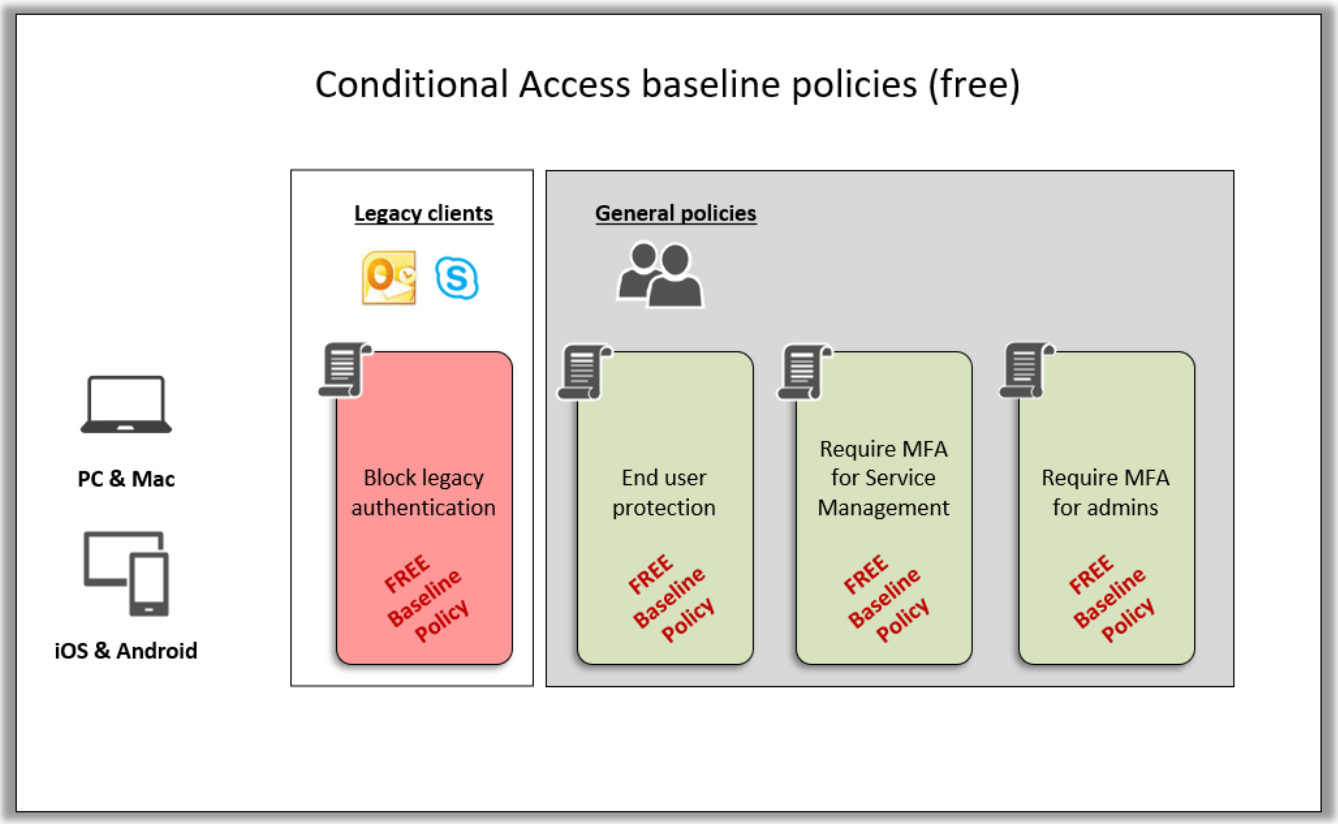
Recommended Conditional Access policies for Microsoft 365

By Alex Fields, ITProMentor.com
Updated: 08/15/2019

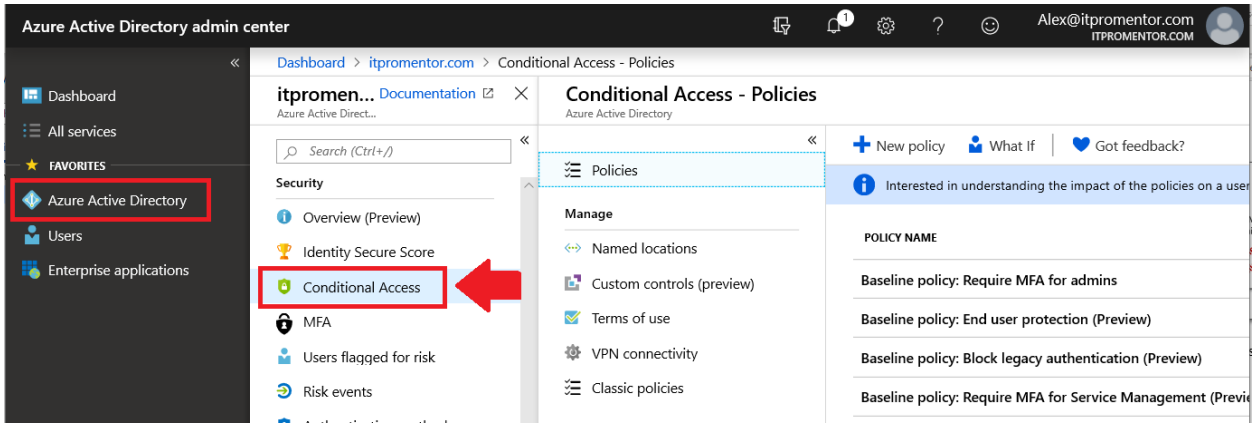
Conditional Access enables you to either block, allow or limit access under different circumstances that you define via policy. This document describes in detail setting up the policies described in [this resource].

Baseline Conditional Access policies

There are four baseline policies (still in preview at the time of this writing) which are included with every subscription. In the diagram below, green policies allow access with stipulations (e.g. multi-factor authentication). Policies in red block access.



Organizations can get their feet wet by starting with the free baseline policies. Find them by navigating to the Azure AD admin center. Locate **Azure Active Directory > Conditional access**.



In the following table, we list each of the free baseline policies, describe their impact and indicate some additional considerations, e.g. what you can do to mitigate the policy's impact (if applicable).

Conditional access policy	Description	Impact	Considerations
Require MFA for Service Management	Access to Azure services require MFA	Azure Portal, Azure PowerShell, etc. will require MFA	Exclude one break glass admin account*
Require MFA for admins	Admin accounts are required to use MFA	Admins must register for MFA	Exclude one break glass admin account*
End user protection	Require MFA for risky sign-ins; require password reset for leaked credentials	Users must register for MFA	No exclusions**
Block legacy authentication	Block legacy apps & protocols such as IMAP, POP and SMTP	Blocks basic auth (Outlook 2010 and any other legacy apps)	No exclusions**

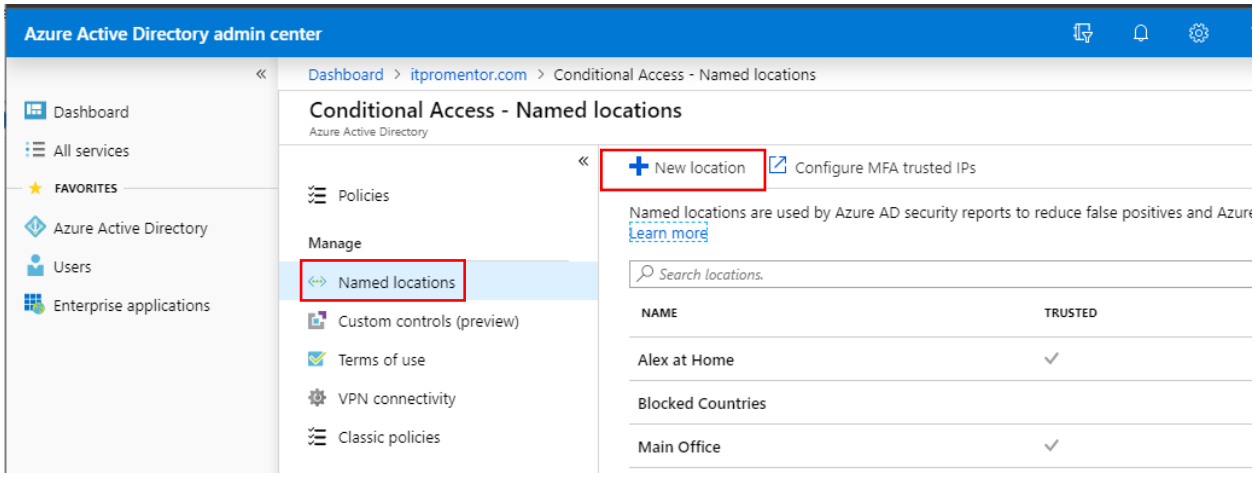
At the time of this writing, just know that the free baseline policies are still in "preview" which means that there could still be changes made to them before they are finalized. Also, Microsoft support may not be able to assist with preview items (though I find they usually make a best effort).

