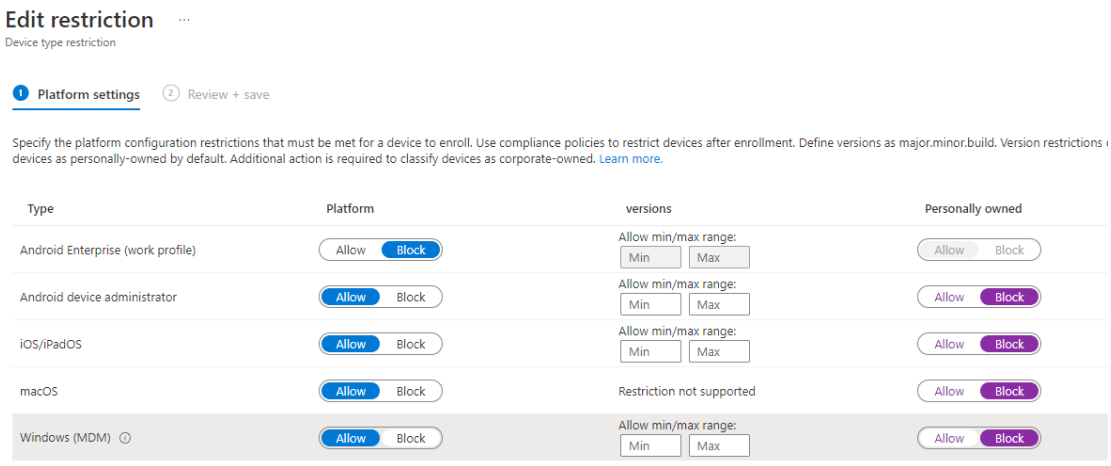
7.1.3 Set-Up Instructions

Overview of enrollment restrictions - Microsoft Intune | Microsoft Learn

Create device platform restrictions - Microsoft Intune | Microsoft Learn

To block personally owned devices from enrolling into Intune:

1. Follow the steps outlined here
2. Under Personally-Owned, select **Block** for each device type



7.1.4

End-User Impact

Level: Medium

Users will not be able to enroll any device that is classified as personal. If you have Windows autoenrollment enabled, users will be prompted to enroll their devices when access common office applications like Teams. If they select Yes to enroll the device and the device is personally owned, they will be prevented from enrolling that device.

7.1.5

Tips

- N/A

7.1.6

PowerShell Scripts

powershell-intune-samples/EnrollmentRestrictions at master · microsoftgraph/powershell-intune-samples (github.com)

7.1.7

Videos

MIH07 - Setup your Microsoft Intune Tenant - Enrolment restrictions and device settings - YouTube

7.2 Devices shall be deleted that haven't checked in for over 30 days

By default, no devices are removed from Intune no matter the level of inactivity. In order to ensure an inventory of active authorized devices, device clean-up rules should be configured to automatically delete devices that have not checked in for over 30 days.

7.2.1

Policy

- Devices are deleted from Intune if they have not checked in for over 30 days

7.2.2

Licensing Considerations

Any tenant with Intune licensing can access this setting.

7.1.3

Set-Up Instructions

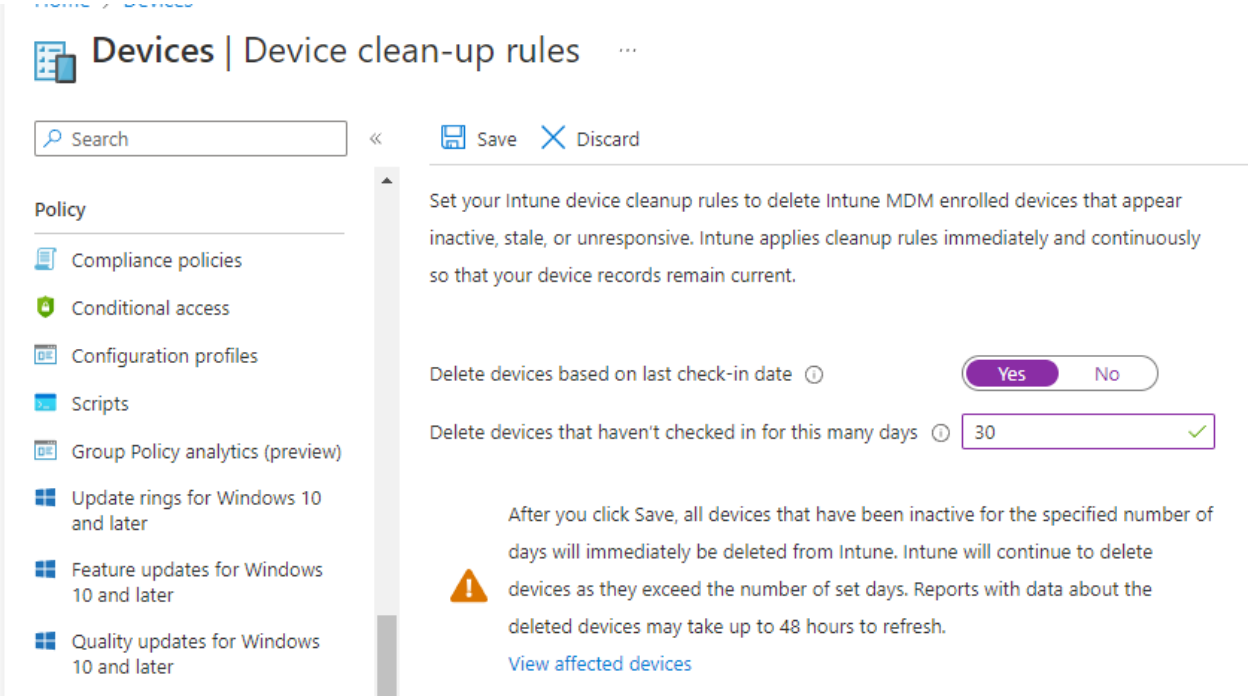
Overview of enrollment restrictions - Microsoft Intune | Microsoft Learn

Create device platform restrictions - Microsoft Intune | Microsoft Learn

To set the device clean-up rule:

1. Go to the **Intune Admin Center**
2. Click on **Devices**

3. Scroll down to **Other** and select **Device Clean-up rules**
4. Select **Yes** for the first option
5. Set the time period to **30 days**
6. Click **Save**



7.2.4

End-User Impact

Level: Low

If users have a device that does no check in for over 30 days it would be removed from Intune. Devices can be recovered if someone were to take an extended leave for up to 180 days.

7.2.5

Tips

- If you are leveraging Intune as a source of truth for your asset inventory, you may want to change this setting to 60 or 90 days so that devices are not removed as quickly. This would give you more time to identify stale devices and take the proper action to reissue or retire the device.

7.2.6

PowerShell Scripts

Microsoft Intune: Device Cleanup rules | Neeraj Kumar

7.2.7

Videos

14. How to Setup Automatic Device Cleanup Rule in Intune - YouTube

7.3 Devices compliance policies shall be configured for every supported device platform

Device compliance policies allow us to define the necessary settings on a particular platform that meets corporate requirements. Device compliance policies paired with conditional access policies allow us to prevent access to corporate resources on noncompliant devices. Devices should be constantly monitored to ensure compliance with corporate policies.

7.3.1

Policy

- A device compliance policy is configured for each device platform that is supported by the corporation.
- Devices that do not meet the compliance standards shall be marked as noncompliant immediately

7.3.2

Licensing Considerations

Any tenant with Intune licensing can access this setting.

7.3.3

Set-Up Instructions

Device compliance policies in Microsoft Intune | Microsoft Learn

To configure device compliance policies by platform:

Windows

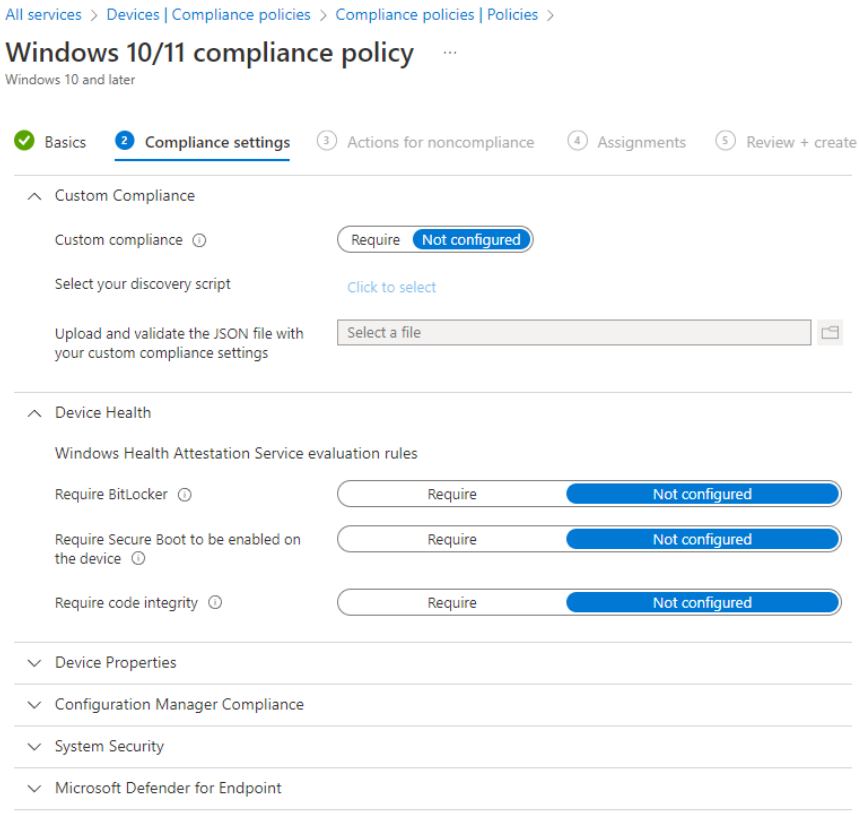
macOS

iOS/iPadOS

Android device administrator

Android (AOSP)

