

pax8ProServices

Add Baseline Protections to Microsoft 365 Business Premium

Add Baseline Protections to Microsoft 365 Business Premium

With remote and hybrid work prevalent across industries, the way we protect our data and users has evolved. In this guide, we'll review some basic measures you can take to maximize your customer's **Microsoft 365 Business Premium** investment. We'll cover four topics in this guide:

- Manage the risks associated with BYOD mobile devices.
- Implement Defender for Office 365 to protect against phishing, malicious attachments, and related threats.
- Secure user identities with multifactor authentication, using Conditional Access in Entra ID P1.
- Create a baseline Windows workstation configuration using Windows in Cloud Configuration.

In addition, we've provided guidance on alignment to the [CIS Critical Security Controls](#). These measures should help with the technical alignment pieces for certain controls (listed throughout).

Disclaimer: We believe these technical measures generally align with certain controls and safeguards in CIS v8 but do not warrant full alignment. Partner is responsible for all surrounding operational maturity requirements such as policy and procedure and enforcement of the standards developed, including any customizations to meet specific customer requirements. There is no such thing as 100% protection. Adequate detect, respond, and recover processes are essential to cybersecurity. Pax8 does not warrant against cyber incidents.

Licensing Requirements

To implement these features, the target tenant will need to be licensed with Microsoft 365 Business Premium, Microsoft 365 E3, or Microsoft 365 E5. While a combination of licenses can be applied to meet these requirements, we do not recommend this approach as it adds complexity to license management and often costs more than the bundled licenses. Every user that will benefit from these features must have the appropriate licensing. Certain functionality will not work without appropriate licensing and may leave the tenant improperly secured or cause user interruptions.

Note: When implementing these features for the first time, we highly recommend that you leverage a test group with a fictitious, licensed user and a test Windows machine. This allows you to validate that the policies are working as intended and experience them before rolling them out to users in production.

How to Defend against BYOD Threats

CIS Safeguards Covered: 9.1 relating to mobile devices.

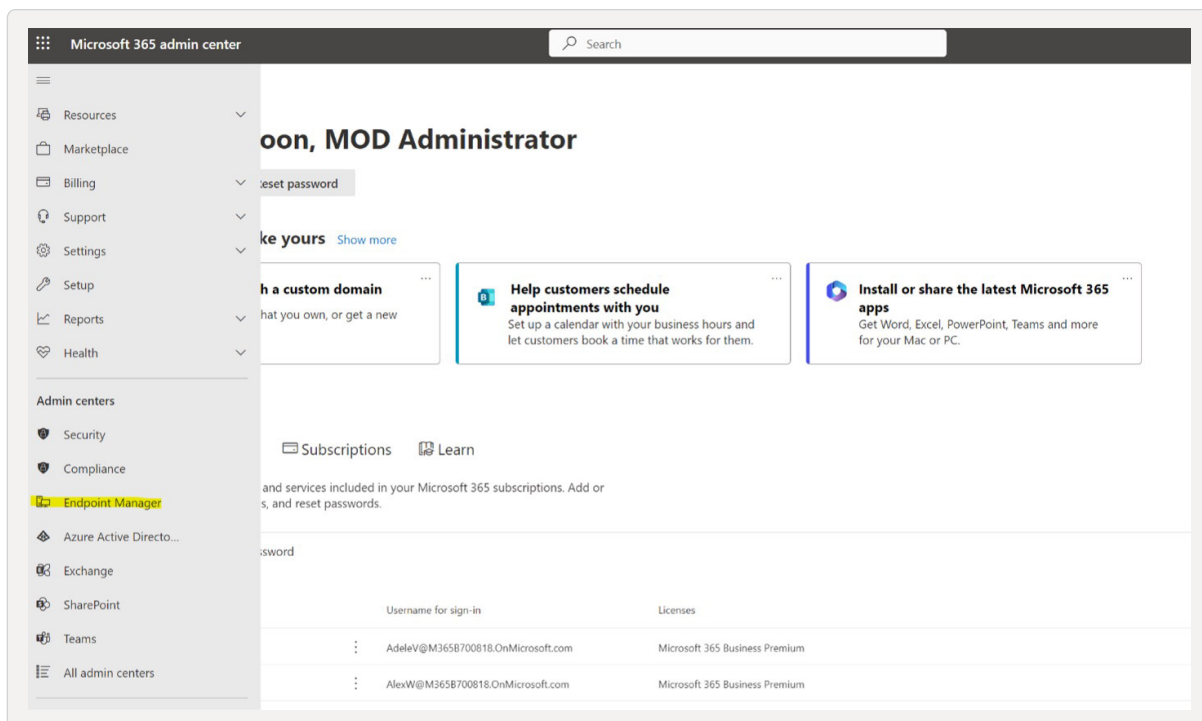
Mobile application management (MAM) in Intune for iOS and Android applies protection policies to core Microsoft applications such as Teams, OneDrive, Outlook, and SharePoint. This management style is ideal for user-owned devices as it only manages the corporate data on those applications. MAM policies strike a great balance between the need to protect corporate data, and the users' privacy. We do not recommend implementing full mobile device management on user-owned devices.

What are app protection policies?

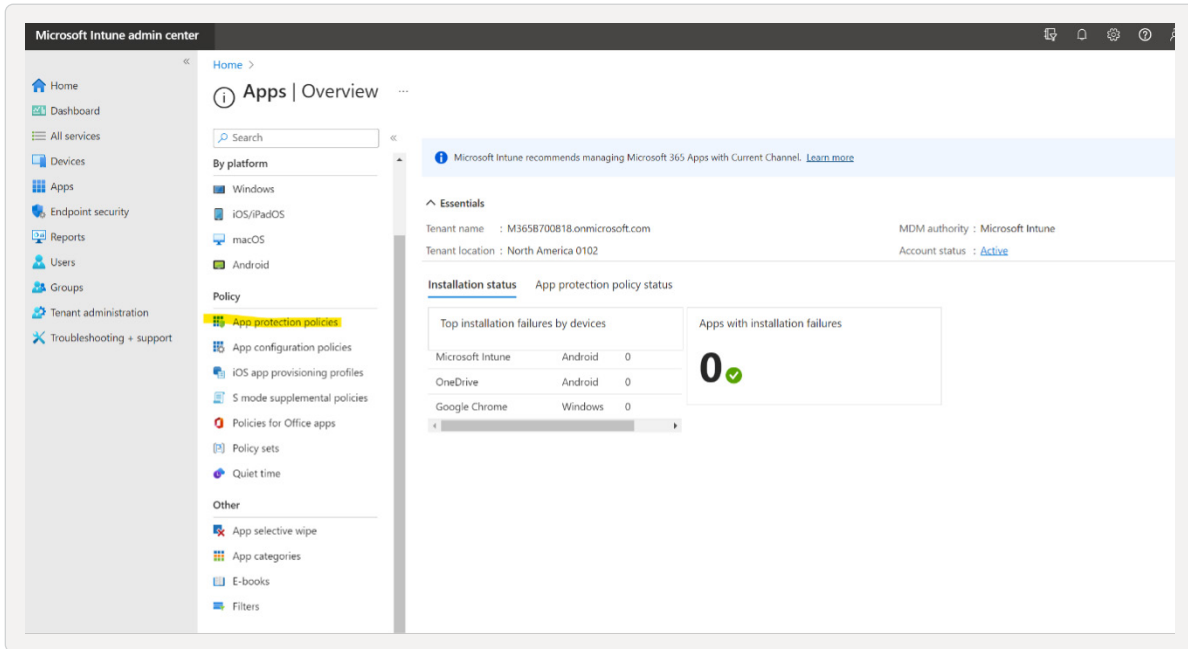
As defined by [Microsoft](#): "App protection policies are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move 'corporate' data or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it and can be managed by Intune."

How to configure iOS App protection policies

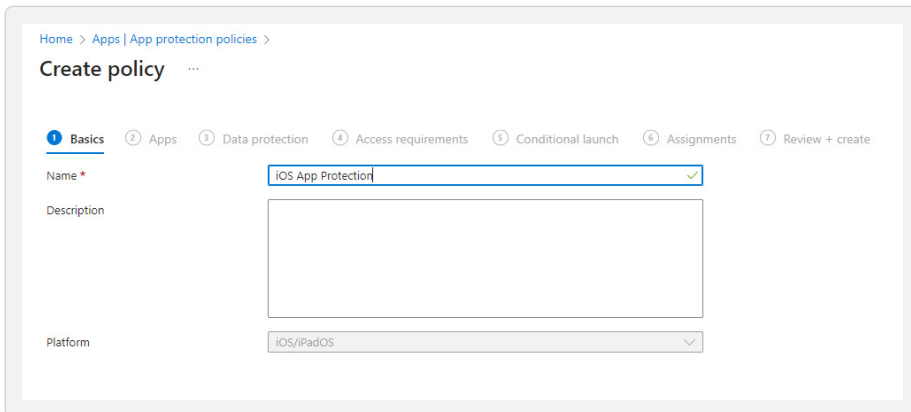
1. Navigate to Endpoint Manager within the Microsoft 365 admin portal.