**It is recommended to exclude at least one global admin account (referred to as an emergency access or "break glass" account) from all conditional access policies. This account should be protected with a very long (e.g. 100 character) randomly generated password.*

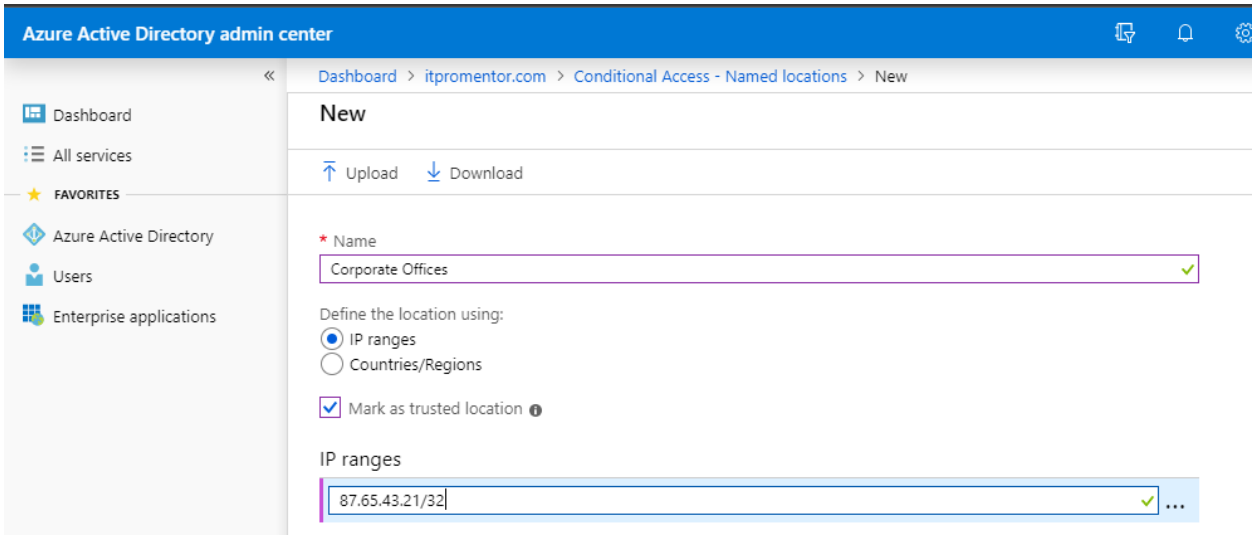
***At this time, it is not possible to exclude accounts from either **End user protection** or **Block legacy authentication**. If you have accounts that must continue to use basic authentication, then these policies are not for you!*

Define trusted locations

Before building any custom policies, go to **Azure Active Directory > Conditional access** and choose **Named locations**. Click **New location**.



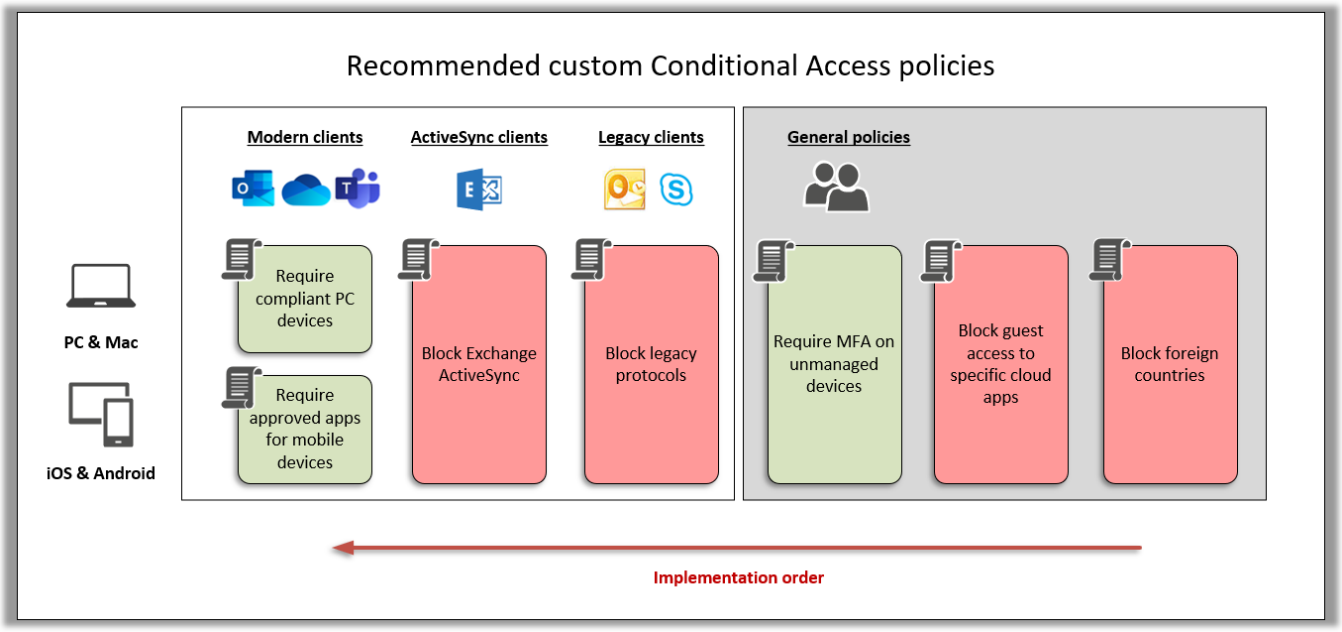
Fill out a **Name** such as *Corporate Offices*, choose **IP ranges** and **Mark as trusted location**. Type the CIDR IP address(es). These must be external addresses (not internal). Click **Create** to finish.



These named locations can be excluded from custom conditional access policies as needed. For example, you could choose *not* to require MFA from trusted locations.

Recommended custom Conditional Access policies

In addition to the baseline policies, there are several recommended custom Conditional Access policies.



Before we build the policies, we will again describe them along with their impacts and other considerations, as we did with the baseline policies.

Conditional access policy	Description	Impact	Considerations
Block foreign countries	Blocks sign-on from other countries	Traveling internationally can be difficult	Exclude an "International travelers" group
Block guest access	Blocks external user access to apps except SharePoint and Teams	Guests will not be able to sign-in to apps other than SharePoint and Teams	Optionally pair this with Require MFA access control
Require MFA for untrusted devices and locations	Prompts users for MFA (untrusted devices or locations only)	Device enrollment and web browser access requires MFA	Exclude service accounts that cannot do MFA
Block legacy protocols	Block legacy apps & protocols such as IMAP, POP and SMTP	Blocks basic auth (Outlook 2010 and any other legacy apps)	Exclude service accounts that require basic auth
Block ActiveSync clients	Blocks Exchange ActiveSync clients	Users should use the modern Outlook app	Alert users to this change before rolling it out
Require approved apps for mobile devices	This policy enables BYOD and blocks native mail applications	Users must use modern apps like Outlook and OneDrive	Alert users to this change before rolling it out
Require compliant devices	Blocks PC's & Mac's that are not compliant with Intune policies	Users must enroll their PC and/or Mac devices or lose access	Enroll using the Company Portal app before enabling

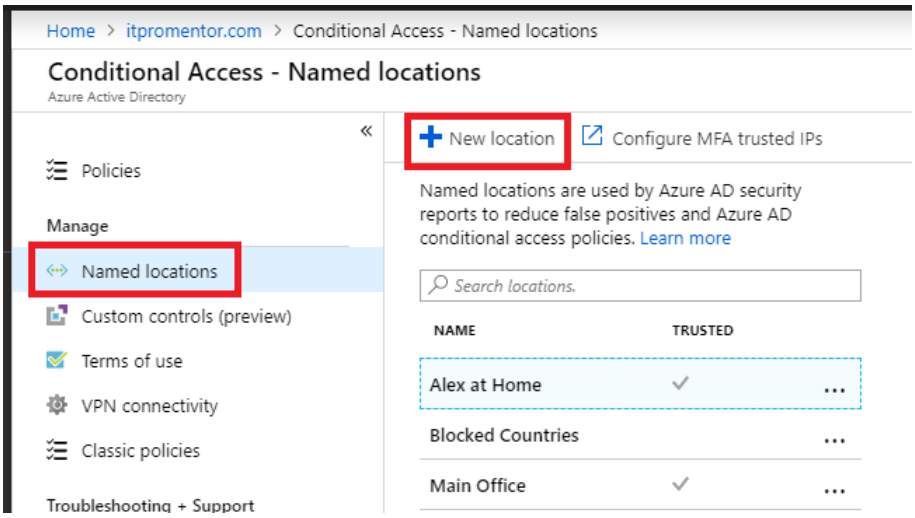
The following table lists all of the settings contained within the recommended custom policies. We will also provide screen shots to assist with the creation of each of these policies.