Android Enterprise



7.3.4

End-User Impact

Level: Medium

Device compliance policies will have no impact to end-users unless they are paired with conditional access policies to block access on noncompliant devices. Devices not in compliance will show up in the Intune admin center from a reporting standpoint. There are certain device compliance policy settings that will prompt the end-user for certain action. For instance, configuring Encryption of data storage on the device will prompt the user to configure Bitlocker encryption if it is not already enabled. It is recommended to push out a configuration profile to automatically configure encryption in this use case to avoid help desk calls.

7.3.5

Tips

- Device compliance policy settings might vary depending on the organization but should be standardized where possible.

7.3.6

PowerShell Scripts

powershell-intune-samples/CompliancePolicy at master · microsoftgraph/powershell-intune-samples (github.com)

7.3.7

Videos

- iOS Device Compliance Policy Intune - YouTube
- Windows 10 Compliance Policy Intune - YouTube
- S04E08 - Custom Compliance policies (I.T) - YouTube

7.4 Noncompliant devices shall be blocked from accessing corporate resources.

Device compliance policies allow us to define the necessary settings on a particular platform that meets corporate requirements. Device compliance policies paired with conditional access policies allow us to prevent access to corporate resources on noncompliant devices. Devices that are not in compliance should not have access to corporate resources.

7.4.1

Policy

- Noncompliant devices shall not be able to access corporate resources

7.4.2

Licensing Considerations

This setting requires at least an Azure AD P1 license which comes standalone or as part of the following bundles:

- EMS+E3/E5
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

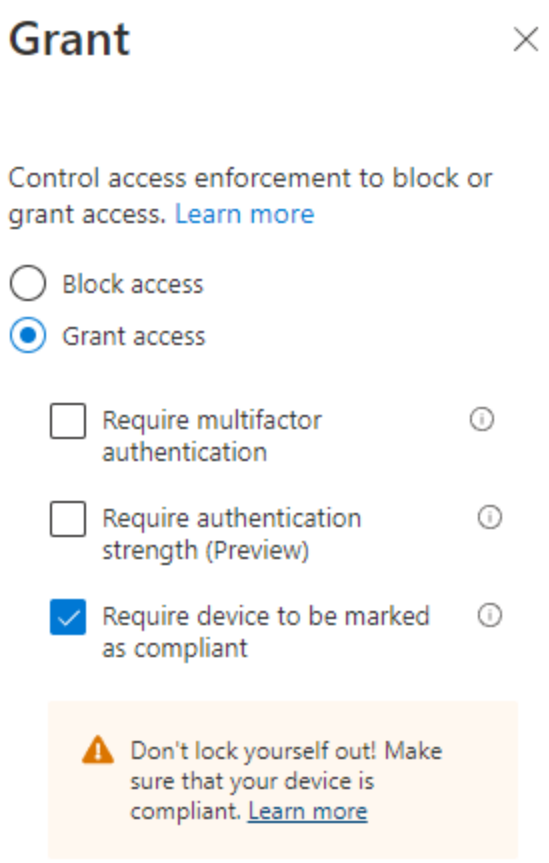
7.4.3

Set-Up Instructions

Device compliance policies in Microsoft Intune | Microsoft Learn

To configure a conditional access policy for compliant devices:

1. Follow the steps outlined here to create a conditional access policy
2. Under the assignments section, **Include all users**. Be sure to **Exclude** a break-glass account to ensure you never lock yourself out.
3. Under the Cloud Apps section, **include all cloud apps**
4. Do not configure anything in the conditions section
5. Under the Grant section, choose **Require device to be marked as compliant**

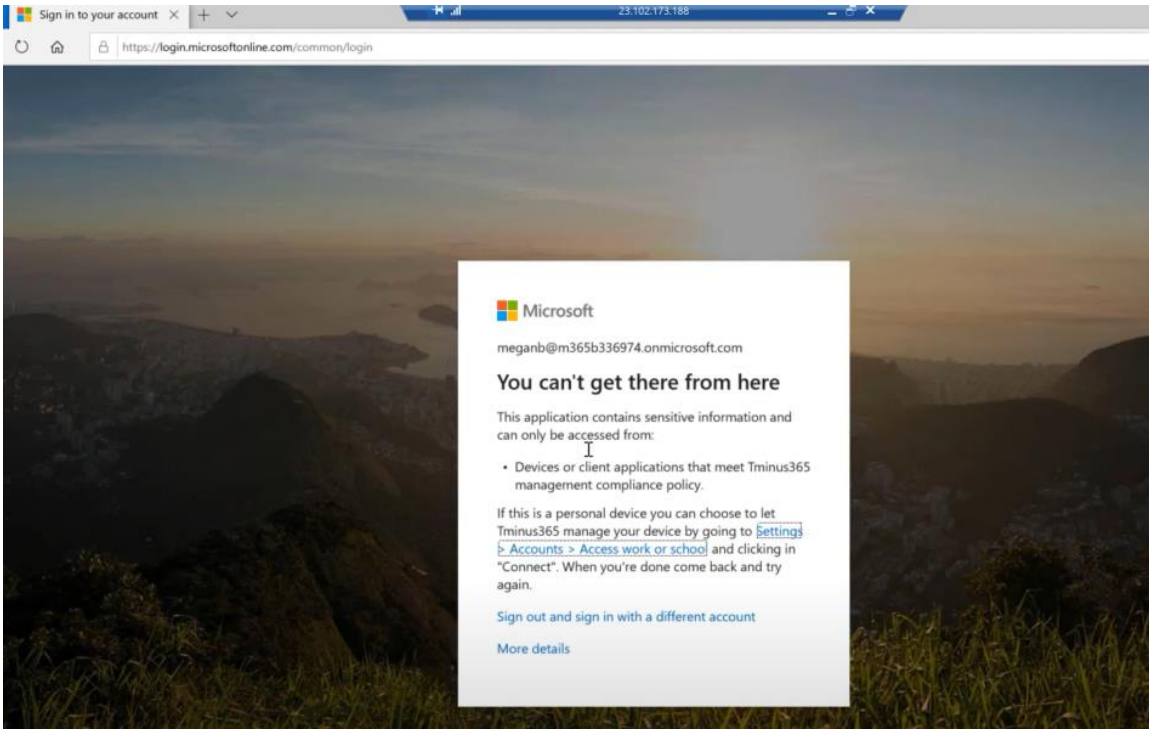


7.4.4

End-User Impact

Level: High

Any user that is trying to access corporate data on a device not marked as compliant shall receive a message letting them know they are blocked and will be told to contact IT. This includes both devices enrolled into Intune and marked as noncompliant as well as devices that are not enrolled at all into the solution.



7.4.5

Tips

- A formal process definition should be in place for investigating noncompliant devices. Common use cases for noncompliant triggers should be documented to expedite resolution
- Automation should be put in place where possible to alert on noncompliant devices in order to be more proactive.
- Users should have way to readily contact support that is not through email as they will not have access to enter outlook

7.4.6

PowerShell Scripts

azure-ad-conditional-access-apis/readme.md at main · Azure-Samples/azure-ad-conditional-access-apis (github.com)

7.4.7

Videos

Preventing Access on Noncompliant Devices - YouTube

7.5 MFA Shall be required for Intune Enrollment

You can use Intune together with Azure Active Directory (Azure AD) conditional access policies to require multifactor authentication (MFA) during device enrollment. If you require MFA, employees and students wanting to enroll devices must first authenticate with a second device and two forms of credentials. We do not want unauthorized users joining devices to our network.