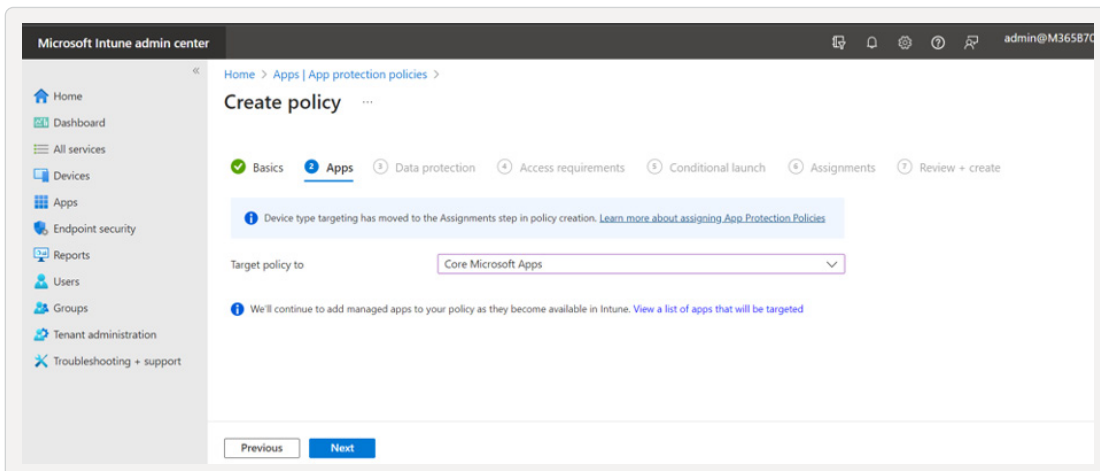
2. Once inside the Endpoint Manager portal, navigate to Apps, then select “App protection policies”.



3. You are now able to build both iOS and Android policies. Start by building iOS:

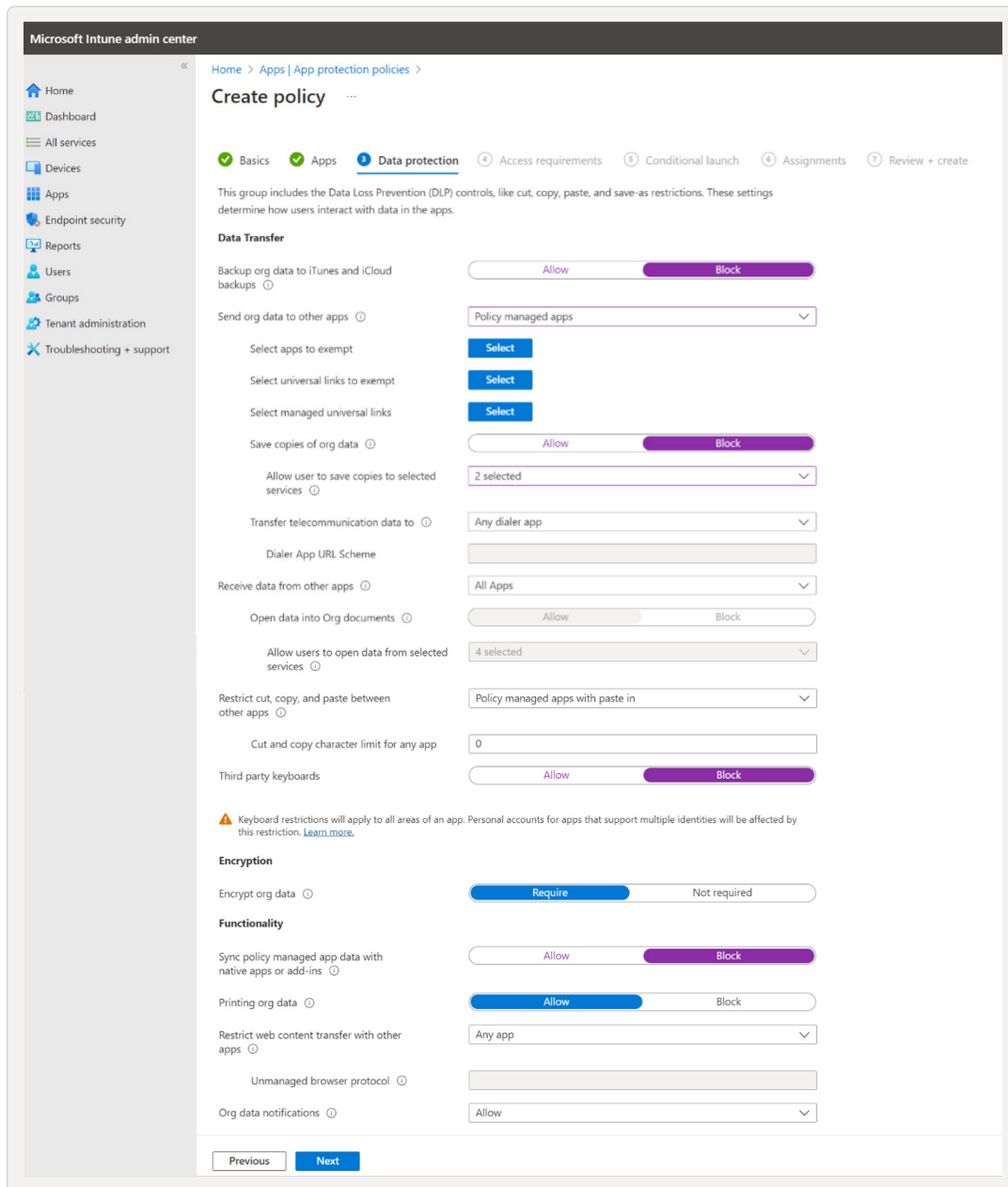


4. Choose “Core Microsoft Apps” for the App selection:

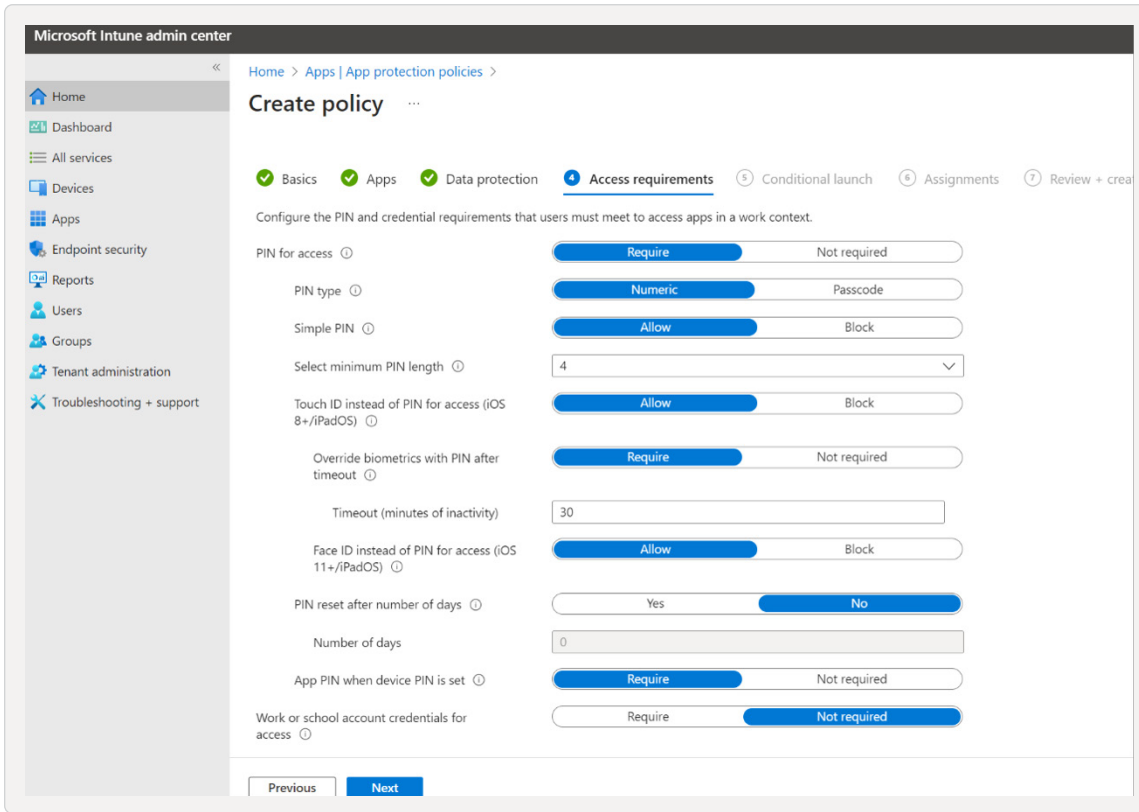


5. Determine your data protection configuration. We recommend these selections:

- Block backups to iCloud (prevents users from backing up company data to personal storage).
- Only send org data to Policy Managed Apps (keeps company data within the company-approved ecosystem, **may limit saving/sharing of data to certain third party apps**).
- Only allow saving copies of org data in OneDrive and SharePoint (prevents saving of files such as email attachments to a personal storage account).
- Restrict cut, copy, and paste to Policy Managed Apps with Paste in (default).
- Block third party keyboards.
- Require encryption of org data (this does require an iOS device level pin).
- Block sync policy managed app data with native apps or add-ins.