Conditional access policy	Assignments	Conditions	Access Control
Block foreign countries	**Users:** All users **Apps:** All cloud apps	**Location:** Include All locations, Exclude the named location for Allowed countries	**Block access**
Block guest access	**Users:** All users **Apps:** Include All cloud apps, Exclude Exchange and SharePoint	**None**	**Block access**
Require MFA for untrusted devices and locations	**Users**: All users **Apps**: All cloud apps	**Location:** Exclude Trusted locations **Device state**: Exclude Device marked as compliant	**Grant access:** Require multi-factor authentication
Block legacy protocols	**Users**: All users **Apps**: All cloud apps	**Client apps**: Mobile apps and desktop clients > Other clients	**Block access**
Block Exchange ActiveSync	**Users**: All users **Apps**: Exchange Online	**Client apps**: Mobile apps and desktop clients > Exchange ActiveSync clients	**Block access**
Require approved apps for mobile devices	**Users**: All users **Apps**: All cloud apps	**Device platforms**: iOS and Android **Client apps**: Mobile apps and desktop clients > Modern authentication clients	**Grant access:** Require approved client app
Require compliant PC devices	**Users**: All users **Apps**: All cloud apps **Excluded apps**: Intune Enrollment	**Device platforms**: Windows and macOS **Client apps**: Mobile apps and desktop clients > Modern authentication clients	**Grant access:** Require device to be marked as compliant

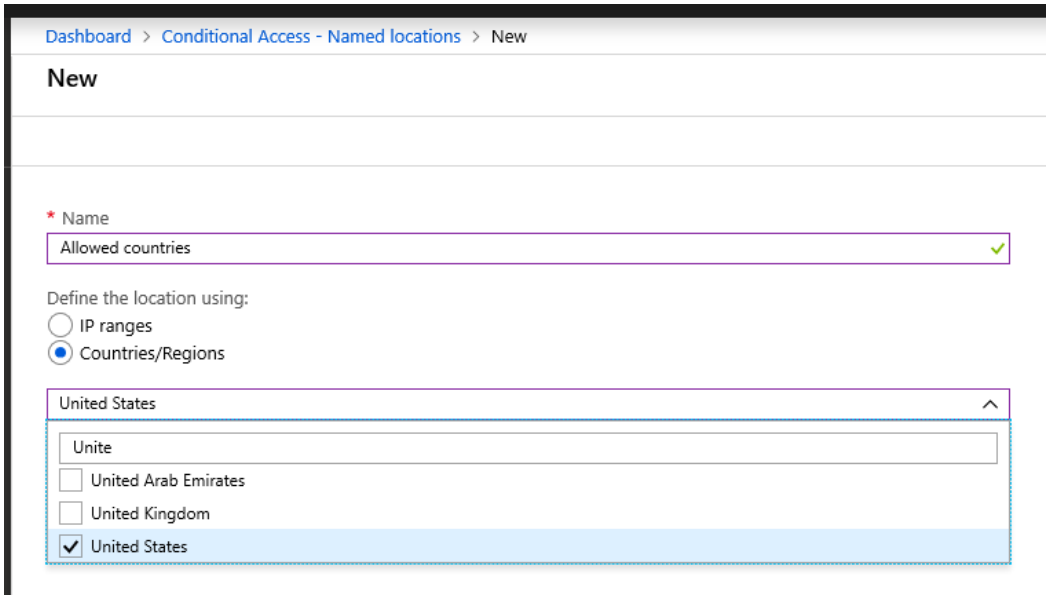
Block foreign countries

This policy is used to block sign-in from foreign countries. Note, this does not prevent users from communicating or doing business with those other countries—only authentication from those locations.

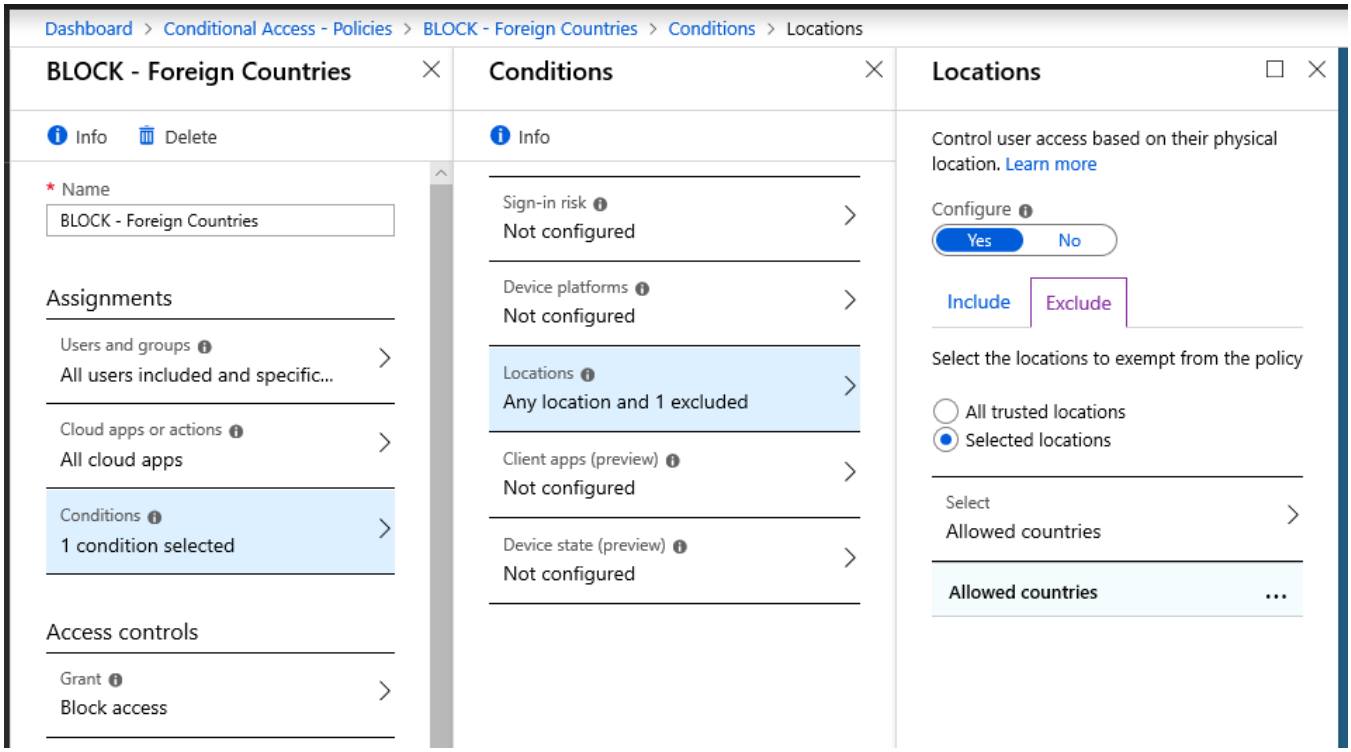
Before creating the policy, navigate from **Conditional access** to **Named locations**. Create a **New location**.