7.5.1

Policy

- MFA Shall be required to enroll devices into Intune

7.5.2

Licensing Considerations

This setting requires at least an Azure AD P1 license which comes standalone or as part of the following bundles:

- EMS+E3/E5
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

7.5.3

Set-Up Instructions

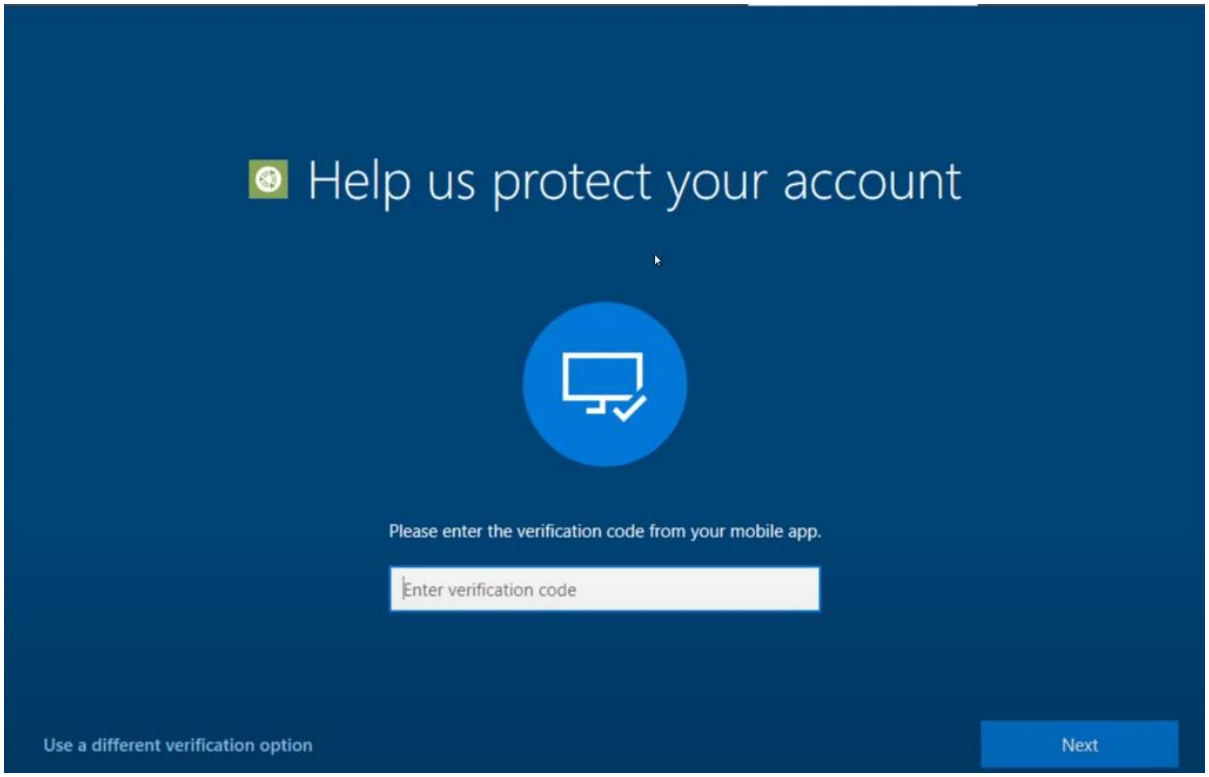
Require multifactor authentication for Intune device enrollment - Microsoft Intune | Microsoft Learn

7.5.4

End-User Impact

Level: Medium

Users must satisfy the MFA prompt in order to be able to successfully enroll a device. For users signing in for the very first time who have not configured MFA methods, a temporary access pass can be used: Configure a Temporary Access Pass in Azure AD to register Passwordless authentication methods - Microsoft Entra | Microsoft Learn



7.5.5

Tips

- For users signing in for the very first time who have not configured MFA methods, a temporary access pass can be used: Configure a Temporary Access Pass in Azure AD to register Passwordless authentication methods - Microsoft Entra | Microsoft Learn

7.5.6

PowerShell Scripts

azure-ad-conditional-access-apis/readme.md at main · Azure-Samples/azure-ad-conditional-access-apis (github.com)

7.5.7

Videos

Enabling MFA when Joining a Device to Azure AD - YouTube

7.6 Security Baselines should be configured for Windows Devices

Security baselines in Intune are pre-configured groups of settings that are best practice recommendations from the relevant Microsoft security teams for the product. Intune supports security baselines for Windows 10/11 device settings, Microsoft Edge, Microsoft Defender for Endpoint Protection, and more.

You can use security baselines to rapidly deploy a *best practice* configuration of device and application settings to protect your users and devices. Security baselines are supported for devices that run Windows 10 version 1809 and later, and Windows 11. These baselines allow you to configure common security settings such as:

- Password Requirements
- Lock screen settings
- App Installation

7.6.1

Policy

- Security Baselines should be configured for Windows Devices

7.6.2

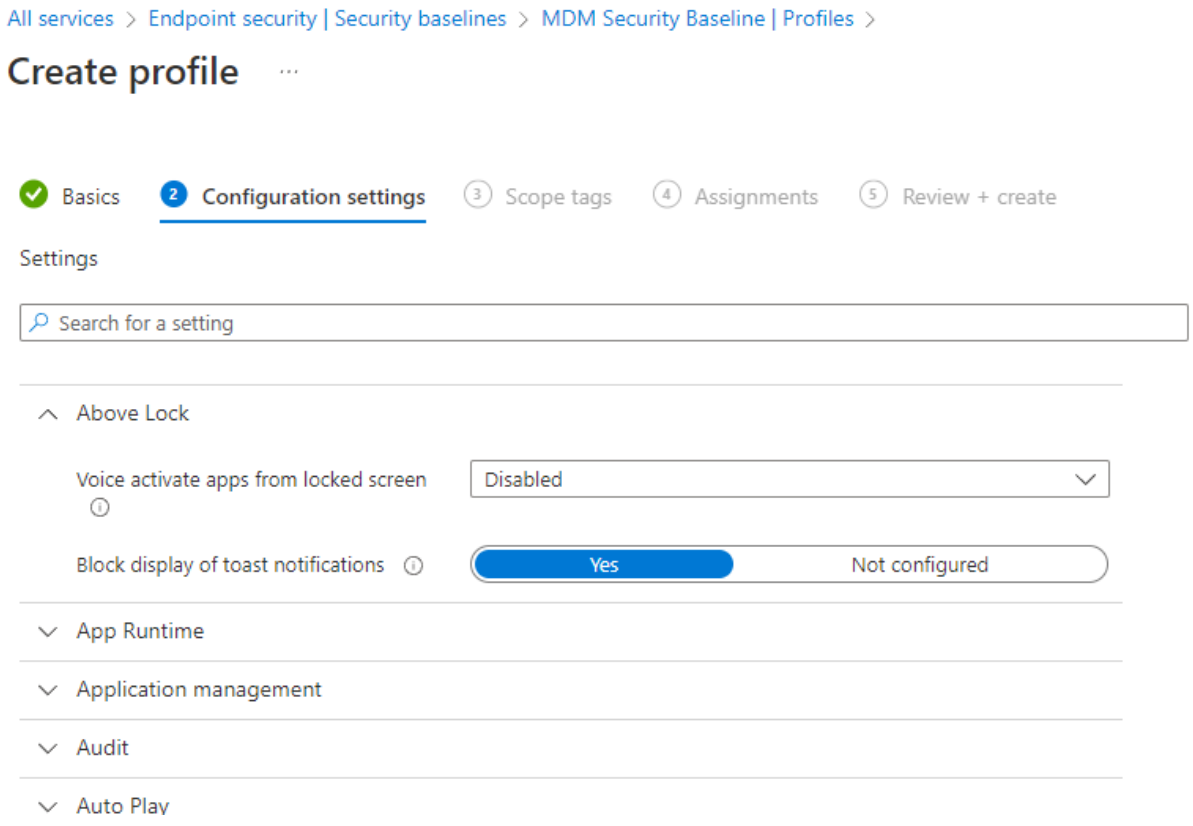
Licensing Considerations

Any tenant with Intune licensing can access this setting.

7.6.3

Set-Up Instructions

Require multifactor authentication for Intune device enrollment - Microsoft Intune | Microsoft Learn



7.6.4

End-User Impact

Level: Medium

Its possible that some of the settings pre-configured as part of the security baseline profile will be disruptive to end-users. As a best practice, proper testing should be done leveraging a device on the corporate network and testing this out with a pilot group of users before broad deployment.

7.6.5

Tips

- Security baselines are one of several methods in Intune to configure settings on devices. When managing settings, it's important to understand what other methods are in use in your environment that can configure your devices so you can avoid conflicts. See Avoid policy conflicts later in this article.

7.6.6

PowerShell Scripts

powershell-intune-samples/EndpointSecurity at master · microsoftgraph/powershell-intune-samples (github.com)

Creating Endpoint Security Policies with PowerShell | Powers Hell (powers-hell.com)

7.6.7

Videos

Microsoft Endpoint Manager: Security baselines - YouTube

Microsoft Endpoint Manager Intune Endpoint Protection Part IV Security Baselines - YouTube

7.7 Windows Update Rings shall be configured for Windows Devices

Windows update rings, also known as Windows Update for Business allow you to manage the patch cycle across Windows devices in your organization.