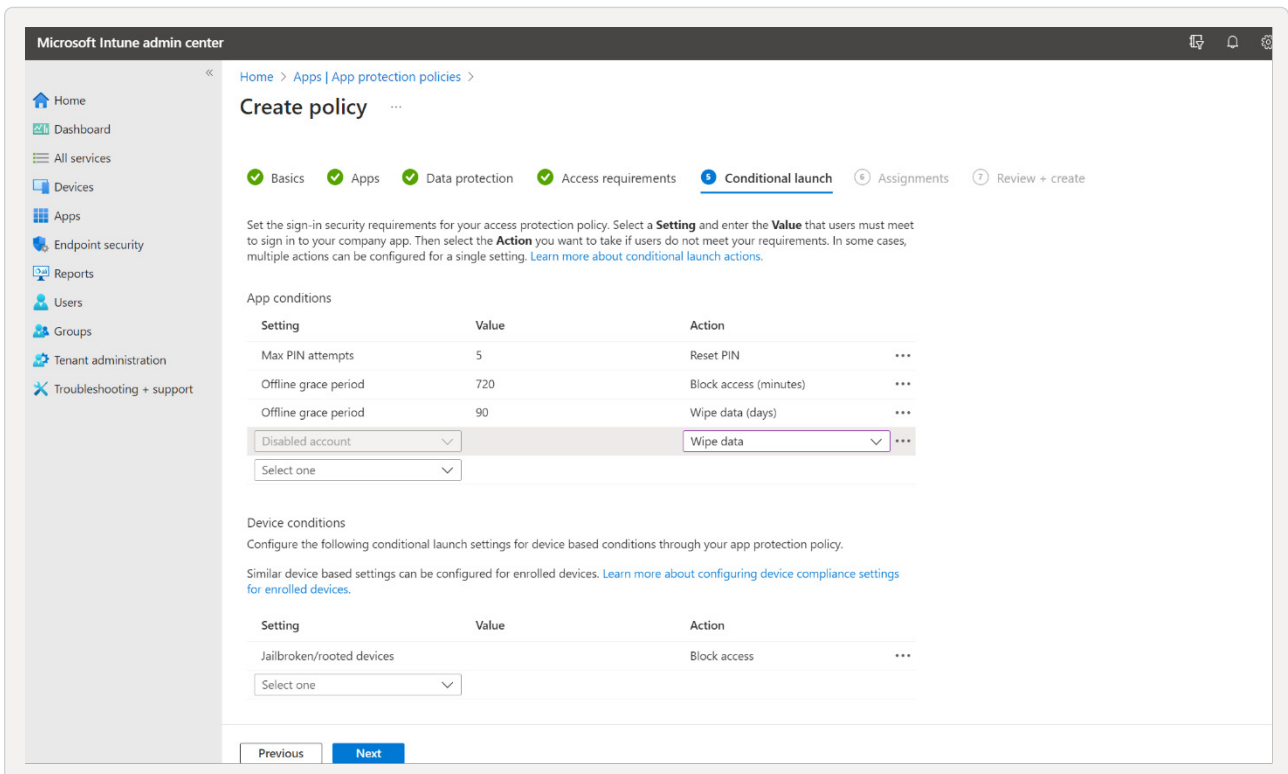


6. Set an app-level pin. Use the settings listed below:



7. Set conditional launch rules:

- Create a new Disabled Account setting with an action of Wipe Data.



8. Assign the policy. Make sure you deploy this to a security group that contains Azure AD identities:

The screenshot shows the 'Create policy' page in the Azure Admin Center, specifically the 'Assignments' step. The breadcrumb navigation is 'Home > Apps | App protection policies >'. The page title is 'Create policy'. There are seven steps in the process: Basics, Apps, Data protection, Access requirements, Conditional launch, Assignments (current step), and Review + create. The 'Included groups' section has an 'Add groups' button and a table with columns: Groups, Group Members, Filter, Filter mode, and Remove. Below this table, it says 'No groups selected'. The 'Excluded groups' section has an information icon and a message: 'When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more about excluding groups.' Below this message is an 'Add groups' button and a table with columns: Groups, Group Members, and Remove. Below this table, it says 'No groups selected'.

How to configure iOS App protection policies

1. Complete steps 1-3 above, as they are the same as with iOS.
2. For Data Protection, see below:
 - Block backup org data to Android backup services.
 - Only send data to policy managed apps.
 - Block saving copies of org data except in SharePoint and OneDrive.
 - Block screen capture and Google Assistant.
 - Allow for Approved Keyboards (more common with Android users).
 - Require encryption.
 - Block sync policy managed app data with native apps or add-ins.

The screenshot shows the 'Create policy' page in the Microsoft Intune admin center, specifically the 'Data protection' tab. The page is divided into several sections with various settings:

- Basics**: Includes 'Data protection' (selected), 'Access requirements', 'Conditional launch', 'Assignments', and 'Review + create'.
- Data Transfer**:
 - 'Backup org data to Android backup services': Set to 'Block'.
 - 'Send org data to other apps': Set to 'Policy managed apps'.
 - 'Select apps to exempt': A 'Select' button is visible.
 - 'Save copies of org data': Set to 'Block'.
 - 'Allow user to save copies to selected services': Set to '2 selected'.
 - 'Transfer telecommunication data to': Set to 'Any dialer app'.
 - 'Dialer App Package ID' and 'Dialer App Name': Empty text input fields.
 - 'Receive data from other apps': Set to 'All Apps'.
 - 'Open data into Org documents': Set to 'Block'.
 - 'Allow users to open data from selected services': Set to '4 selected'.
 - 'Cut and copy character limit for any app': Set to '0'.
- Screen capture and Google Assistant**: Set to 'Block'.
- Approved keyboards**: Set to 'Require'.
- Encryption**:
 - 'Encrypt org data': Set to 'Require'.
 - 'Encrypt org data on enrolled devices': Set to 'Require'.
- Functionality**:
 - 'Sync policy managed app data with native apps or add-ins': Set to 'Block'.
 - 'Printing org data': Set to 'Allow'.
 - 'Restrict web content transfer with other apps': Set to 'Any app'.
 - 'Unmanaged Browser ID' and 'Unmanaged Browser Name': Empty text input fields.
 - 'Org data notifications': Set to 'Allow'.
 - 'Start Microsoft Tunnel connection on app-launch': Set to 'No'.

At the bottom of the page, there are 'Previous' and 'Next' buttons.

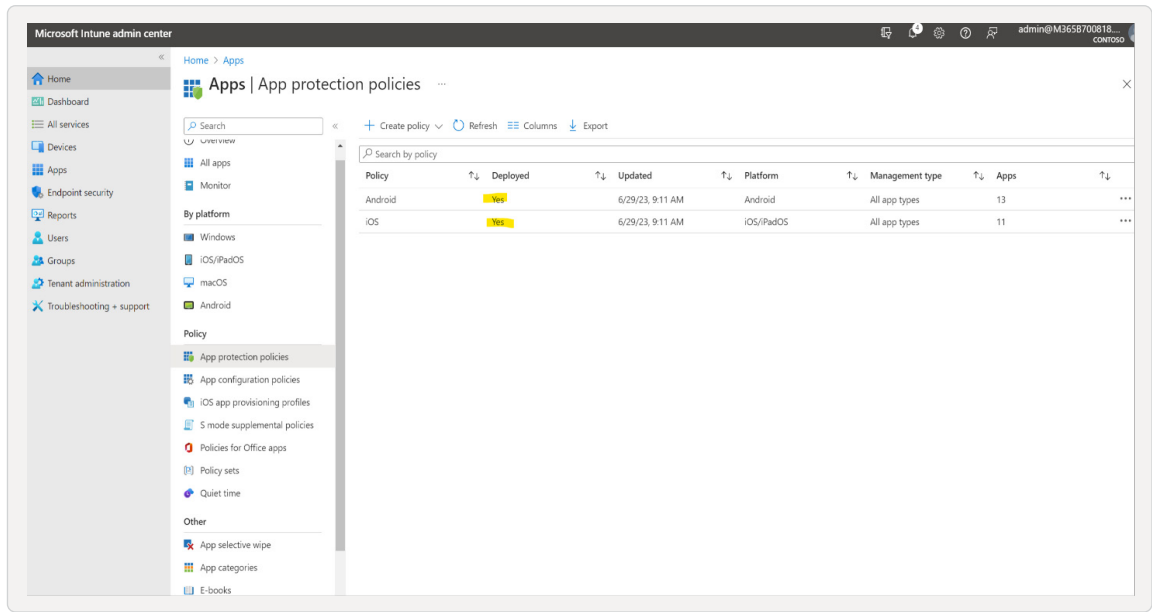
3. Complete steps 6-8 as in the iOS policy creation.