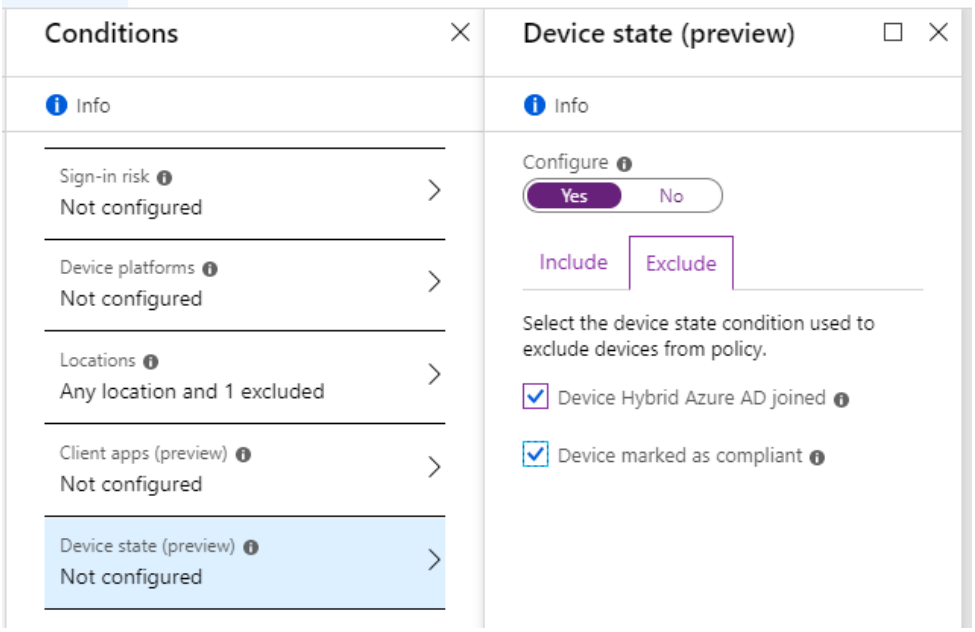
Name the location **Allowed countries**. Pick the **Countries/Regions** option. You can then filter this list by any country or countries you wish to exclude from the Block policy. For example, I live in the United States, and let's say my company also has offices in Canada. Then I might only select those two countries.



Create the named location. Now return to **Policies**. Create and assign the policy to **All users** and **All cloud apps**, excluding your "break glass" admin account. Under **Conditions**, configure **Locations** and use the **Exclude** tab to choose **Allowed countries**. Under **Access controls**, choose **Block access**.

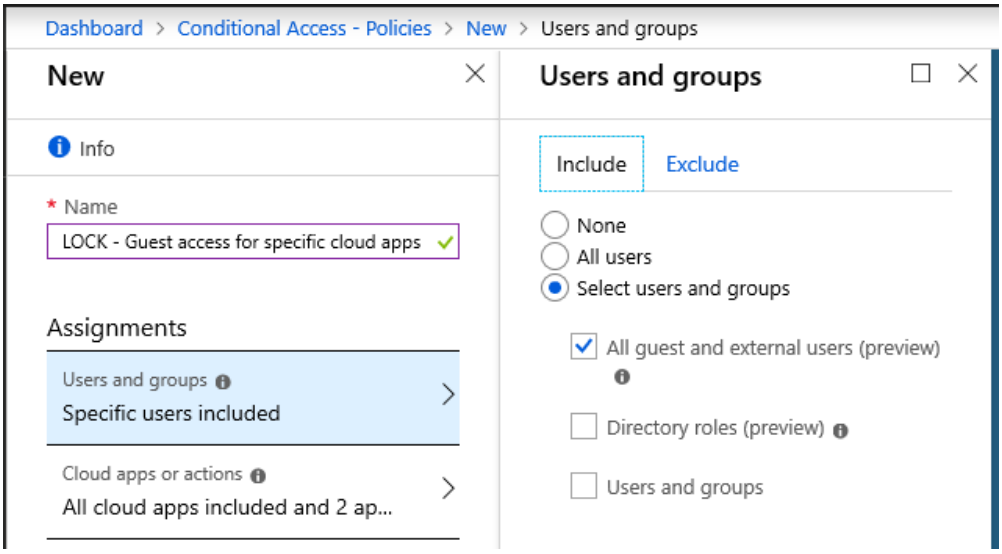


Optionally, you can also exclude managed devices so that users who are traveling abroad can still use known devices to access their resources. Use the **Device state** condition, choose the **Exclude** tab and select both check boxes to exclude managed devices.

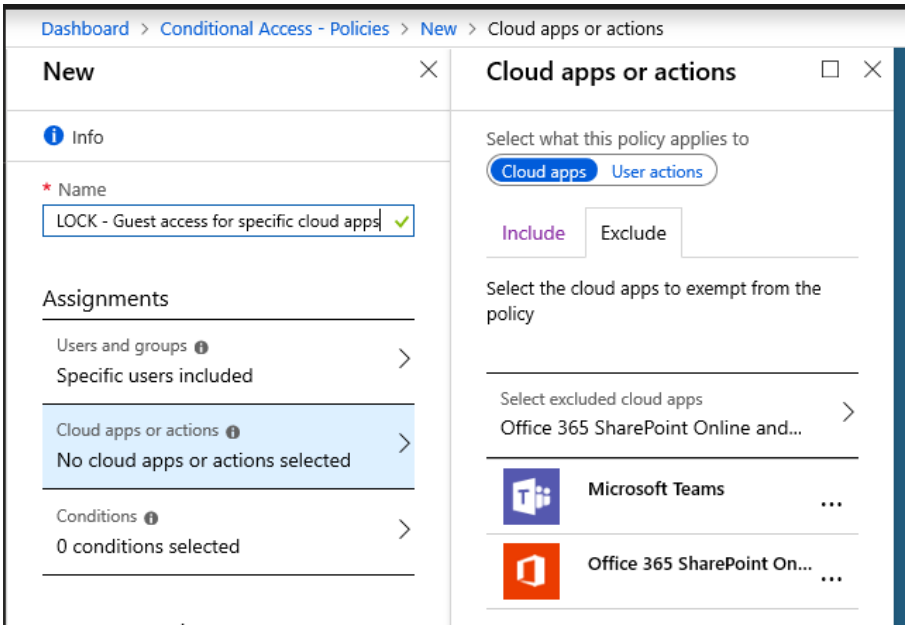


Block guest access

This policy will block guest access to apps other than Teams and SharePoint Online. Under **Assignments** pick **Select users and groups > All guests and external users**. **Create** and enable the policy.



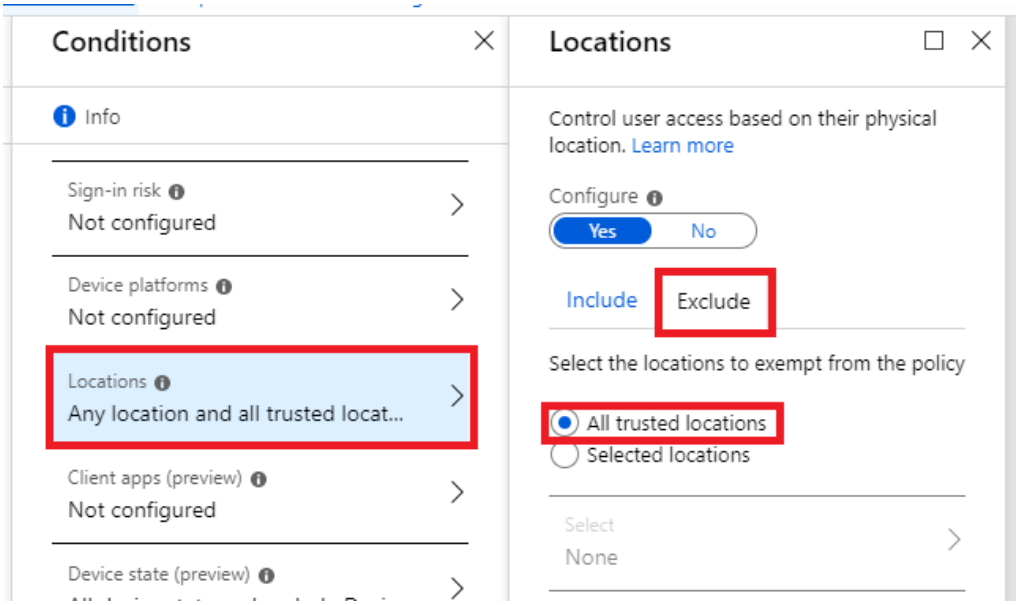
Under **Cloud apps or actions**, *Include* **All cloud apps**, but use the *Exclude* tab to leave out **Microsoft Teams** and **Office 365 SharePoint Online**. Choose **Block access** as your Access control. **Create** and enable the policy.