Updates should be staggered across devices in your organization in order to manage any new features or bugs as part of the new update. Critical updates should be deployed immediately to all devices leveraging the Windows update ring service.

If you are an enterprise customer, Windows Autopatch is another feature that can automate your deployment of Windows update rings.

7.7.1

Policy

- Windows update rings are configured and assigned to all windows devices

7.7.2

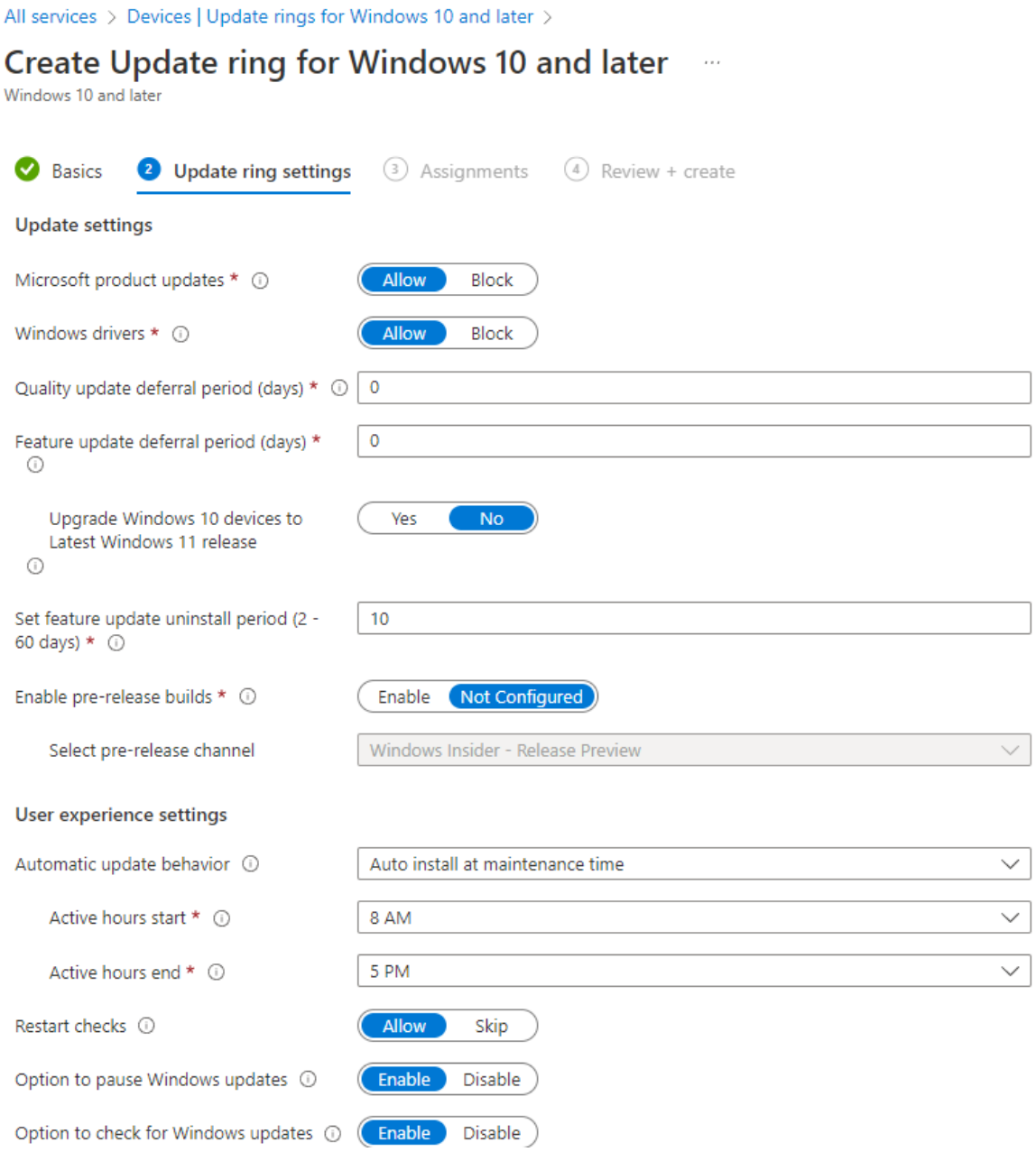
Licensing Considerations

- Any tenant with Intune licensing can access this setting.
- OS Requirements: Configure Update rings for Windows 10 and later policy in Intune | Microsoft Learn
- Windows Autopatch Prerequisites: Prerequisites - Windows Deployment | Microsoft Learn

7.7.3

Set-Up Instructions

Configure Update rings for Windows 10 and later policy in Intune | Microsoft Learn



7.7.4

End-User Impact

Level: Medium-High

Patching has always been notorious for being disruptive to end-users. When you configure the Windows update rings, you can define specific time periods where updates will try to be deployed. This is typically in the after hours of business. You

can also decide how long end-users can defer updates before they are forced to install them. There will always be use cases where you also have to uninstall updates due to those updates having bugs or disrupting some type of line of business application.

7.7.5

Tips

- Have a defined process in place for when you need to roll back updates or when you need to push out critical updates to all devices.
- In your broad deployment, make sure the quality or deferred updates are pushed out at least 14 days to avoid more frequent rollbacks.

7.7.6

PowerShell Scripts

powershell-intune-samples/SoftwareUpdates at master · microsoftgraph/powershell-intune-samples (github.com)

7.7.9

Videos

- Windows Update Rings: https://www.youtube.com/watch?v=RKfDZeQL97w&t
- Automate Windows Patching | Microsoft Tutorial - YouTube

7.8 Update Policies shall be configured for Apple Devices

You can use Microsoft Intune to manage software updates for macOS, iOS, and iPad devices that enrolled as supervised devices. Just like the Windows update rings in the previous section, we can leverage these policies to manage the patch cycle on Apple devices enrolled into Intune.

7.8.1

Policy

- Update policies are configured for macOS, iOS, and iPad Devices

7.8.2

Licensing Considerations

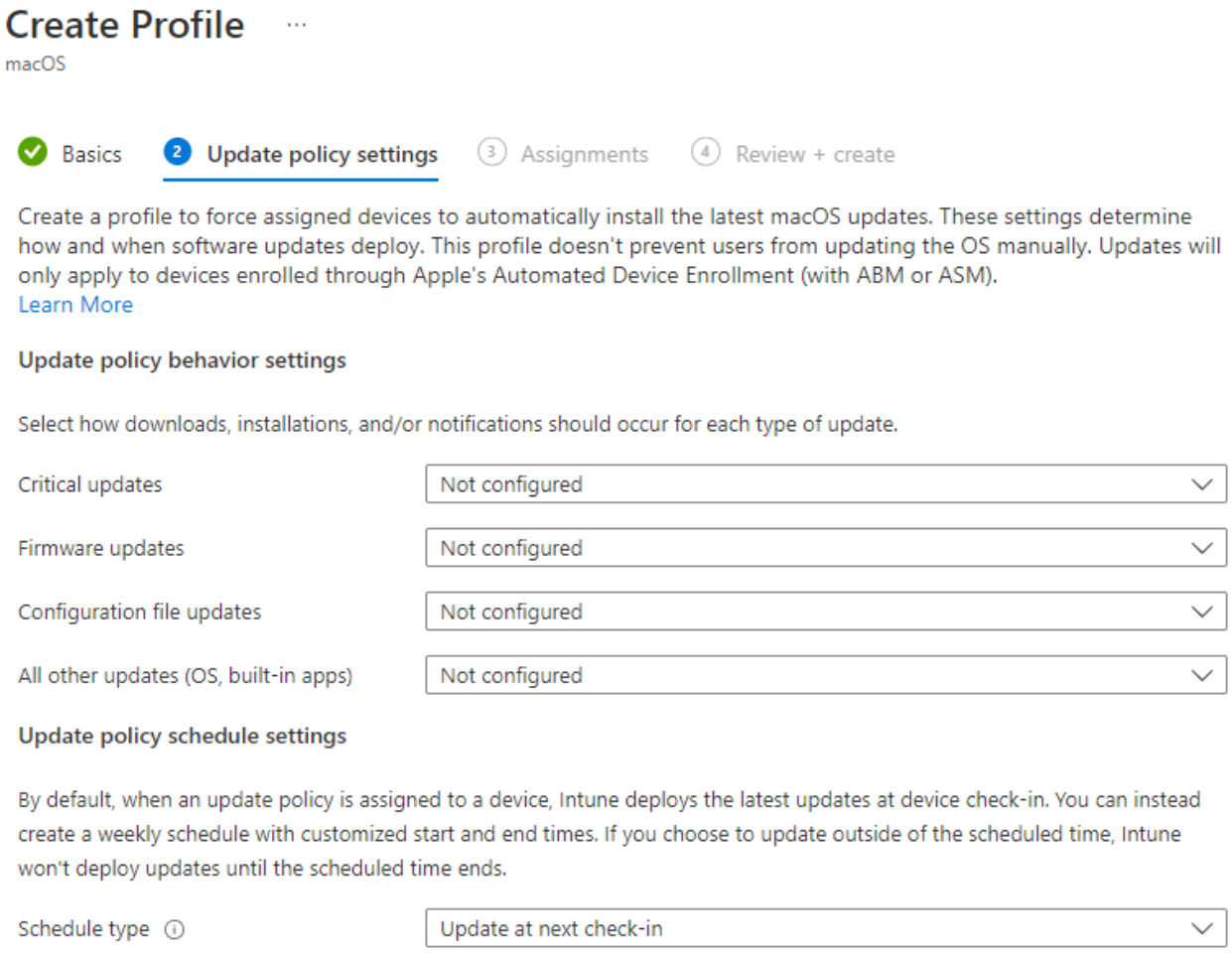
- Any tenant with Intune licensing can access this setting.