Conditional access

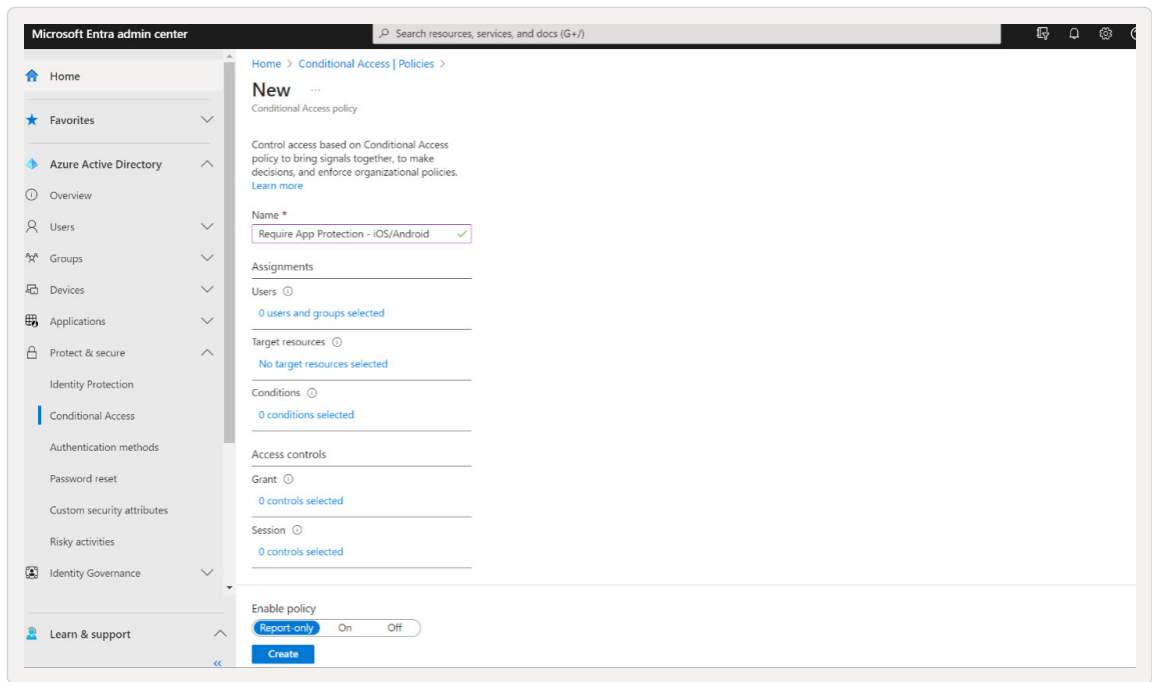
Conditional access forces mobile device access from only protected apps (Microsoft apps such as Outlook, Teams, Office, etc.)

Note: Once you turn on this Conditional Access policy, users will no longer be able to use built-in mail and collaboration apps such as iOS mail or Samsung Mail. We recommend guiding users through the transition to first-party apps (like Outlook mobile) before enforcing this policy.

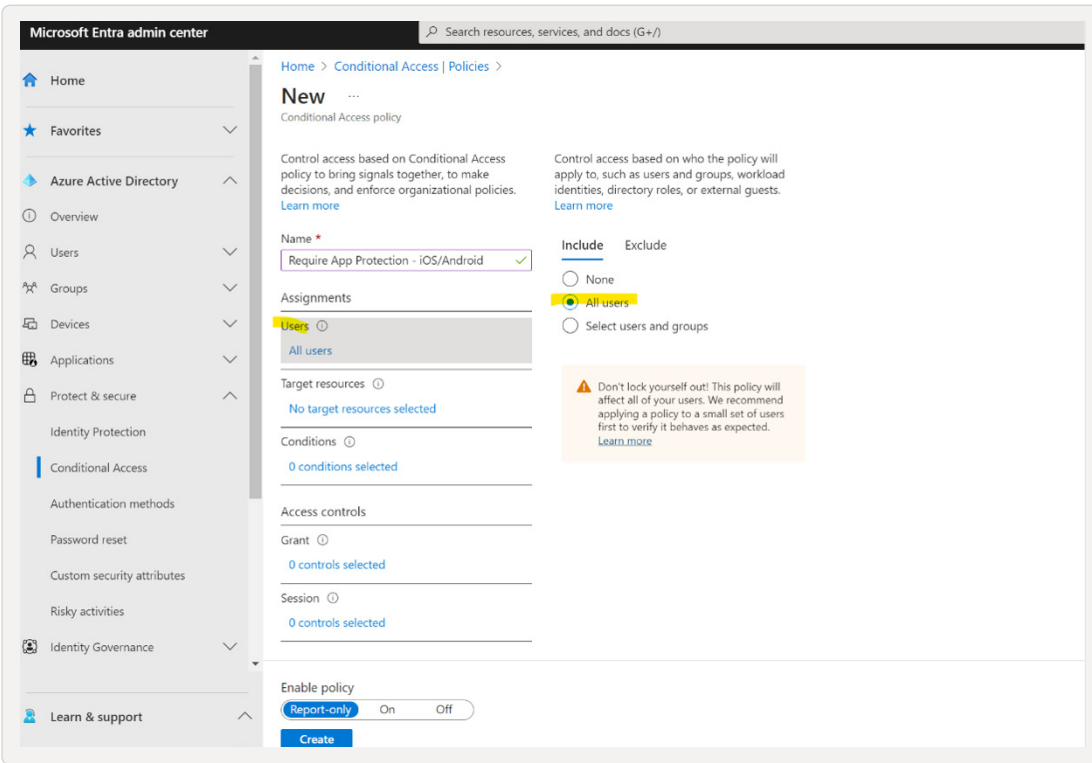
1. Before creating your conditional access policy, confirm that your app protection policies are built and properly deployed. Ensure that enough time has passed since these have been built



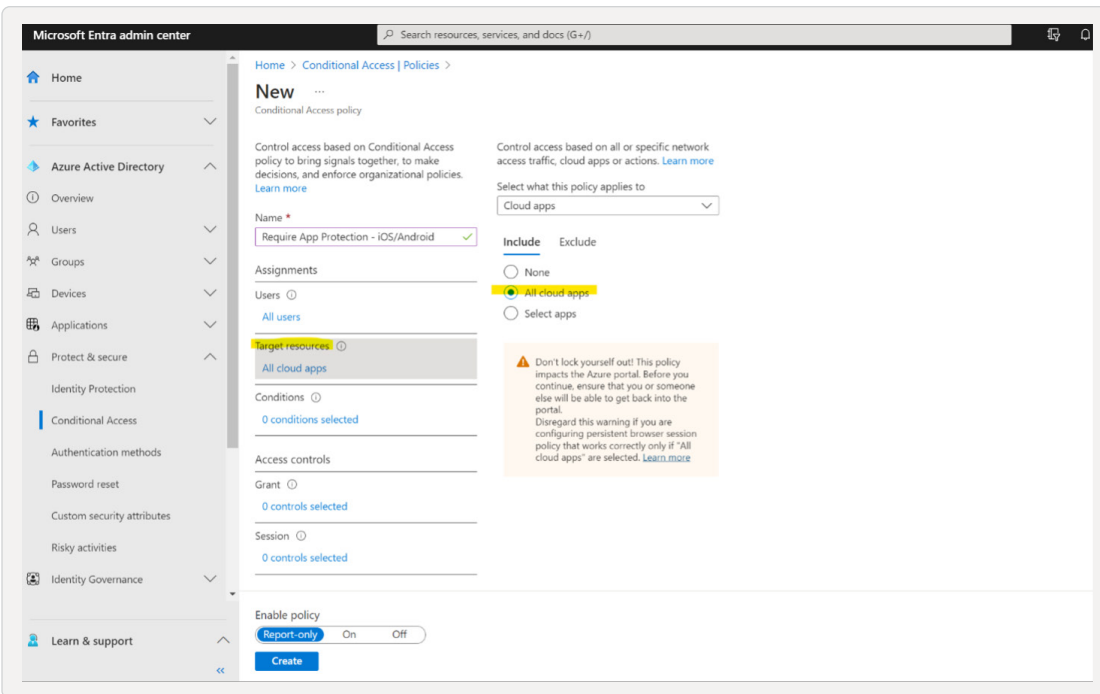
2. Now navigate to “Azure AD/Entra” and build your conditional access policy:



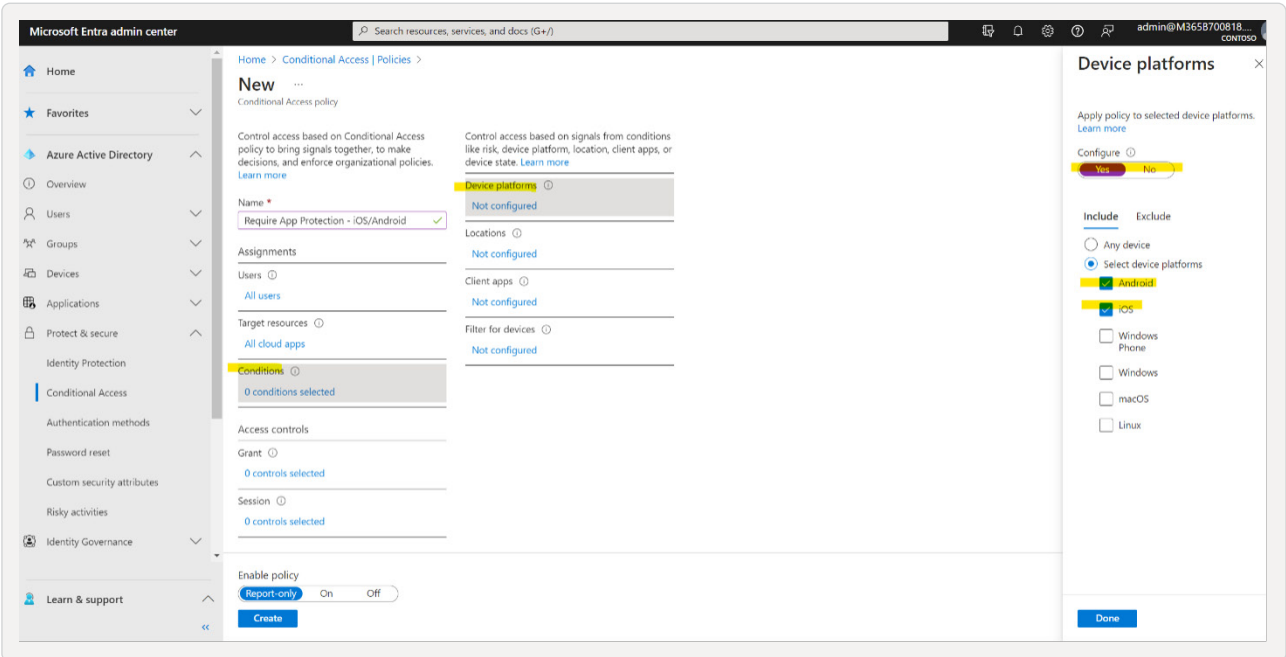
3. For the “Users” scope, select “All Users”:



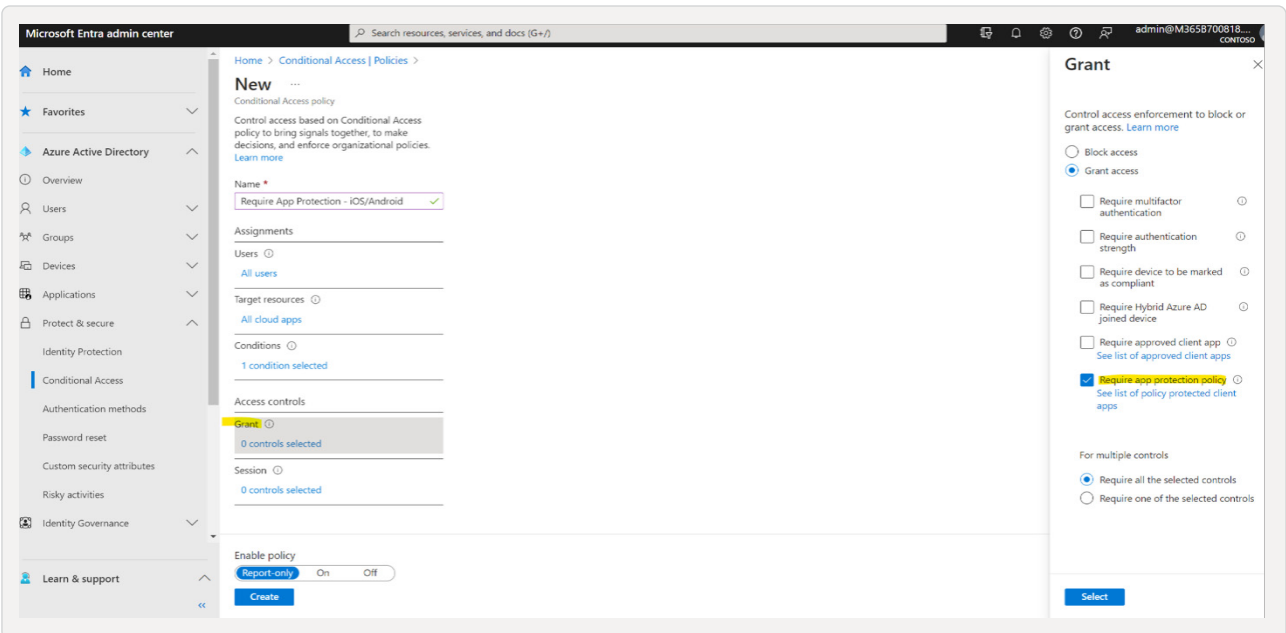
4. For “Target resources,” choose “All cloud apps”:



5. For “Conditions,” choose “iOS and Android” for “Device platforms”:



6. For the “Grant” action, select “Require app protection policy”:



7. Set the policy to “Report-only”.

Secure Collaboration with Defender for Office 365

CIS Safeguards Covered: 9.7

This document will guide you through the standard configuration of the following:

- Defender for Office 365: Safe Links
- Defender for Office 365: Safe Attachments
- Defender for Office 365: Anti-Phishing

Implementation of these safeguards satisfies CIS Control 9.7 and is associated with the Protect function outlined in the framework. Success with this control protects users from detected malicious content.

Note: Implementing these policies will have an impact on user experience, specifically as it relates to email attachments. We recommend reviewing the [documentation](#) on Safe Attachments prior to implementing this policy.

Defender for Office 365: Safe Links

1. Navigate to:
2. Select “Threat policies.”
3. Select “Safe links.”
4. Choose “Create to create a new safe links policy.”
5. Step: name your policy.
 - Name the policy “Global Safe Links Policy” (or another easily identifiable name).
 - Select Next.
6. Step: users and domains.
 - Under the “Domains” field, enter all tenant domains that should be protected by this policy.
Note: Ensure that the tenant.onmicrosoft.com domain is also added to this list to avoid circumvention of this protection.
 - Select “Next.”
7. Step: URL and click-protection settings.
 - Uncheck “Do not rewrite URLs, do checks via Safe Links API only.”
Note: Default settings are acceptable in most engagements, except for this option. This option should be disabled to ensure URLs are scanned when clicked from any email client.
 - If URL rewrites should be excluded from specific domains, they can be specified by clicking the link in the “Do not rewrite the following URLs in email” section.
 - Uncheck “Let users click through to the original URL.”
Note: Leaving this option enabled will allow users to bypass a known (or suspected) threat.
 - Select “Next.”
8. Step: Notification.
 - Use the default notification text in most engagements. If a predetermined notification text has been provided, enter it in the “Use custom notification” text field.
 - Select “Next.”
9. Step: Review.
 - Review all settings of the new safe links policy and choose “Submit” to begin immediate enforcement.

Defender for Office 365: Safe Attachments

1. Navigate to [policies & rules](#).
2. Select “Threat policies.”
3. Select “Safe attachments.”
4. Choose “Create” to create a new safe attachments policy.
5. Step: Name your policy.
 - Name the policy “Global Safe Attachments Policy” (or another easily identifiable name).
 - Select “Next.”
6. Step: Users and domains.
 - Under the Domains field, enter all tenant domains that should be protected by this policy.
Note: Ensure that the tenant.onmicrosoft.com domain is also added to this list to avoid circumvention of this protection.
 - Select “Next.”
7. Step: Settings.
 - Choose “Dynamic Delivery to immediately deliver messages without attachments.”
Note: Once the attachment is scanned by Defender, the files will be reattached to the original message automatically. A text file will be provided to the user as an attachment while the scanning is in progress to explain this behavior.
 - Leave all other default settings intact and choose “Next.”
8. Step: Review.
 - Review all settings of the new safe attachments policy and choose “Submit” to begin immediate enforcement.

Defender for Office 365: Anti-phishing

1. Navigate to [security policies and rules](#).
2. Select “Threat policies.”
3. Select “Anti-phishing.”
4. Choose “Create to create a new anti-phishing policy.”
5. Step: name your policy.
 - Name the policy “Global Anti-phishing Policy” (or another easily identifiable name).
 - Select “Next.”
6. Step: users, group, and domains.
 - Under the “Domains” field, enter all tenant domains that should be protected by this policy.
Note: Ensure that the tenant.onmicrosoft.com domain is also added to this list to avoid circumvention of this protection.
 - Select “Next.”
7. Step: phishing threshold and protection.
 - Phishing email threshold:
 - » 1-Standard.
 - Impersonation:
 - » Select “Enable domains to protect.”
 - » Select “Include domains I own.”
 - » Select “Enable mailbox intelligence.”
 - » Select “Enable intelligence for impersonation protection.”
 - Spoof:
 - » Select “Enable spoof intelligence.”
 - Select “Next.”
8. Step: actions.
 - Message actions:
 - » If a message is detected as domain impersonation: quarantine the message.
 - » Apply quarantine policy: AdminOnlyAccessPolicy.
 - » If Mailbox Intelligence detects an impersonated user: quarantine the message.
 - » Apply quarantine policy: AdminOnlyAccessPolicy.
 - » If the message is detected as spoof-by-spoof intelligence: quarantine the message.
 - » Apply quarantine policy: AdminOnlyAccessPolicy.
 - Safety tips and indicators:
 - » Enable all options.
 - Select Next.
9. Step: review.
 - Review all settings of the new anti-phishing policy and choose “Submit” to begin immediate enforcement.

Secure User Identities with Entra ID Conditional Access

CIS Safeguards Covered: 6.3, 6.5

Note: These policies will impact the login experience for users by requiring secure multifactor authentication. This policy will require that users leverage push notifications with the Microsoft Authenticator app or use FIDO2 security keys (such as a YubiKey). This policy will **prevent the use of SMS or other insecure MFA methods**.