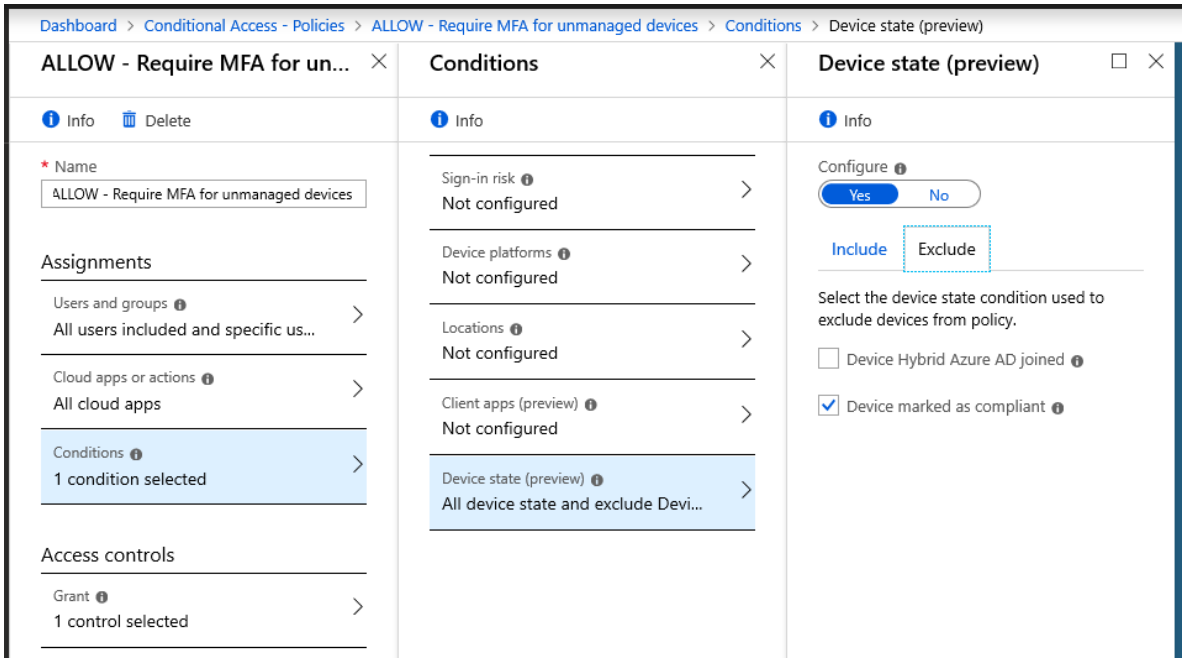
Require MFA for untrusted devices and locations

This policy will require users to provide MFA for any sign-in on an unmanaged device. That means MFA is always required for both Intune enrollment, and web access. Create a new policy and assign **All users** (excluding your "break glass" admin account). Choose **All cloud apps**.

Under **Conditions > Locations**, include **Any location**, but also choose **Exclude** > **All trusted locations**.



Also from **Conditions**, choose **Device state**, configure the policy, on the **Exclude** tab pick **Device marked as compliant**. That means Intune managed devices are not subject to this policy.

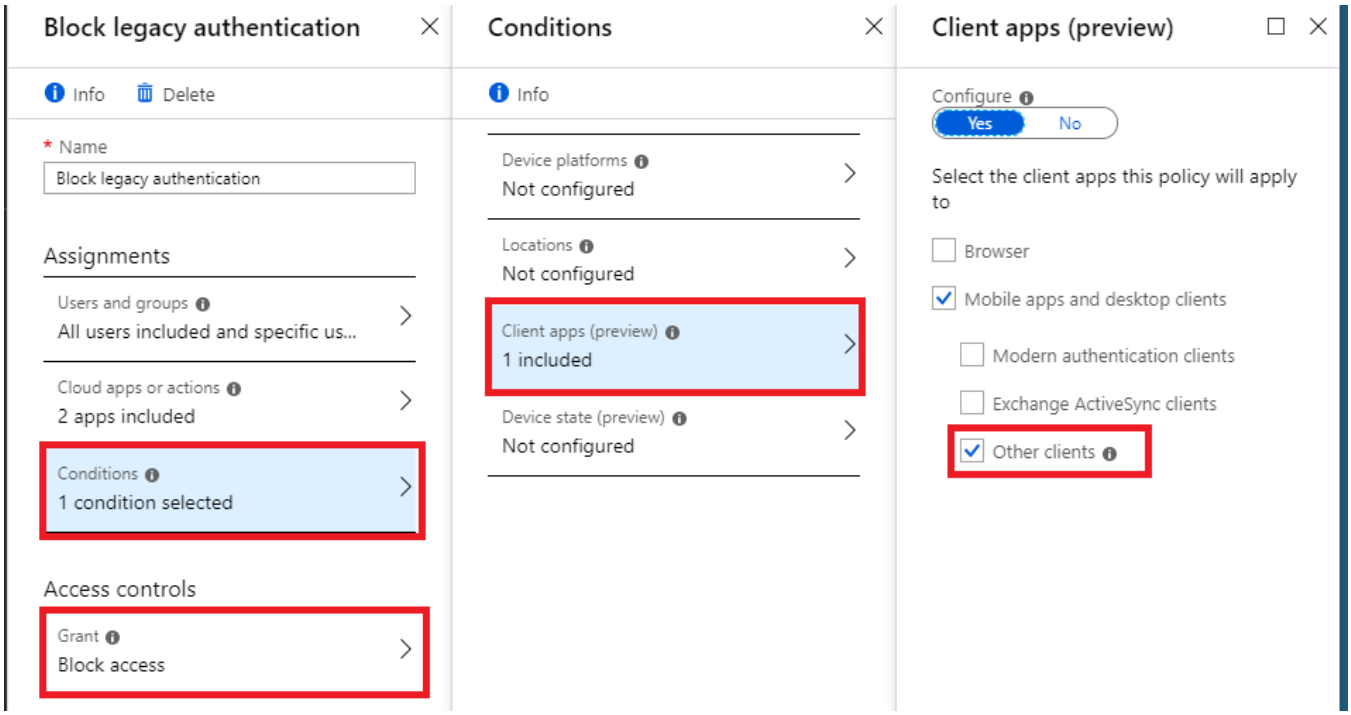


Last, navigate to **Access controls**, choose **Grant access** and **Require multi-factor authentication**.

Block legacy protocols

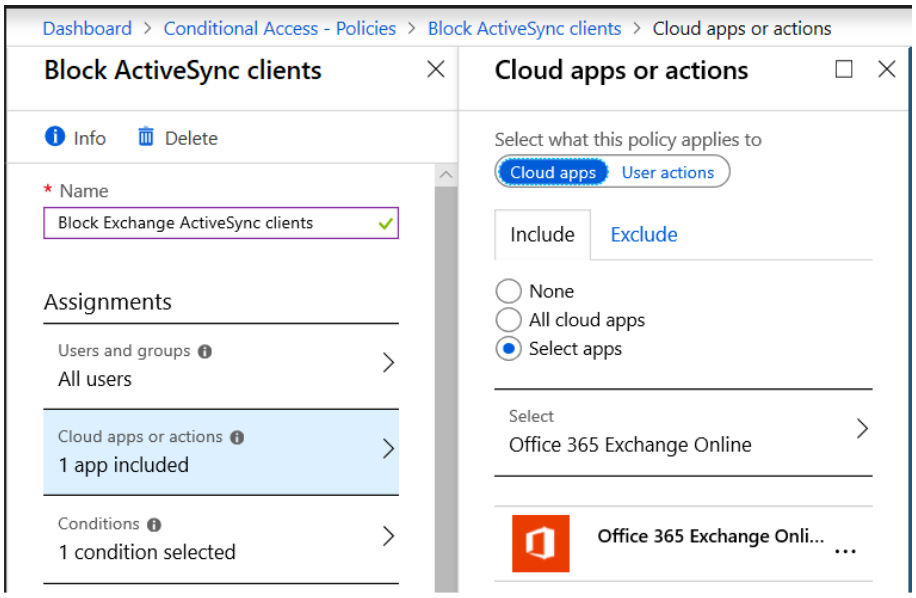
Even though we have a baseline policy that does this for you already, you may still consider creating a custom policy. Especially if you want to implement this setting while making exclusions for service accounts and/or trusted locations/applications. A custom policy will therefore give you more granular control.

- Create and name a new policy. Choose **All users** and set any excluded users from the policy.
- **Cloud apps:** pick apps to protect for example **Office 365 Exchange Online** and **SharePoint Online**.
- **Conditions:** pick **Client apps > Mobile apps and desktop clients > Other clients**. Clear all other options.
- **Access controls**: choose **Block access**.

