Intune Mobile App Management

Application Protection Policy

aka Nudge for iOS/iPadOS

Contents

[What is this? 2](#_Toc119925327)

[Requirement 2](#_Toc119925328)

[User experience 3](#_Toc119925329)

[Test cases 5](#_Toc119925330)

# What:

The purpose of this document is to walk through a sample configuration which is required for the end goal of configuring Conditional Launch settings for Minimum OS Requirement.

Mobile Application Management (MAM) app protection policies are set of conditions an organization can use for licensed users who use their Azure AD credentials to login into Intune-managed app with app protection policies.

These policies will subject the user’s device whether, managed in an MDM or unmanaged, to a Minimal OS Requirement at application launch. The goal is to encourage users to meet the minimum OS requirement set in the App Protection Policy.

# Requirements

* Application PIN Required: A minimum 4-digit PIN to access the Core Microsoft Apps listed below. 6-digit PINs are stronger and therefore recommended.
  + Users will be required to create an access PIN the first time that they open the app from a work or school account, if they don’t have one set.
* Microsoft Core Apps: Edge, Excel, Office, OneDrive, OneNote, Outlook, PowerPoint, SharePoint, Teams, To-do and Word.
* Apps you can manage with app protection policies.
  + https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy#apps-you-can-manage-with-app-protection-policies

# 

# User experience

|  |  |
| --- | --- |
| 1. Applying Organization’s protection policies:   A black square with white text  Description automatically generated | 1. Device Passcode Requirement: |
| 1. iOS Update Warning:   A screenshot of a phone  Description automatically generated | 1. App Access Blocked: |
| 1. Outlook Org Data Removal |  |

# App Protection Policy Settings

**iOS App Protection policy settings**

**Basics**

Name: iOS/iPadOS Warn and Block OS Requirement

Description: Enforces iOS version and Device Passcode requirements Warn below iOS Vers.x Block below iOS Vers.x

**Apps**

Target Policy to: *Core Microsoft Apps*(11 apps)