Enable FIDO2 Authentication

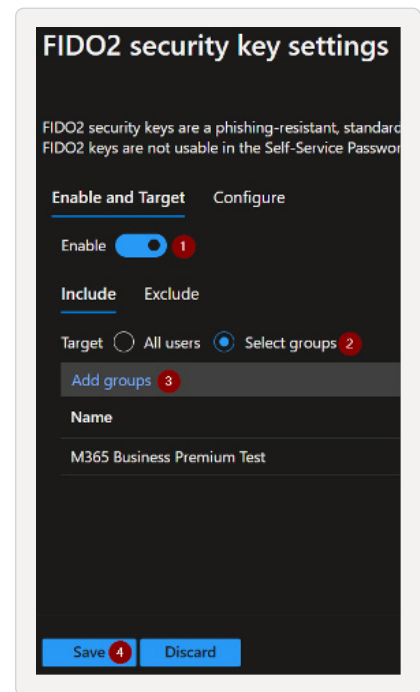
FIDO2 is a highly secure and phishing resistant yet simple form of authentication. It involves the use of a hardware key to authenticate. The user authenticates by having possession of their hardware key (type 2) and presenting a security key PIN (type 1) or biometric (type 3) depending on the key's model. The PIN or biometric is specific to the key itself and cannot be used elsewhere. FIDO2 is also the underlying mechanism used in Passkeys, which will ultimately allow for the replacement of the security key with a mobile device.

During authentication, Microsoft will present a “challenge” (one time use value) that is then cryptographically signed using a private key that is only available on the hardware key. Microsoft will then use the public key half of the keypair to validate the cryptographic signature and authenticate the user. Under this model, no secret (password) ever crosses the network. Just a signed challenge that is only usable for that single authentication instance. FIDO keys do not require their own internet connection, they interact over USB, NFC, or Bluetooth Low Energy (BLE).

FIDO2 is widely regarded as the most phishing resistant authentication method that is easy to implement. Because secrets are not shared, there is no opportunity to intercept a password. Additionally, the hardware key and server mutually authenticate each other. Your security key will only sign a challenge for the appropriate domain for which it was enrolled, preventing adversary-in-the-middle attack. Pax8 and Microsoft recommend [YubiKey](#) security keys.


- Ensure all phishing resistant authentication methods are enabled.
- Navigate to Microsoft [Entra Portal](#).
- Select “Protect & secure.”
- Select “Authentication methods.”
- Select “FIDO2 security key.”
- Select “Enable.”
- Target your test group by selecting “Select groups” and “Add groups,” and choose your test group.
- Select “Save.”

Tip: You can safely enable FIDO2 for all users instead of scoping it to a group. Enabling this method simply allows users to enroll and use it, it does not force them to do so.



Enable Microsoft Authenticator Sign On


Authenticator sign-on allows a user to verify their identity using the Microsoft Authenticator mobile app, without a password. The authentication factors for this method are possession of the device being used (type 2) and the ability to unlock the device with biometrics (type 3) or a PIN (type 1). In addition, the user must enter a number shown on the login page, reducing the likelihood of MFA fatigue attacks.

- Ensure all phishing resistant authentication methods are enabled.
- Navigate to Microsoft [Entra Portal](#).
- Select “Protect & secure.”
- Select “Authentication methods.”
- Select “Microsoft Authenticator”
- Flip the “Enable” switch **Enable** 
- Under “Include” change the option to “Select” groups and add your test group

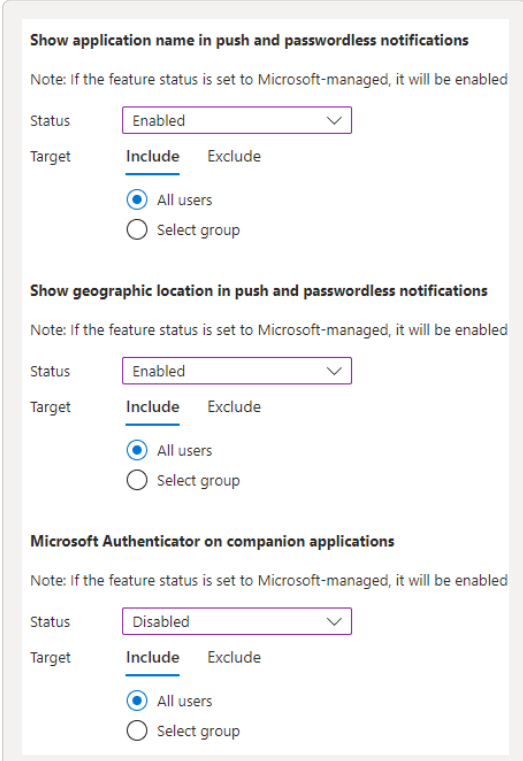
Include Exclude

Target All users Select groups

[Add groups](#)

- Go to the “Configure” tab **Enable and Target** **Configure** 

- Choose whether to enable Microsoft Authenticator OTP. Authenticator OTP involves using the ephemeral code displayed within the app and is the only way to authenticate when the device is offline.
- **Require number matching for push notifications** is no longer an optional setting due to MFA fatigue attacks coming online. [Learn more.](#)
- **Show application name in push and passwordless notifications** provides additional context to the user around what they are logging into. We recommend setting the status to “Enabled” to give the user additional context. This information is also useful for investigative purposes.
- **Show geographic location in push and passwordless notifications** will show the user from where the authentication request is coming from, based on the request’s IP address. We recommend you turn it on, but be aware that if a user is using a remote desktop (such as AVD), the location of that endpoint will be shown and may be different than their physical location.
- **Microsoft Authenticator on companion applications** enables the use of companion apps for wearable devices. Most of these companion apps are being deprecated, so we recommend **disabling** these settings until they are rebuilt and can be tested.



The screenshot shows three configuration sections for Microsoft Authenticator:

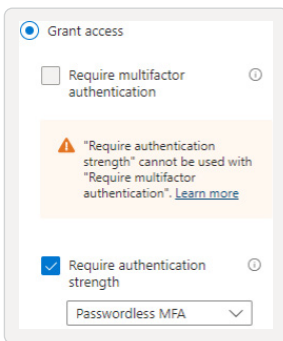
- Show application name in push and passwordless notifications**: Status is set to "Enabled", Target is "Include" with "All users" selected.
- Show geographic location in push and passwordless notifications**: Status is set to "Enabled", Target is "Include" with "All users" selected.
- Microsoft Authenticator on companion applications**: Status is set to "Disabled", Target is "Include" with "All users" selected.

Tip: You can safely enable Authenticator for all users instead of scoping it to a group. Enabling this method simply allows users to enroll and use it, it does not force them to do so.

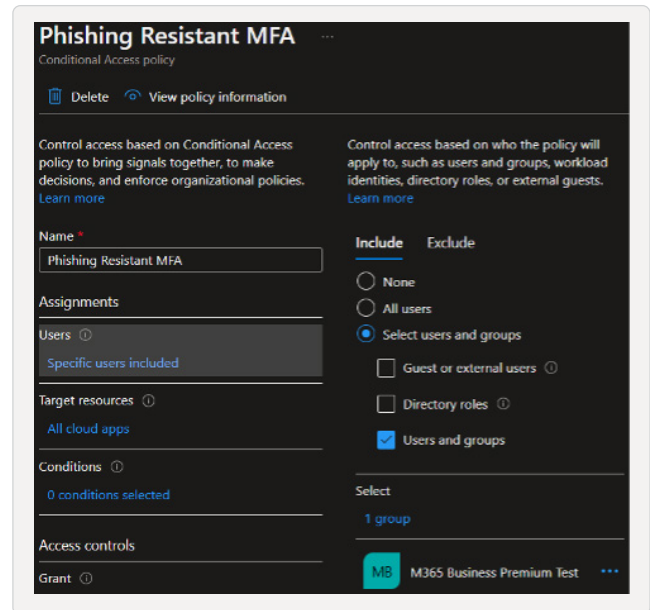
Note: Microsoft Authenticator sign-on and MFA is known to be vulnerable to adversary-in-the-middle proxy-based attacks (in which the user’s session token is stolen in flight after authentication). Users should be educated to double check the domain name to which they are authenticating and should be wary if the location presented by Authenticator does not match their current location. Users should also be trained to never share the challenge number with anyone.

Require Secure MFA with Conditional Access

- Create an initial test group in Azure AD titled “Identity Security Test.”
- Navigate to Microsoft [Entra Portal](#).
- Navigate to [Conditional Access](#).
- Select “New policy.”
- Name: “Require Secure MFA.”
- Users: Select your test group.
 - Target resources: All cloud apps.
 - Conditions: Not configured.
 - Grant: Grant access – Select “Require authentication strength” and select “Passwordless MFA.”



- Set Policy to “On.” – Only set the policy to on if you have properly scoped it to your test group.



Note: Enabling this policy for everyone takes effect immediately and will prevent copiers, applications, and other third-party items from accessing the tenant unless they do so with Graph API and enterprise applications. Care should be taken when rolling this policy into production, and service accounts may need to be excluded. Consider [Entra Workload ID](#) to more securely implement these services.