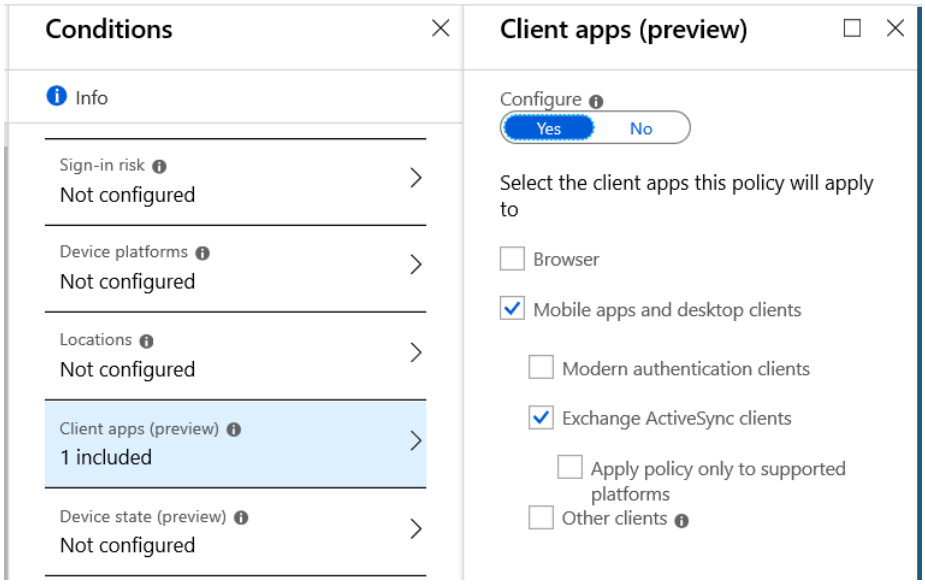


Block ActiveSync clients

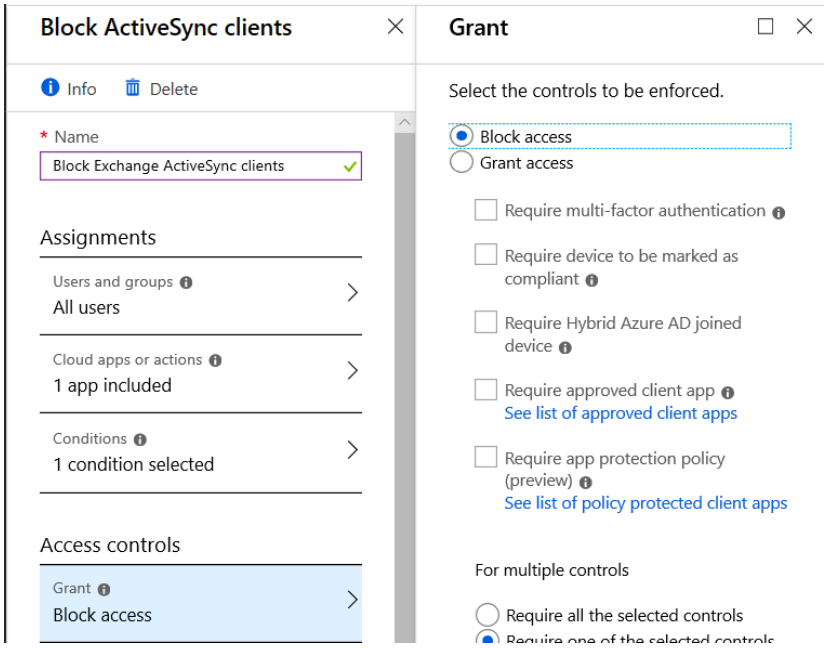
With Microsoft 365, it is recommended to use modern clients such as Outlook, which also support application protection policies (MAM), so ActiveSync clients are not necessary. Target **All users** and under **Cloud apps or actions** include only **Office 365 Exchange Online**. EAS clients only pertain to Exchange Online.



Next select **Conditions > Client apps**. Choose **Mobile apps and desktop clients** and **Exchange ActiveSync clients**.



Last select **Access controls > Block access**.

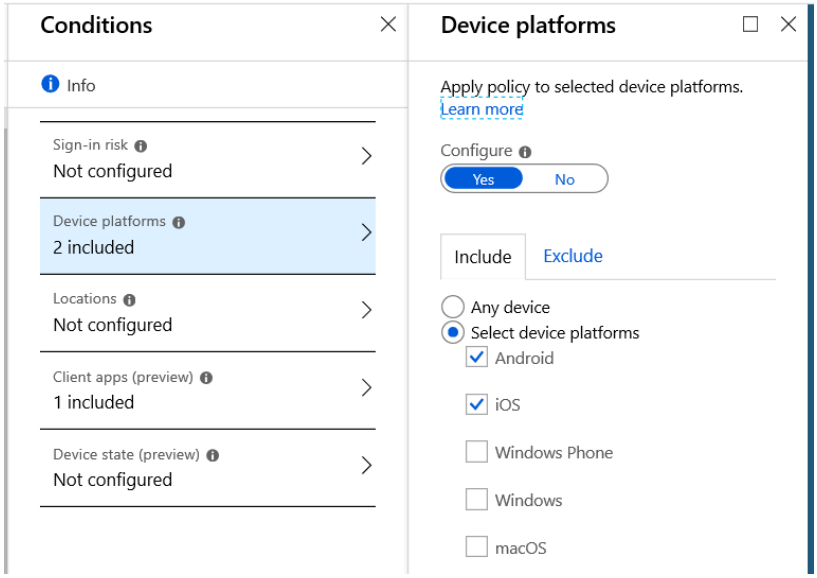


<u>Note</u>: Microsoft's documentation indicates that you should pick Grant access with the option to Require approved client app, but technically that control is only supported for mobile devices (iOS and Android). Therefore, just Block access here.

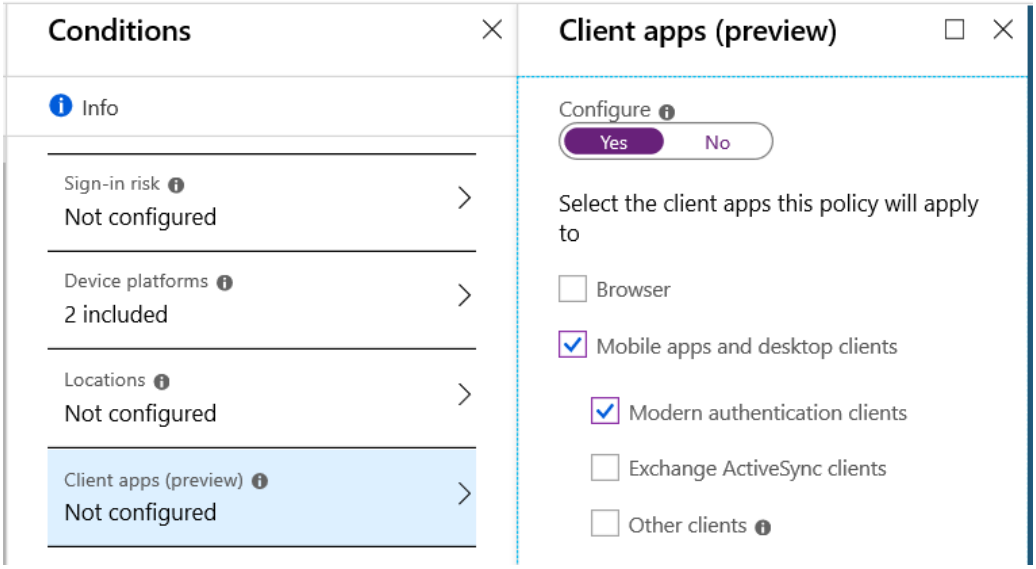
Require approved apps for mobile devices (iOS & Android)

This policy is best when combined with App protection (MAM) policies for both iOS and Android, which allow you to control access to the client application (e.g. PIN code, fingerprint, etc.) as well as to restrict the ability to copy/paste and save data from the managed applications into other specified apps and locations.