7.8.3

Set-Up Instructions

Use Microsoft Intune policies to manage macOS software updates | Microsoft Learn

Use Microsoft Intune policies to manage iOS/iPadOS software updates | Microsoft Learn

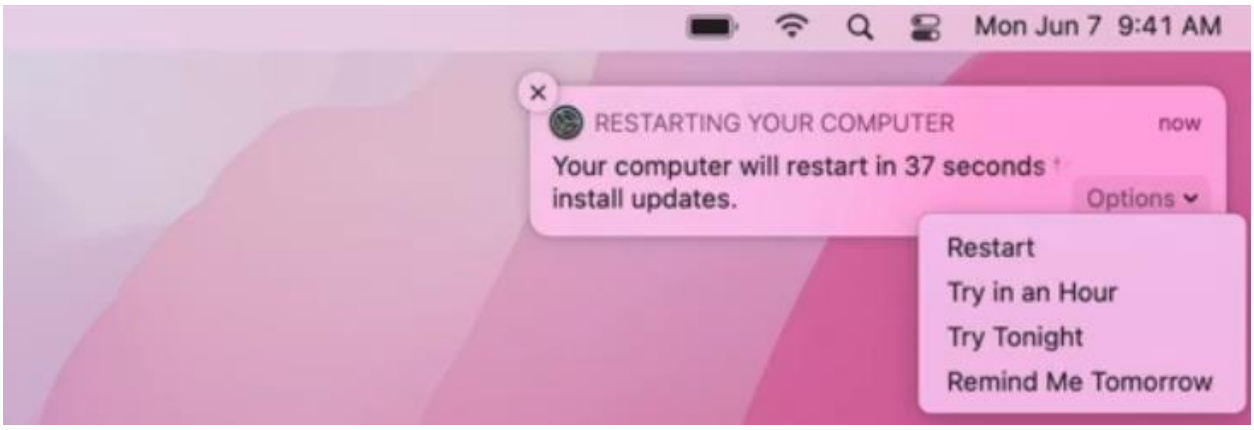


7.8.4

End-User Impact

Level: Medium-High

Patching has always been notorious for being disruptive to end-users. When you configure the update policies, you can define specific time periods where updates will try to be deployed. This is typically in the after hours of business. When you use update policies for macOS, you might want to hide updates from users of supervised macOS devices for a period of time. You can accomplish this with a settings catalog policy for macOS devices that configure update restriction periods. You can follow these instructions to configure these settings: Use Microsoft Intune policies to manage macOS software updates | Microsoft Learn



7.8.5

Tips

- The Install immediately setting is the most user-impactful setting as it will reboot the computer immediately.

7.8.6

PowerShell Scripts

powershell-intune-samples/SoftwareUpdates at master · microsoftgraph/powershell-intune-samples (github.com)

7.8.7

Videos

Patching macOS Devices with Microsoft Intune | Microsoft Tutorial - YouTube

7.9 App Protection policies should be created for mobile devices

Leveraging the mobile application management (MAM) features of Microsoft Intune, app protection policies can be created so that users can access corporate applications on mobile devices securely, without having to enroll that device into the MDM solution. These settings allow you to place additional protection on applications such as requiring a pin or preventing cut, copy, and paste to

unmanaged applications. App protection policies should be configured for iOS and Android devices.

7.9.1

Policy

- App protection policies are configured for iOS and Android devices

7.9.2

Licensing Considerations

- Any tenant with Intune licensing can access this setting.

7.9.3

Set-Up Instructions

Create and deploy app protection policies - Microsoft Intune | Microsoft Learn

Android app protection policy settings - Microsoft Intune | Microsoft Learn

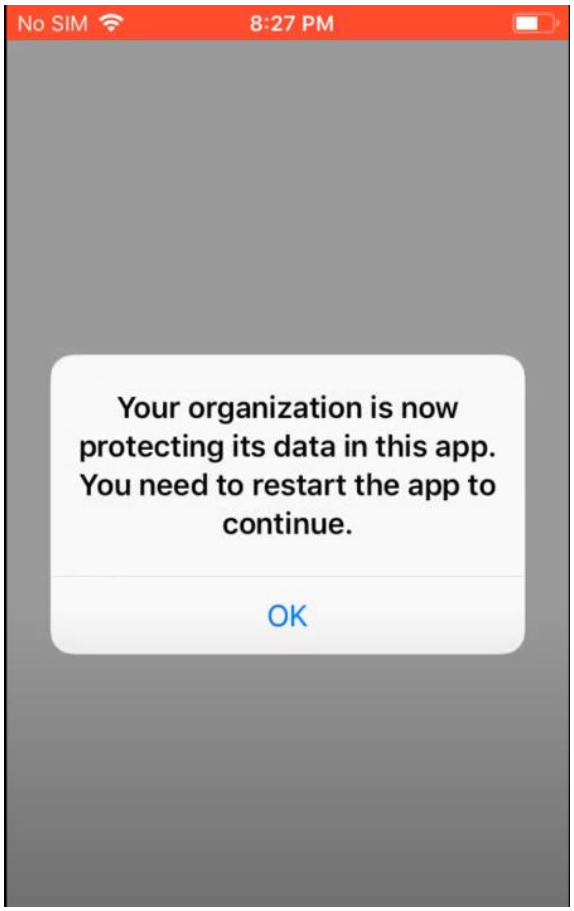
iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn

7.9.4

End-User Impact

Level: Medium

When users go to access corporate data on a managed application like Outlook, they will receive a prompt that the devices is under corporate management. Depending on what settings are configured in the policy they might also have to a take additional action such as setting up an application pin.



7.9.5

Tips

- Do not configure this setting for all apps on the device. The recommended setting is to configure all Microsoft Apps.

7.9.6

PowerShell Scripts

powershell-intune-samples/AppProtectionPolicy at master · microsoftgraph/powershell-intune-samples (github.com)

7.9.7

Videos

Protecting Corporate Data on iOS and Android Devices - YouTube

Android App Protection Policies - YouTube

iOS App Protection Policies - YouTube

7.10 Mobile devices shall only be able to access corporate data through approved client apps

Conditional Access policies can be set up to only allow access to corporate data on client approved apps. This setting would prevent a user from leveraging the native mail client on their mobile application. A client that you are not able to control or wipe if they leave the organization.

7.10.1

Policy

- Mobile devices shall only be able to access corporate data through approved client apps

7.10.2

Licensing Considerations

This setting requires at least an Azure AD P1 license which comes standalone or as part of the following bundles:

- EMS+E3/E5
- Microsoft 365 Business Premium
- Microsoft 365 E3
- Microsoft 365 E5

7.10.3

Set-Up Instructions

1. Follow the steps outlined here to create a conditional access policy that requires approved client apps for mobile devices.
2. In the Access Controls, only select the Required Approved Client App settings

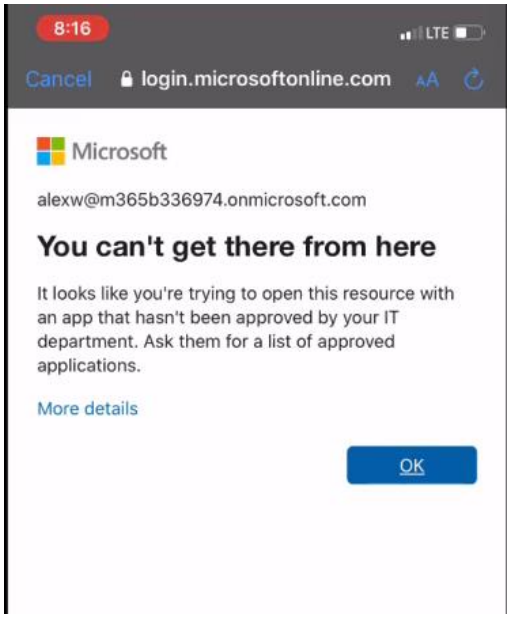
Note You may chose to app the require app protection policy setting here as well but it will required that these devices enroll in the MDM solution. More information here: Grant controls in Conditional Access policy - Azure Active Directory - Microsoft Entra | Microsoft Learn

7.10.4

End-User Impact

Level: Medium

If a user goes to access corporate data on an unapproved client app, like the native mail app on the mobile device, they will be redirected to the Apple Store or Google Play store to download the approved client app (in this case, Outlook).