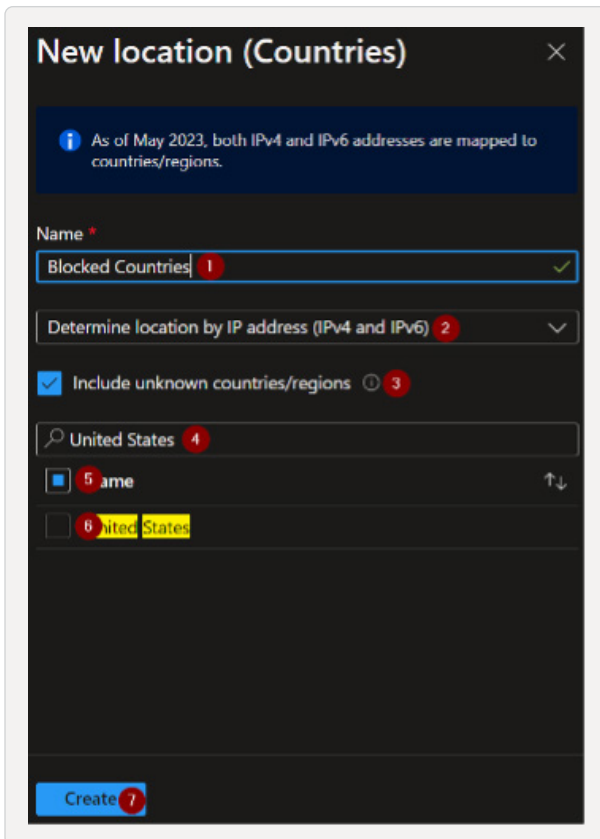
Optional: Geo-fencing to country/countries of choice

Many attacks start with an automated test. Geo-fencing will not stop a motivated threat actor, who can quickly change countries for pennies. However, it helps stop automated attacks running in other countries. Geographic policies use IP address databases to understand where a particular request is coming from. We’ve seen this be highly effective. However, from time to time, an IP address may be matched to the wrong country. Always keep your geo-fencing policy as a stand-alone policy, and give it a telltale name so it shows clearly in audit logs.

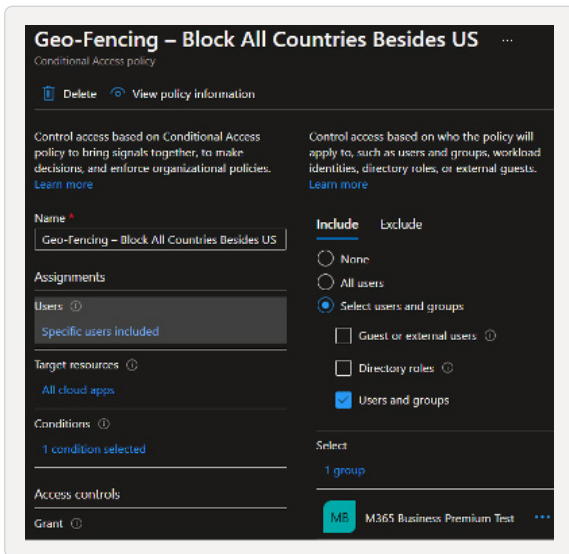
If you have users that travel internationally, consider allowing countries they travel to often and implementing a “travel notification” process so that users can alert you of impending travel. This will allow you to either temporarily exclude the user from the policy or allow the country(ies) to which they are traveling.

In these steps, we'll be creating a "Travelers" group so that you can add users to this group when they are traveling and remove them upon their return.

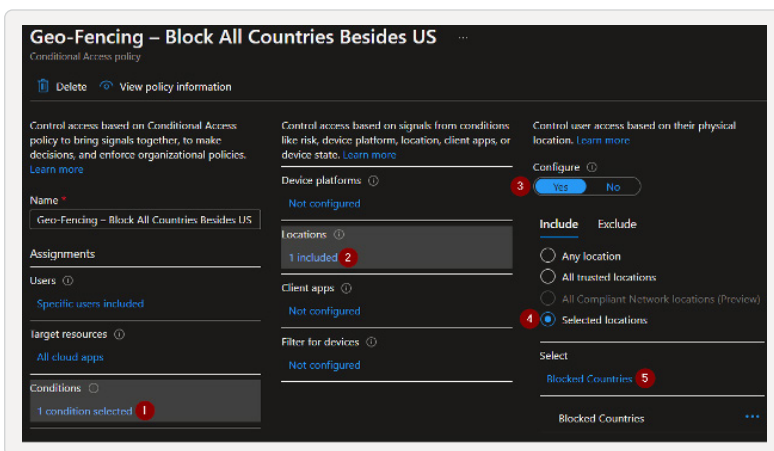
- Navigate to Microsoft [Entra Portal](#).
- Navigate to Groups > All groups and create a new security group called "Travelers." Leave it empty for now, this group will be used to add traveling users to temporarily exclude them from this policy.
- Navigate to [Conditional Access](#).
- Select "Named locations."
 - Select "+ Countries location."
 - Name: "Blocked Countries."
 - Select "Determine location by IP address."
 - Check "Include unknown countries/regions."
 - Select the check box to the left of the "Name" column to select all countries.
 - Search for United States and deselect the United States and other countries where business is conducted.
 - Click "Create."



- Navigate back to Conditional Access by selecting “Policies.”
- Select “New policy.”
 - Name: “Geo-Fencing – Allow trusted countries only “
 - Users: Select your test group.
 - In the **Exclude** tab, add your Travelers group.



- Target resources: All cloud apps.
- Conditions:
 - » Locations – Select “Yes” to configure.
 - » Under “Include,” select “Selected locations.”
 - » Select the named location created in the steps above titled “Blocked Countries.”



- Grant: Select “Block access” and click “Select” at the bottom to save the selection.
- Set policy to “On.” – Only turn the policy on if you have scoped it to your test group.

Tip: If your customer has frequent cases of international travel, Entra ID P2 with Privileged Access Management (PAM) can be used to allow users to self-service add themselves to the Travelers group, subject to policy set in PAM. Setting this up is outside of the scope of this guide, but Pax8 Professional Services can assist.

Baseline Windows Management: Windows in Cloud Configuration

CIS Safeguards Covered: 3.6, 4.1, 4.5, 4.11, 10.3, 10.5 relating to Windows Workstations

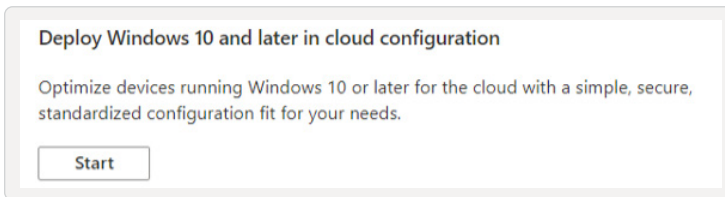
Windows in Cloud Configuration is a baseline set of policies, recommended by Microsoft, that create a more hardened Windows environment out of the box. It covers the “basics” of endpoint management such as disk encryption, patching, and Office app deployment.

Windows in Cloud Configuration can be modified or extended post deployment to deploy additional apps or tweak settings as needed.

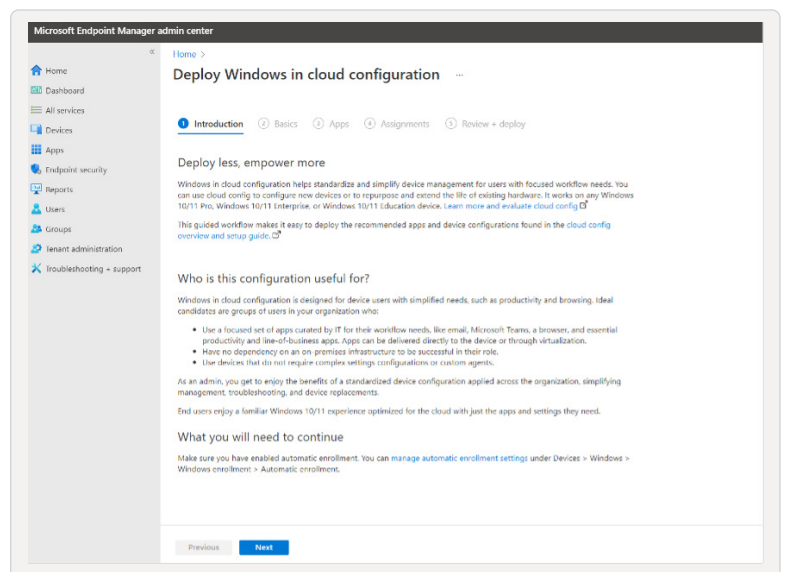
Note: By default, Windows in Cloud Configuration will create a patching policy with which Intune will assume control of patching Windows. If you wish to manage patches with your RMM tool, complete this guide and then remove or unassign the patching policies that are created under Devices > Windows devices in the Intune admin center.