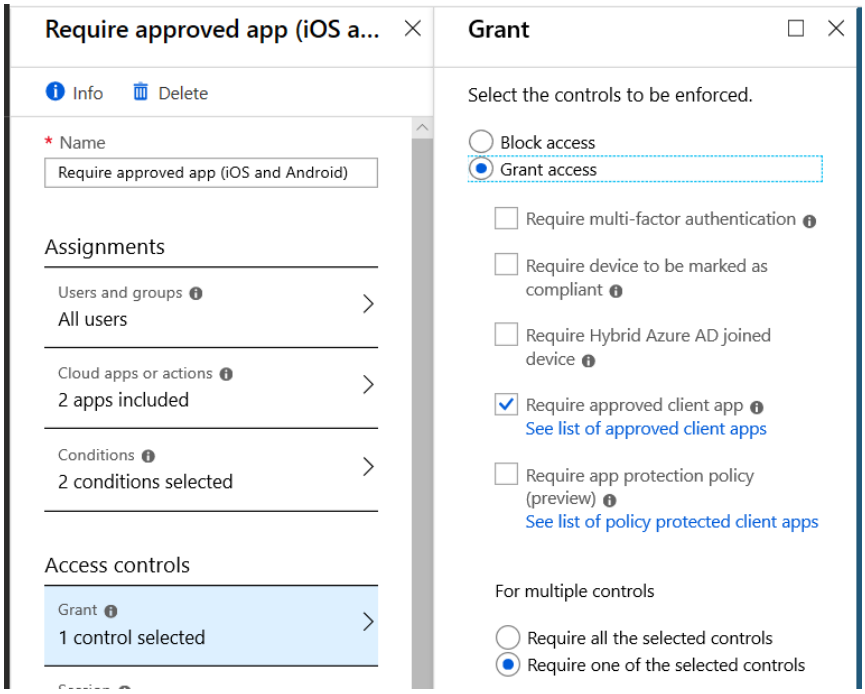
Create the policy, target **All users** and under **Cloud apps or actions** add **All cloud apps**. Under **Conditions > Device platforms**, choose only **Android** and **iOS**. The access control "*Require approved client app*" only applies to these mobile platforms.



Next under **Clients apps** pick only **Mobile and desktop clients** & **Modern authentication clients**. All other client types are being blocked by other policies.



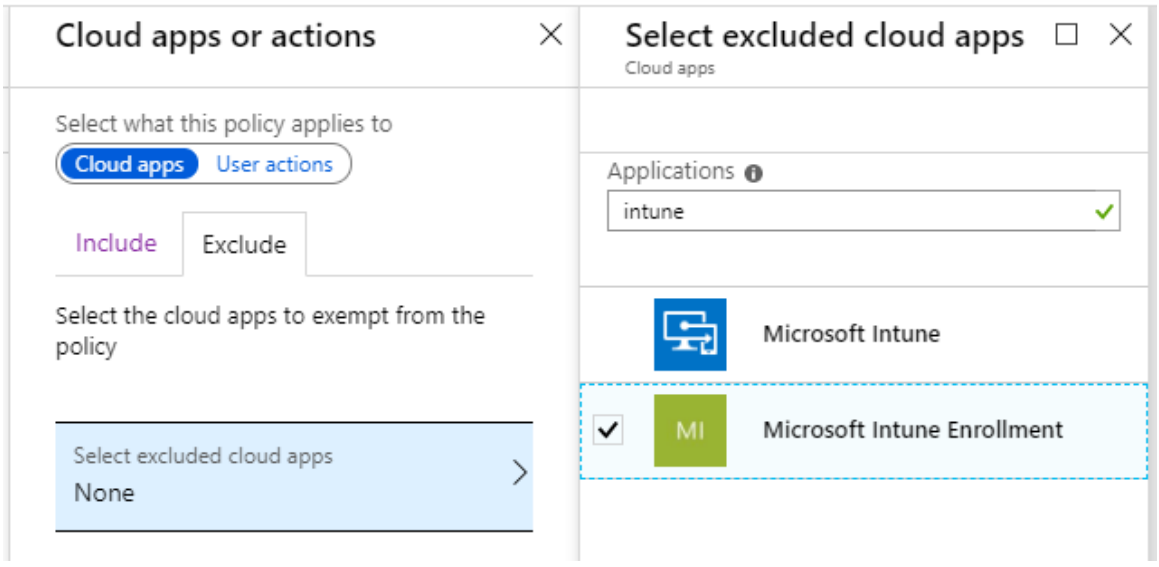
Finally, go to **Access controls** and choose **Grant access** and **Require approved client app**. This access control only applies to iOS and Android devices. **Save** the policy.



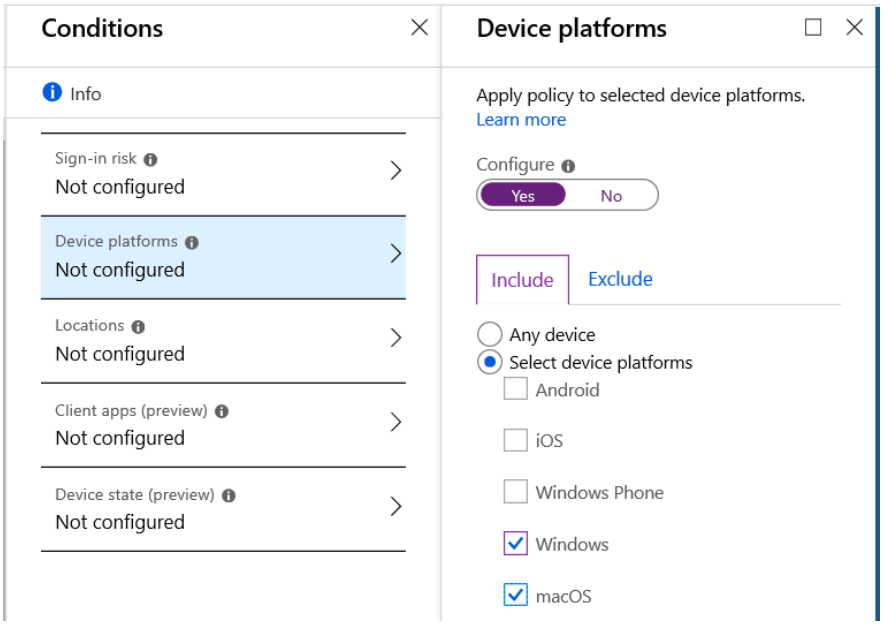
Require compliant PC devices (PC & Mac)

This policy assumes that you have already created a corresponding Compliance policy for each type of device within Intune/Device management. Assign your compliance policies and enroll end-user devices first.

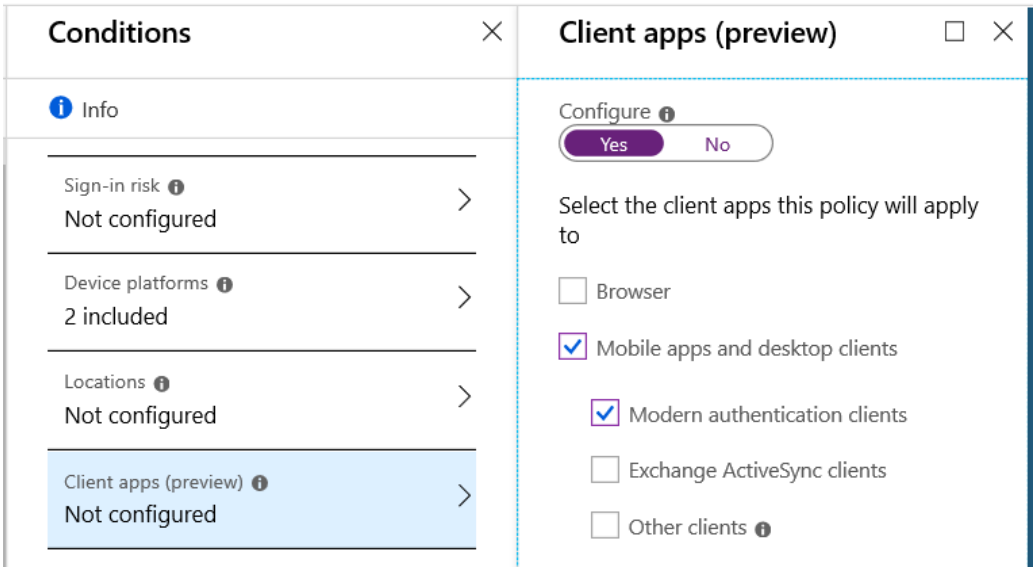
Create the policy, targeting **All users** and under **Cloud apps or actions**, select **All cloud apps**. However, on the **Exclude** tab, choose **Microsoft Intune Enrollment.**