7.10.5

Tips

- App Protection policies can be scoped to managed or unmanaged devices. If you have them scoped to managed devices, its likely you will want to include the “Require App Protection Policy” setting in the grant controls of the conditional access policy

7.10.6

PowerShell Scripts

- None Currently

7.10.7

Videos

S02E27 - Configure Conditional Access & App Protection Policies for iOS in Microsoft Intune - (I.T) - YouTube

7.11 Lockout screen and password settings shall be configured for each device

Lockout screen timeouts should be configured for a certain number of minutes of activity for all device platforms. Password complexity requirements should be enforced and users should be prompted to change their password if it does not meet corporate requirements. In Intune, the location to configure these settings varies depending on the platform.

Windows: Security Baselines (Device Lock, Local Policies Security Options), Configuration Profiles (Device Restrictions: Password)

macOS: Compliance Policy (System Security)

iOS: Compliance Policy (System Security)

Android: Compliance Policy (System Security)

7.11.1

Policy

- All supported devices have configuration settings defined/enforced for lockout screen timeouts and passwords

7.11.2

Licensing Considerations

- Any tenant with Intune licensing can access this setting.

7.11.3

Set-Up Instructions

Windows Security Baselines: Create security baseline profiles in Microsoft Intune | Microsoft Learn

1. Under Device Lock set the password requirements
2. Under Local Policies Security Options, Set the Minutes of lock screen inactivity until screen save activates policy

macOS Compliancy Policy: macOS device compliance settings in Microsoft Intune | Microsoft Learn

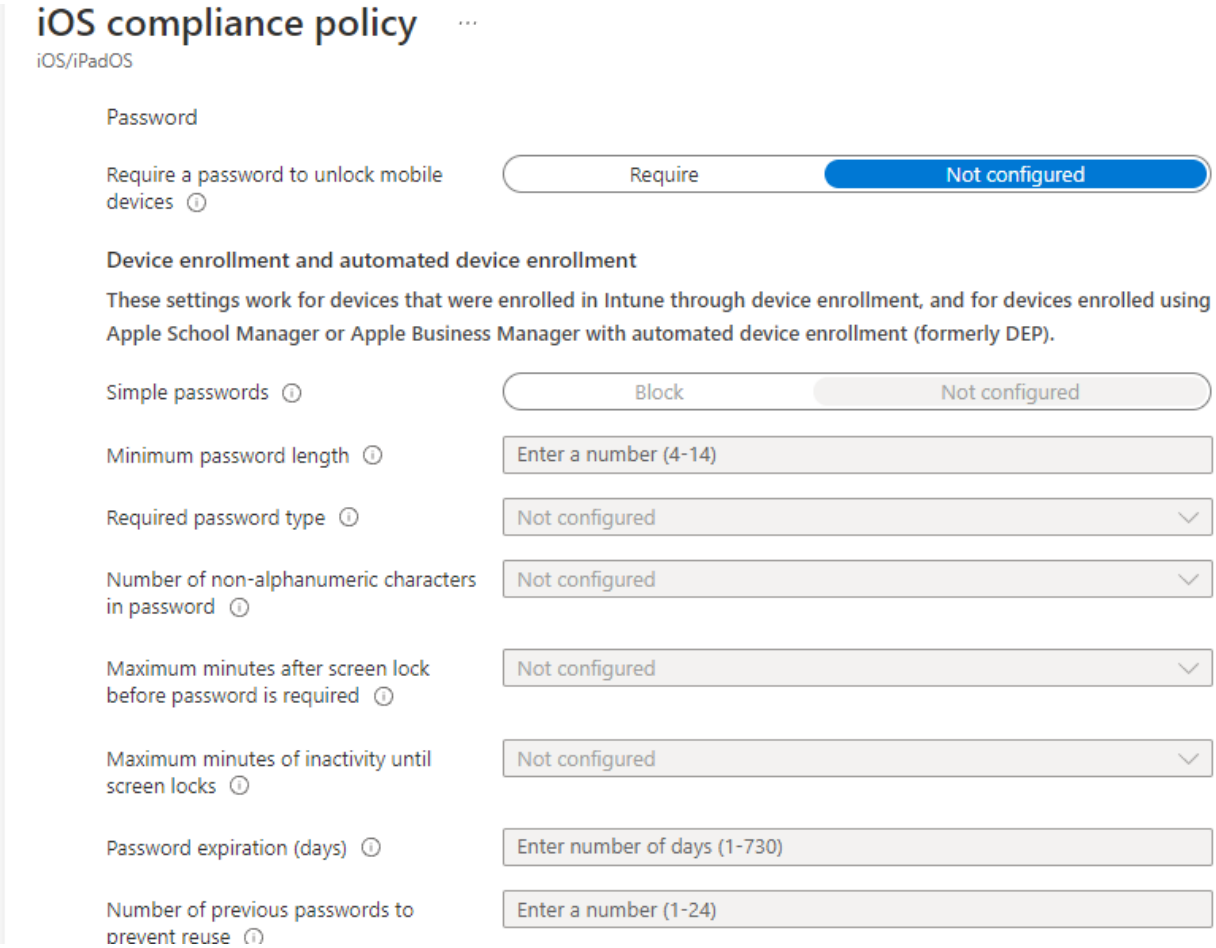
1. Under System Security, modify the Password requirements and minutes of inactivity before password required

iOS Compliancy Policy: iOS/iPadOS device compliance settings in Microsoft Intune | Microsoft Learn

1. Under System Security, modify the Password requirements and minutes of inactivity before password required

Android Compliancy Policy: Android Enterprise compliance settings in Microsoft Intune | Microsoft Learn

1. Under System Security, modify the Password requirements and minutes of inactivity before password required



7.11.4

End-User Impact

Level: Medium

End users who enroll devices into Intune after this policy is enforced may be prompted to update their password if the policy requirements are not met on the device.

7.11.5

Tips

- Make sure you don't have conflicting policies between configuration profiles, security baselines, and compliance policies

7.11.6

PowerShell Scripts

powershell-intune-samples/CompliancePolicy at master · microsoftgraph/powershell-intune-samples (github.com)

powershell-intune-samples/DeviceConfiguration at master · microsoftgraph/powershell-intune-samples (github.com)

7.11.7

Videos

macOS Configuration Profiles Intune - YouTube

iOS Device Restrictions-Microsoft Intune - YouTube

7.12 Encryption shall be required on all devices

Disk encryption shall be configured on all corporate owned devices. Encryption of corporate data should also be configured at an application layer where applicable. In the Endpoint Manager Admin center, there is multiple locations to configure device encryption:

Endpoint Security>Disk Encryption: Allows you to configure encryption settings for FileVault (macOS) and Bitlocker (Windows).

Configuration Profiles: Endpoint Protection (Windows Encryption, FileVault), Device Restrictions (iOS, Android)

App Protection Policies (For application data encryption): iOS and Android

7.12.1

Policy

- Disk encryption shall be required on all devices

7.12.2

Licensing Considerations

- Any tenant with Intune licensing can access this setting.

7.12.3

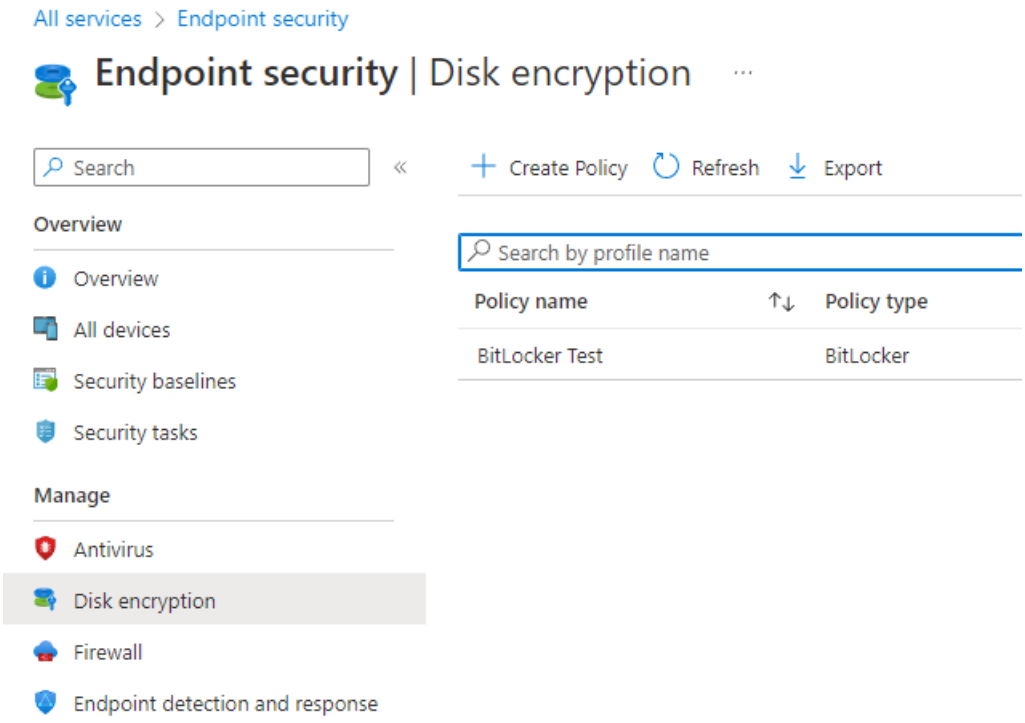
Set-Up Instructions

Disk Encryption: Manage disk encryption with endpoint security policies in Microsoft Intune | Microsoft Learn

Configuration Profiles: Configure Endpoint protection settings in Microsoft Intune | Microsoft Learn

App Protection Policies:

- iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn
- Android app protection policy settings - Microsoft Intune | Microsoft Learn



7.12.4

End-User Impact

Level: Low

If configured correctly, the end user should have no interaction with configuring encryption on the device. Leveraging configuration profiles or disk encryption settings should automatically configure the device encryption. There could be a use case where the configuration fails and the end user is prompted to fix on their device.