Step 1: Navigate to Windows in Cloud Configuration

1. Navigate to endpoint.microsoft.com and sign in with an Intune (or higher level) Administrator account.
2. On the Home screen, select “See All” next to Guided Scenarios.
 - You may be presented with an introduction screen next, where you will click “Got It” to show the next steps.
3. Select “Deploy Windows 10 and Later in Cloud Configuration” as seen below:



4. Once you click “Start,” you will see a page that outlines prerequisites and other information around the overall configuration:



*If you are unsure about the Windows in Cloud Configuration, refer to the included documents:

[Windows 11 Cloud Configuration for Endpoint Management - Microsoft 365](#)
[Windows in cloud configuration \(microsoft.com\)](#)

Step 2: Windows in Cloud Configuration Basics and Device Name Template

1. Once you have read the introduction page, you can click “Next” at the bottom. This will now bring you to the Basics page, where you can create a device name template and a resource name prefix:

Microsoft Endpoint Manager admin center

Deploy Windows in cloud configuration

Autopilot device name template

Devices will be configured to enroll with Windows Autopilot. You can apply a device name template to organize your devices.

Apply device name template No Yes

Create a unique name for your devices. Names must be 15 characters or less, and can contain letters (a-z, A-Z), numbers (0-9), and hyphens. Names must not contain only numbers. Names cannot include a blank space. Use the %SERIAL% macro to add a hardware-specific serial number. Alternatively, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

Enter a name *

Resource name prefix

Give a name to the resources that will be created and deployed as part of cloud config. The list at the bottom of this page shows how the name will appear next to each resource.

Enter a resource prefix name *

Resources to be created

- M365 (Teams) 20220121_9:40:53
- Microsoft Edge 20220121_9:40:53
- security baseline 20220121_9:40:53
- BitLocker endpoint security profile 20220121_9:40:53
- Autopilot profile 20220121_9:40:53
- ESP 20220121_9:40:53
- OneDrive Known Folder Move settings 20220121_9:40:53
- Microsoft Edge app settings 20220121_9:40:53
- compliance policy 20220121_9:40:53
- built-in app removal script 20220121_9:40:53
- update ring 20220121_9:40:53

2. The device name template applies to devices that will enroll using Autopilot. If you are not using Autopilot, we will leave this set to “No” unless otherwise stated by the partner.
3. The resource name template allows you to add a prefix to the resources that will be created. Title it as “Cloud Config” and select “Office Open XML” as a document type:

Resource name prefix

Give a name to the resources that will be created and deployed as part of cloud config. The list at the bottom of this page shows how the name will appear next to each resource.

Enter a resource prefix name *

Resources to be created

Default File Format *

- Cloud Config M365 (Teams) 20230628_14:04:12
- Cloud Config Microsoft Edge 20230628_14:04:12
- Cloud Config security baseline 20230628_14:04:12
- Cloud Config BitLocker endpoint security profile 20230628_14:04:12
- Cloud Config Autopilot profile 20230628_14:04:12
- Cloud Config ESP 20230628_14:04:12
- Cloud Config OneDrive Known Folder Move settings 20230628_14:04:12
- Cloud Config Microsoft Edge app settings 20230628_14:04:12
- Cloud Config compliance policy 20230628_14:04:12
- Cloud Config built-in app removal script 20230628_14:04:12
- Cloud Config update ring 20230628_14:04:12

Step 3: Deploy Additional M365 Apps

Deploy Apps as listed below unless otherwise designated by the partner:

The screenshot shows the 'Choose apps' step in a wizard. The progress bar at the top indicates: Introduction (checked), Basics (checked), Apps (active), Assignments (disabled), and Review + deploy (disabled). The main heading is 'Choose apps'. Below it, a note states: 'Cloud config comes with Microsoft Edge for Windows and Microsoft Teams. You can remove these apps, add other Microsoft 365 apps, and deploy essential line-of-business apps to devices anytime. We recommend choosing the smallest number of additional apps possible to help keep your cloud config devices simple and easy to manage.' Under 'Cloud config defaults', there are three checkboxes: 'M365 app name' (checked), 'Microsoft Teams' (unchecked), and 'Microsoft Edge for Windows 10 and later' (unchecked). Under 'Select additional M365 apps (optional)', there is a section for 'M365 app name' with a list of apps: 'Access' (checked), 'Excel' (checked), 'OneNote' (checked), 'Outlook' (checked), 'PowerPoint' (checked), 'Publisher' (checked), 'Skype for Business' (unchecked), and 'Word' (checked).

Step 4: Create a new Security Group or Assign to an Existing One

Here, we will create a new group titled "Intune Test" with no users added for the initial deployment and testing. Alternatively, we can select a group if a partner has opted to go with a current group for testing:

The screenshot shows the 'Choose groups' step in a wizard. The progress bar at the top indicates: Introduction (checked), Basics (checked), Apps (checked), Assignments (active), and Review + deploy (disabled). The main heading is 'Choose groups'. There are two radio button options: 'Create a new group' (selected) and 'Choose an existing group' (unselected). Below this, a blue information box contains a note: 'We recommend assigning cloud config to devices that don't have other profiles and apps assigned to them yet. You can remove or exclude existing resources from groups temporarily and add them back in after you deploy cloud config.' At the bottom, there is a 'Group name *' label and a text input field containing 'Intune Test' with a green checkmark icon to its right.

Step 5: Review the Cloud Configuration

Once you have decided on your security group, you can proceed to the next page. This will be a review of any resources and applications that are being deployed. Double check that you chose the correct security group before pressing deploy.

Microsoft Endpoint Manager admin center

Home >

Deploy Windows in cloud configuration

Introduction Basics Apps Assignments **Review + deploy**

Summary

Basics

Apply device name template No

Enter a resource prefix name Basic

Apps

Selected apps Microsoft Teams
Microsoft Edge for Windows 10 and later

Assignments

Group name Win10_Cloud_Config_Test

What happens when I select Deploy?

The group you chose will be configured with Windows in cloud configuration.

Configurations to be made

Resource	Resource Type	More
Win10_Cloud_Config_Test	AAD Security Group	Docs
Basic M365 (Teams) 20220121_9:40:53	M365 App Suite	Docs
Basic Microsoft Edge 20220121_9:40:53	App	Docs
Basic security baseline 20220121_9:40:53	Security baseline for Windows 10 and later	Docs
Basic BitLocker endpoint security profile 20220121_9:40:53	Endpoint security profile	Docs
Basic Autopilot profile 20220121_9:40:53	Autopilot profile	Docs

Previous Deploy

*If you are unsure about what is included in some of the resources, click on “Configurations to be made,” and it will open a portion that includes docs for each resource included in the configuration.

Step 6: Deploying the Cloud Configuration

Now that you have clicked deploy after the review page, it will first create your resources one by one and then assign them to the security group. Once complete, you will get a notification telling you that the deployment has finished:

The screenshot displays the Microsoft Endpoint Manager admin center interface. The main content area shows a confirmation message: "Deployment succeeded." Below this, a table titled "Deployment details" lists the resources that were created and assigned. The table has four columns: Resource, Resource Type, More, and Assignment. The resources listed include Win10_Cloud_Config_Test, Basic MS365 (teams), Basic Microsoft Edge, Basic security baseline, Basic BitLocker endpoint security profile, Basic Autopilot profile, Basic ESP, Basic OneDrive Known Folder Move, Basic Microsoft Edge app settings, Basic compliance policy, Basic built-in app removal script, and Basic update ring. Each resource has a "Created" status and is assigned to the "AAD Security Group".

Resource	Resource Type	More	Resource	Assignment
Win10_Cloud_Config_Test	AAD Security Group	Docs	Created	---
Basic MS365 (teams) 20220121_1001:11	MS365 App Suite	Docs	Created	Assigned
Basic Microsoft Edge 20220121_1001:11	App	Docs	Created	Assigned
Basic security baseline 20220121_1001:11	Security baseline for Windows 10 and later	Docs	Created	Assigned
Basic BitLocker endpoint security profile 20220121_1001:11	Endpoint security profile	Docs	Created	Assigned
Basic Autopilot profile 20220121_1001:11	Autopilot profile	Docs	Created	Assigned
Basic ESP 20220121_1001:11	Enrollment Status Page	Docs	Created	Assigned
Basic OneDrive Known Folder Move 20220121_1001:11	Administrative template	Docs	Created	Assigned
Basic Microsoft Edge app settings 20220121_1001:11	Administrative template	Docs	Created	Assigned
Basic compliance policy 20220121_1001:11	Compliance policy	Docs	Created	Assigned
Basic built-in app removal script 20220121_1001:11	Script	Docs	Created	Assigned
Basic update ring 20220121_1001:11	Update rings for Windows 10 and later	Docs	Created	Assigned

What can I do next?

- Add devices to the group you configured**
Add your pre-registered Autopilot devices or other existing devices to the group you configured. For existing devices, we recommend removing other profiles and apps and resetting them, so they start fresh with just cloud config applied.
- Deploy essential line-of-business apps and configurations**
We recommend keeping additional essential configurations to a minimum, including the number of line-of-business apps you deploy on top of cloud config. This helps keep device management and troubleshooting simpler.
- Deploy essentials that users might need to access work or school resources**
Be sure to configure the certificates, VPN profiles, Wi-Fi profiles, and desktop/app virtualization clients that enable access to your organization's resources.

You have now successfully deployed Windows in Cloud Configuration for your endpoints!