Microsoft Edge



Microsoft Excel



Microsoft Office



Microsoft OneDrive



Microsoft OneNote



Microsoft Outlook



Microsoft PowerPoint



Microsoft SharePoint



Microsoft Teams



Microsoft To-Do



Microsoft Word

|  |  |  |
| --- | --- | --- |
| **Config. Item** | **Default Values** | **Info** |
| **Data Protection** |  |  |
| **Data Transfer** |  |  |
| Backup org data to iTunes and iCloud backups | **Allow** | Select Block to prevent backup of org data to iTunes or iCloud. Select Allow to permit backup of org data to iTunes or iCloud. Personal or unmanaged data is not affected. |
| Send org data to other apps | **None Selected** | Select one of the following options to specify the apps that this app can send org data to:  **None:** Do not allow sending org data to any app  **Policy managed apps:** Only allow sending org data to other policy managed apps  **Policy managed apps with OS sharing:** Only allow sending org data to other policy managed apps and sending org documents to other MDM managed apps on enrolled devices  **Policy managed apps with Open-In/Share filtering:** Only allow sending org data to other policy managed apps and filter OS Open-in/Share dialogs to only display policy managed apps  **All apps:** Allow sending org data to any app |
| Save copies of org data | **Greyed out** | Select **Block** to prevent saving a copy of org data to a new location, other than the selected storage services, using "Save As. Select **Allow** to permit saving a copy of org data to a new location using "Save As".  Note: This setting does not apply to all applications. For more information see https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-jos#data-protection. |
| Allow user to save copies to selected services | **Greyed out** | Select the storage services users can save copies of org data to. All other services are blocked. Selecting no services will prevent users from saving a copy of org data. |
| Transfer telecoms data to | **Greyed out** | Typically, when a user selects a hyperlinked phone number in an app, a dialer app will open with the phone number repopulated and ready to call. For this setting, choose how to handle this type of content transfer when it's initiated from a policy-managed app. Additional steps may be necessary in order for this setting to take effect. First, verify that tel and telprompt have been removed from the Select apps to exempt list.  Then, ensure the application is using a newer version of Intune SDK (Version 12.7.0+). |
| Receive data from other apps | **Greyed out** | Select one of the following options to specify the apps that this app can receive data from:  **None:** Do not allow receiving data in org documents or accounts from any app  **Policy managed apps:** Only allow receiving data in org documents or accounts from other policy managed apps  **Any app with incoming org data:** Allow receiving data in org documents or accounts from from any app and treat all incoming data without an user account as org data  All apps: Allow receiving data in org documents or accounts from any app |
| Restrict cut, copy and paste between other apps | **Nothing Selected** | Cut, copy, and paste data between your app and other approved apps installed on the device. Choose to block these actions completely between apps, allow these actions for use with any app, or restrict use to apps that your organization manages.  Policy-managed apps with paste in gives you the option to accept incoming content pasted from another app. However, it blocks users from sharing content outwardly, unless sharing with a managed app. |
| Third party keyboards | **Allow** |  |
| **Encryption:** |  |  |
| Encrypt Org data | **Require** | Choose **Require** to enable encryption of work or school data in this app. Intune enforces iOS/iPadOS device encryption to protect app data while the device is locked.  Applications may optionally encrypt app data using Intune APP SDK encryption. Intune  APP SDK uses iOS/iPadOS cryptography methods to apply 128-bit AES encryption to app data.  When you enable this setting, the user may be required to set up and use a PIN to access their device. If there's no device PIN and encryption is required, the user is prompted to set a PIN with the message "Your organization has required you to first enable a device PIN to access this app."  Go to the official Apple documentation to see which iOS encryption modules are FIPS  140-2 compliant or pending FIPS 140-2 compliance. |
| **Functionality:** |  |  |
| Sync policy managed app data with native apps or add-ins | **Allow** | Choose **Block** to prevent policy managed apps from saving data to the device's native apps (like Contacts, Calendar and widgets), or to prevent the use of add-ins within the policy managed apps. If you choose **Allow**, the policy managed app can save data to the native apps or use add-ins, if those features are supported and enabled within the policy managed app.  Apps may provide additional configuration capability with app configuration policies.  For more information, see the app's documentation. |
| Printing Org data | **Allow** | If blocked, the app cannot print protected data. |
| Restrict web content transfer with other apps | **None Slected** | Select one of the following options to specify the apps that this app can open web content in:  **Microsoft Edge:** Allow web content to open only in Microsoft Edge. Learn how  Microsoft Edge protects your data.  **Unmanaged browser:** Allow web content to open only in the unmanaged browser defined by "Unmanaged browser protocol" setting  **Any app:** Allow web links in any ado |
| Org data notifications | **None Selected** | Select one of the following options to specify how notifications for org accounts are shown for this app and any connected devices such as wearables:  **Block:** Do not share notifications.  **Block org Data:** Do not share org data in notifications. If not supported by the application, notifications are blocked.  **Allow:** Share all notifications.  **Android only:** Note: This setting does not apply to all applications. For more information see  https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-android#data-protection  **iOS only:** Note: This setting does not apply to all applications. For more information see https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios#data-protection |
| **Access requirements** |  |  |
| Configure the PIN and credential requirements that users must meet to access apps in a work context. | | |
| PIN for access | **Require** | If required, a PIN must be used to access the policy-managed app. Users must create an access PIN the first time that they open the app from a work or school account. |
| PIN type | **Numeric** | Numeric PINs are made up of all numbers. Passcodes are made up of alphanumeric characters and special characters. On iOS/iPadOS, to configure "Passcode" type, it requires the app to have Intune SDK version 7.1.12 or above. Numeric type has no  Intune SDK version restriction. |
| Simple PIN | **Allow** | If blocked, users may not create a simple PIN. A simple PIN is a string of consecutive or repetitive digits, such as 1234, ABCD, or 1111. Please note that blocking simple PIN of type 'Passcode' requires the passcode to have at least one number, one letter, and one special character. |
| Select minimum PIN length | **None Selected** | Numeric PINs are made up of all numbers. Passcodes are made up of alphanumeric characters and special characters. On iOS/iPadOS, to configure "Passcode" type, it requires the app to have Intune SDK version 7.1.12 or above. Numeric type has no  Intune SDK version restriction. |
| **TouchID instead of PIN** | **Allow** | Touch ID uses fingerprint recognition technology to authenticate users on iOS devices.  Intune calls the LocalAuthentication API to authenticate users using Touch ID. If allowed, Touch ID must be used to access the app on a Touch ID capable device. |
| **Override biometrics with PIN after timeout** | **Require** | If required, depending on the timeout (minutes of inactivity), a PIN prompt will override biometric prompts. If this timeout value is not met, the biometric prompt will continue to show. This timeout value should be greater than the value specified under Recheck the access requirements after (minutes of inactivity)'. On iOS/iPadOS, this feature requires the app to have Intune SDK version 8.1.1 or above. |
| Timeout (minutes of inactivity) | **30** | Consider 1440 = 24 hrs |
| FaceID instead of PIN for access | **Allow** | Face ID uses facial recognition technology to authenticate users on iOS/iPadOS devices.  Intune calls the LocalAuthentication API to authenticate users using Face ID. If allowed,  Face ID must be used to access the app on a Face ID capable device. |
| PIN reset after X days | **No** | Specify the number of days that must pass before the user must reset the PIN. |
| App PIN when device PIN is set | **Rquired** | If not required, an app PIN does not need to be used to access the app if the device  PIN is set on an MDM enrolled device.  Note: Intune cannot detect device enrollment with a third-party EMM solution on iOS. |
| Work or School creds for access | **Not required** | If required, work or school credentials must be used to access the policy-managed app.  If PIN or biometric methods also required for access to the app, the work or school account credentials will be required on top of those prompts. |
| Recheck access reqs after (mins inactive) | **30** | If the policy-managed app is inactive for longer than the number of minutes of inactivity specified, the app will prompt the access requirements (I.e PIN, conditional launch settings) to be rechecked after the app is launched. |
| **Conditional Launch** | Set the sign-in security requirements for your access protection policy. Select a **Setting** and enter the **Value** that users must meet to sign in to your company app. Then select the **Action** you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. Learn more about conditional launch actions. https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios | |
| **App Conditions** | | |
| Max PIN attempts | **5** | **Reset PIN** |
| Offline grace period | **720** | **Block access (minutes)** |
| Offline grace period | **90** | **Wipe Data (days)** |
| Device Conditions | Configure the following conditional launch settings for device based conditions through your app protection policy.  Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices. https://learn.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started | |
| Jailbroken/rooted devices | **Block** | **Block access** |
| Min OS version | **16.5.1** | **Warning Notification** |
| Min OS version | **16.5** | **Block access** **Notification** |
| Assignments | **Include all eligible groups whether they are BYOD, managed in any MDM, and unmanaged iOS and iPadOS devices** | |