7.12.5

Tips

- Make sure you don't have conflicting policies between configuration profiles, security baselines, compliance policies, and disk encryption profiles
- As a best practice, its best to push out the configuration profiles for disk encryption before enforcing any compliance policies that require device

encryption. This will ensure that the encryption is silently configured an the user does not get prompted to set that up on their own.

7.12.6

PowerShell Scripts

- Configure disk encryption

7.12.7

Videos

Troubleshooting Bitlocker Encryption with Intune - YouTube

Enforce FileVault on macOS with Microsoft Intune - YouTube

S01E04 - Configuring and Deploying BitLocker Client Policies from Intune - (I.T) - YouTube

Configure BitLocker Policy in Intune - Create your own Intune lab (12/15) - YouTube

7.13 Windows Hello for Business should be configured where applicable

For Windows 10/11 devices, use of Windows Hello for Business replaces the use of passwords with strong two-factor authentication on devices. This authentication consists of a user credential that's tied to a device and uses a biometric or PIN.

7.13.1

Policy

Windows Hello for Business should be configured where applicable

7.13.2

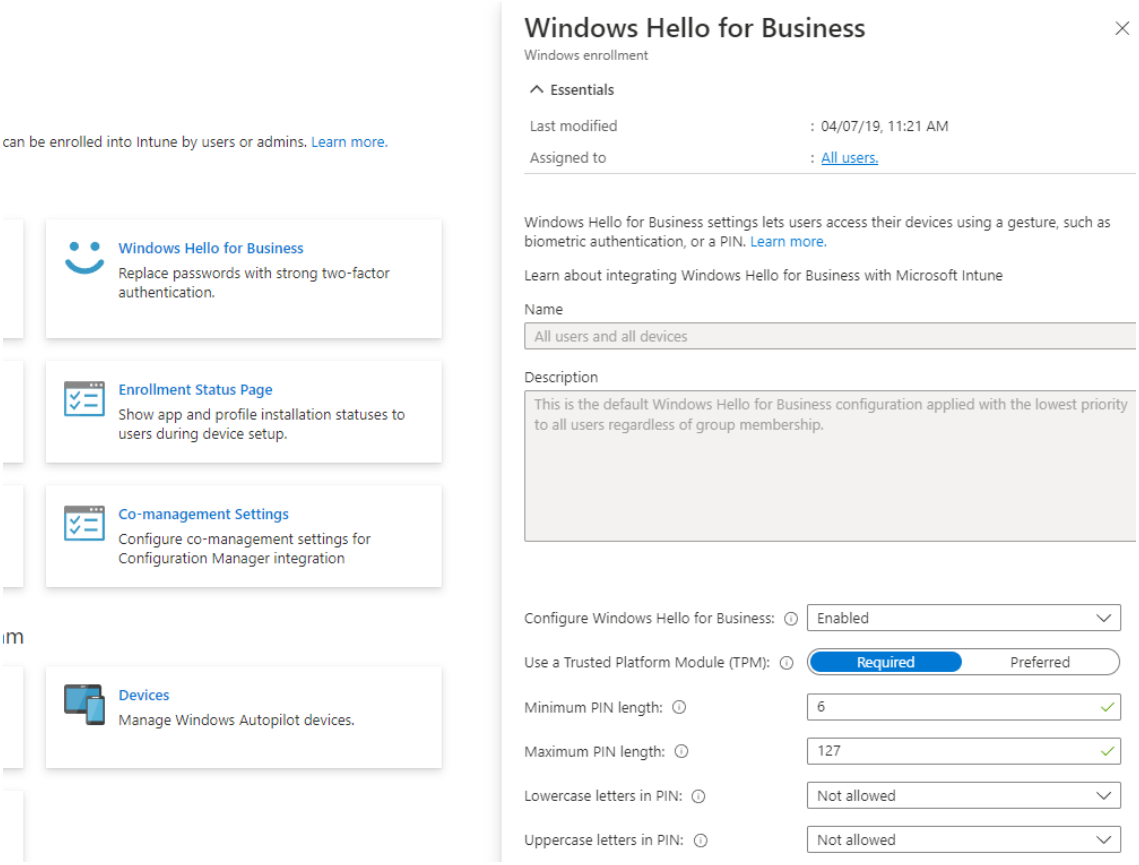
Licensing Considerations

- Any tenant with Intune licensing can access this setting.

7.13.3

Set-Up Instructions

- Configure Windows Hello at the time of enrollment: Configure a tenant-wide Windows Hello for Business policy with Microsoft Intune - Microsoft Intune | Microsoft Learn
- Configure Windows Hello after device enrollment: Deploy policy for Windows Hello to groups of Windows 10 and Windows 11 devices in Microsoft Intune | Microsoft Learn



7.13.4

End-User Impact

Level: Low

Users will be prompted to set up facial recognition or fingerprint depending on the device. Users will also be asked to establish a pin in case that biometric authentication fails or cannot be accessed.

7.13.5

Tips

- N/A

7.13.6

PowerShell Scripts

powershell-intune-samples/DeviceConfiguration at master · microsoftgraph/powershell-intune-samples (github.com)

7.13.7

Videos

Deploy Windows Hello for Business using Configuration Profiles - YouTube

• Configure Windows Hello For Business intune - YouTube

7.14 Authorized Applications should be deployed to managed devices

An authorized application inventory should be kept for corporate approved applications. These applications should be packaged and deployed in Microsoft Intune from the applications section of the Intune Admin Center. The application lifecycle should be maintained through Intune, including the patch cycle.

7.14.1

Policy

Authorized Applications should be deployed to managed devices

7.14.2

Licensing Considerations

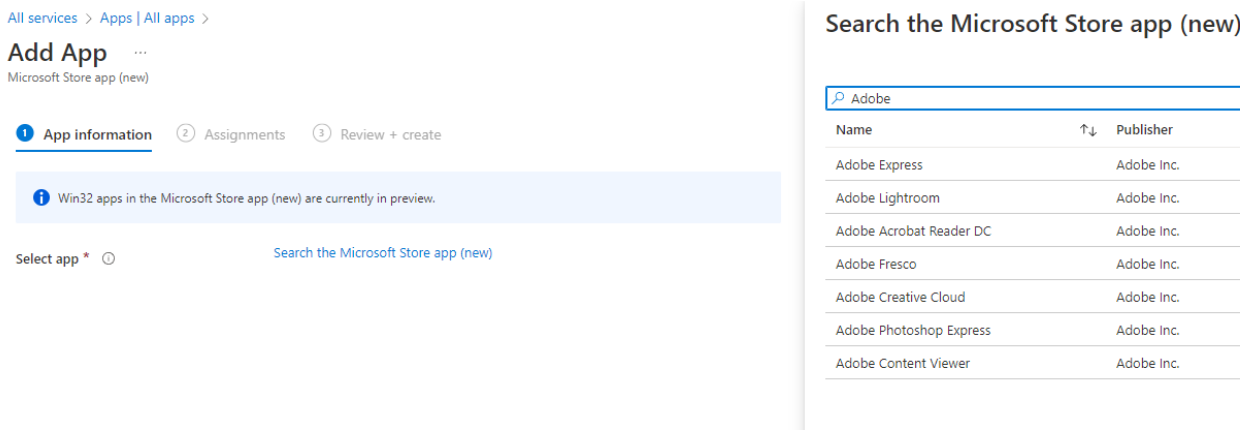
- Any tenant with Intune licensing can access this setting.

7.14.3

Set-Up Instructions

https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-prepare

Add Microsoft Store apps to Microsoft Intune | Microsoft Learn



7.14.4

End-User Impact

Level: Low

This will vary depending on the applications you are pushing out. The installation package you define will determine if the application will install automatically or provide the option to the user to install the application.

7.14.5

Tips

- Leverage packaging tools like Winget and Chocolatey to help automate the app packaging and deployment.

7.14.6

PowerShell Scripts

- https://github.com/Romanitho/Winget-Install
- https://github.com/Romanitho/Winget-AutoUpdate
- https://github.com/o-l-a-v/winget-intune-win32
- powershell-intune-samples/Applications at master · microsoftgraph/powershell-intune-samples (github.com)

7.14.7

Videos

Automate App Packaging: How to automate app packaging for Windows Devices - YouTube

Deploying Apps in Intune: https://www.youtube.com/watch?v=FGZ7hrVBSE4

Winget + Intune: https://www.youtube.com/watch?v=y2PbdOueUNQ

7.15 Device Use Shall be restricted until required applications are installed

When a user is first onboarding to a new device, required applications, such as your AV or Endpoint protection software, should be allowed to install before the user begins to access the device. This setting can be configured as part of the enrollment status page for people enrolling Windows devices and signing in for the first time.

7.15.1

Policy

Device Use Shall be restricted until required applications are installed

7.15.2

Licensing Considerations

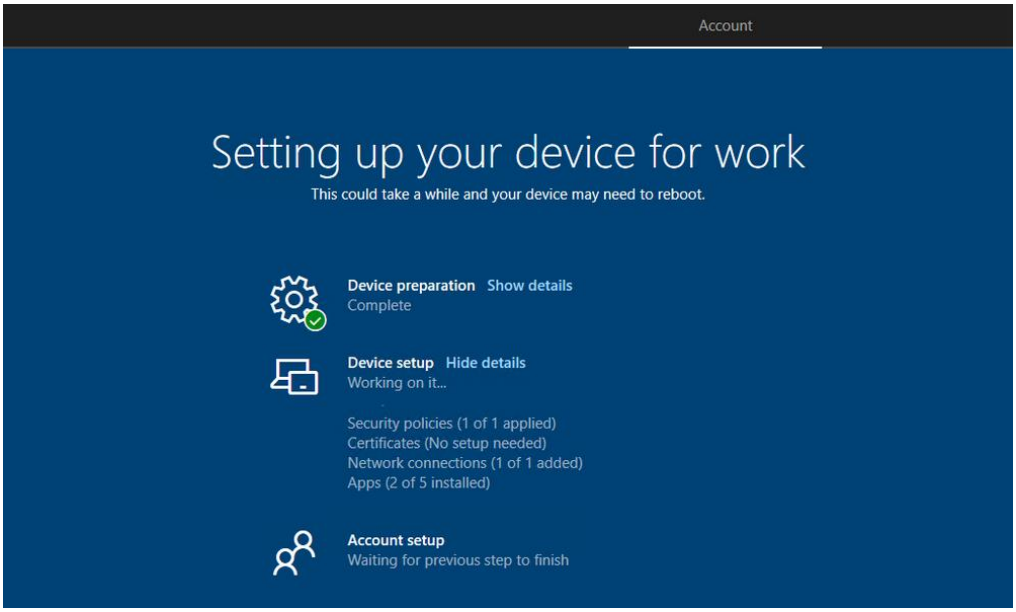
- Any tenant with Intune licensing can access this setting.

7.15.3

Set-Up Instructions

Set up the Enrollment Status Page in the admin center - Microsoft Intune | Microsoft Learn

Selecting Required Apps for your Enrollment Status Page - Microsoft Community Hub



7.15.4

End-User Impact

Level: Medium

This will vary depending on the applications being installed. Its possible the user will have to wait some time for the applications to finish installing. For this reason, its best to define the minimum blocking applications as part of the settings and not make this the full list that will be installed.

7.15.5

Tips

- N/A

7.15.6

PowerShell Scripts

None Currently

7.15.7

Videos

S03E02 - Enrollment Status Page What it is and What it isn't - (I.T) - YouTube

Decode the Windows Enrollment Status Page | Microsoft Intune - YouTube

Set up the Enrollment Status Page - YouTube

7.16 Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device

Standard operating procedures should be put into place to remotely wipe devices and applications when a user leaves the organization or a device is lost or stolen.

7.16.1

Policy

Devices and Applications shall be wiped when a user leaves the organization or reports a lost/stolen device

7.16.2

Licensing Considerations

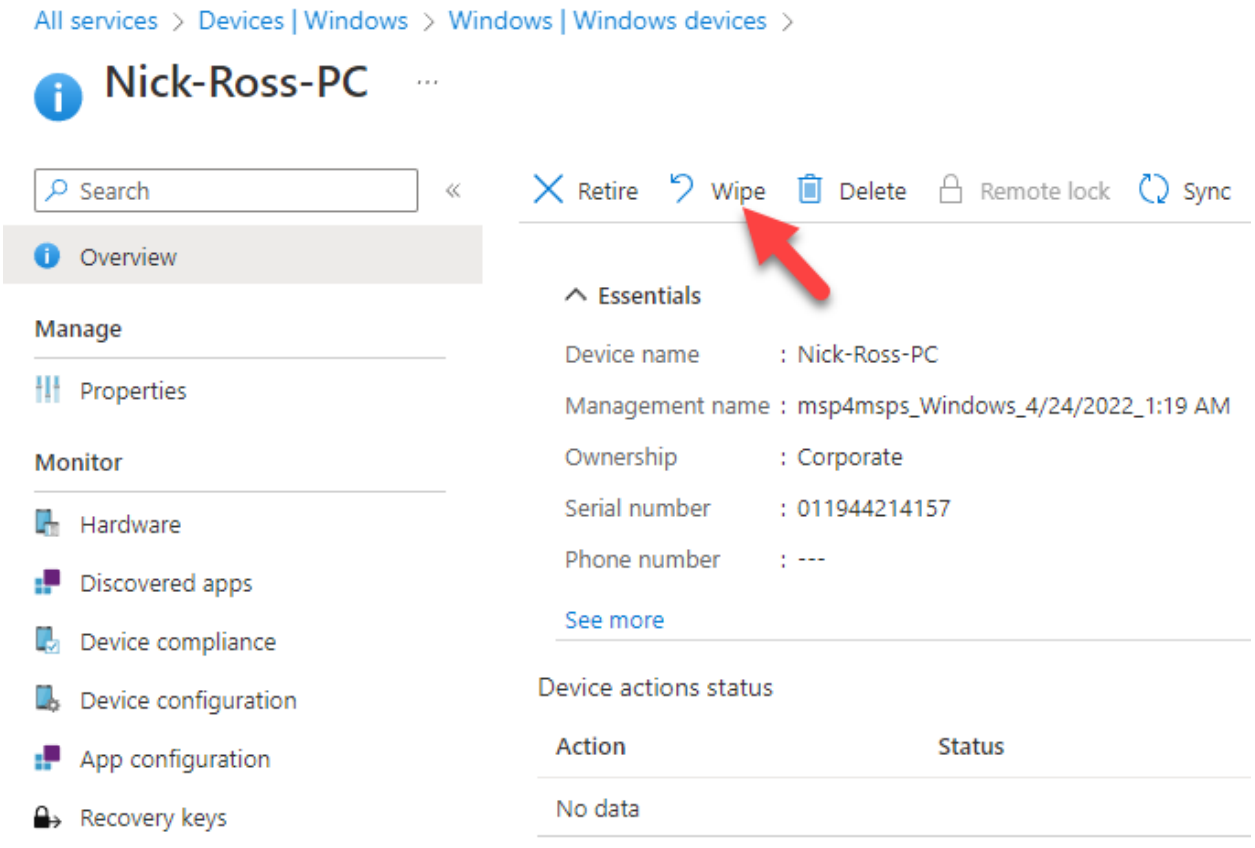
- Any tenant with Intune licensing can access this setting.

7.16.3

Set-Up Instructions

Retire or wipe devices using Microsoft Intune | Microsoft Learn

How to wipe only corporate data from apps - Microsoft Intune | Microsoft Learn



7.16.4

End-User Impact

Level: None

There should be no user impact here unless the actions to remotely wipe a device or application is done in error where the user should not have had that action performed against their device.

7.16.5

Tips

- N/A

7.16.6

PowerShell Scripts

None Currently

7.16.7

Videos

28. How to Wipe and Remove a Windows 10 Device in Intune - YouTube

Remotely Erase MacOS using Microsoft Endpoint Manager (Intune) - YouTube

Windows Autopilot Reset - YouTube

MS28 - How to Perform Selective Wipe from Microsoft Intune - YouTube

Bonus: Review CIS Microsoft Intune Benchmarks

CIS post benchmarks for Microsoft Intune Windows Devices. Currently they have benchmarks for Windows 10 and Windows 11 devices. The granularity of these benchmarks is too verbose to cover in this guide but I would encourage you to review it over time to see what additional controls you would want to add to your baseline depending on your environment.

You can download the benchmarks here in the Microsoft Intune for Windows section: CIS Downloads (cisecurity.org)

Appendix

Customer Checklist

Conditional Access Policy Customer Checklist

Security Baseline Matrix/Checklist