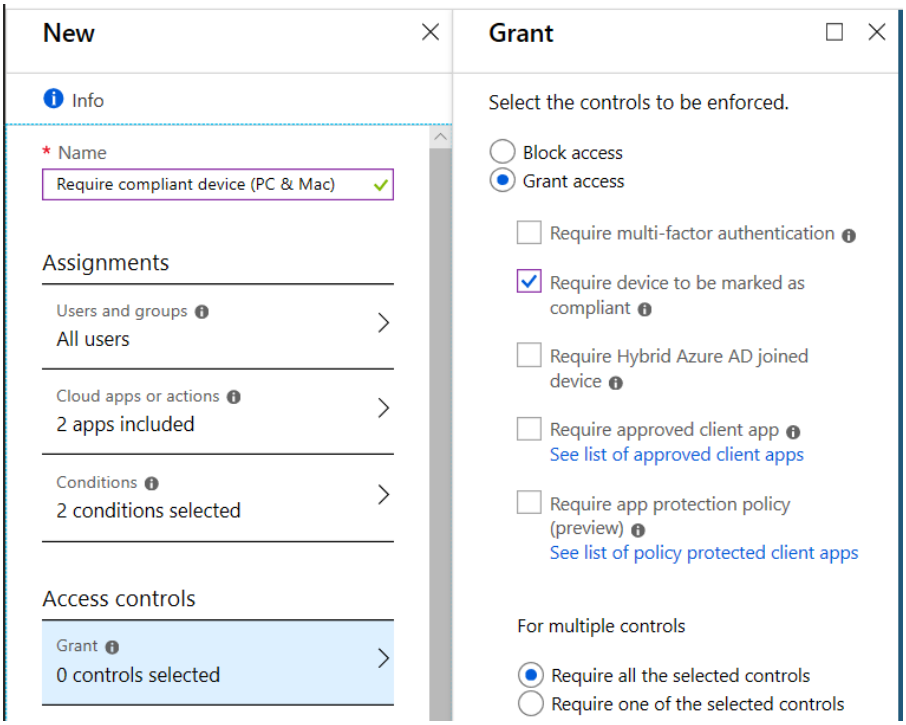
Next pick **Conditions > Device platforms**, choose Windows and macOS.



Next under **Clients apps** pick only **Mobile and desktop clients** and **Modern authentication clients**. All other client types are being blocked by other policies.

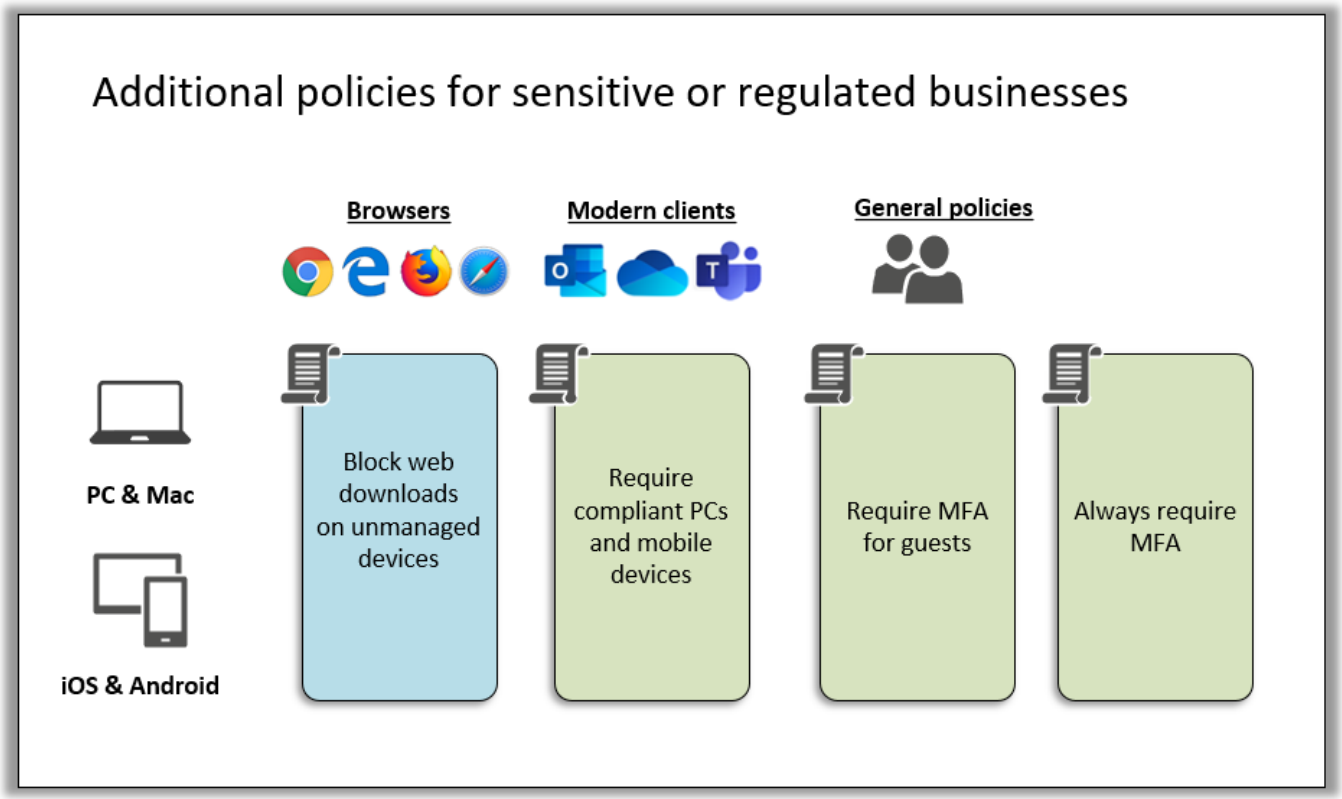


Proceed to select **Access controls > Grant access**, then pick only **Require device to be marked as compliant**. **Save** the policy.



Recommended Conditional Access Policies for highly sensitive or regulated businesses

The policy set for sensitive or highly regulated businesses will contain a few additional policies that enforce more restrictive access controls. Let's take a look, the blue policy is a session-based control:



Before you create and turn them on, we will describe each policy's impacts and considerations, again in a table as we did before.

Conditional access policy	Description	Impact	Considerations
Always require MFA	Multi-factor challenge required for access	Users required to perform MFA more frequently	Alert users to this change before rolling it out
Require MFA for guests	Multi-factor challenge required for guest access	Guests required to perform MFA	Alert users to this change before rolling it out
Block access from apps on unmanaged devices	Blocks devices that are not compliant with Intune policies	Users must enroll all devices or lose access	Enroll using the Company Portal app before enabling
Block downloads on unmanaged devices	Web downloads from SharePoint, OneDrive and Outlook are not possible from unmanaged devices	Users cannot download attachments or files over the web on an unmanaged device	Alert users to this change before rolling it out
Block unsupported devices	Blocks unwanted device platforms	Users cannot connect unless they use a device platform that is explicitly allowed	Communicate this change to the users in advance.

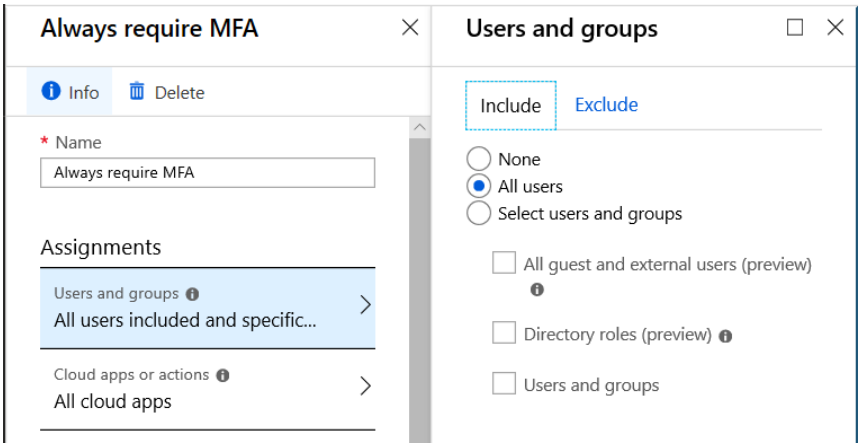
The following table describes how to build out the policies.

Conditional access policy	Assignments	Conditions	Access Control
Always require MFA	**Users**: All users **Apps**: All cloud apps	**None**	**Grant access:** Require multi-factor authentication
Require MFA for guests	**Users**: All guest and external users **Apps**: All cloud apps	**None**	**Grant access:** Require multi-factor authentication
Require compliant PCs and mobile devices	**Users**: All users **Apps**: All cloud apps **Excluded apps**: Intune Enrollment	**Client apps**: Modern authentication clients	**Grant access:** Require device to be marked as compliant
Block downloads on unmanaged devices	**Users**: All users **Apps**: Exchange Online, SharePoint Online	**Client apps:** Browser	**Session:** Use app enforced restrictions
Block unsupported devices	**Users:** All users **Apps:** All cloud apps	**Device platforms:** Any **Exclude**: choose specific device platforms that are supported	**Block access**

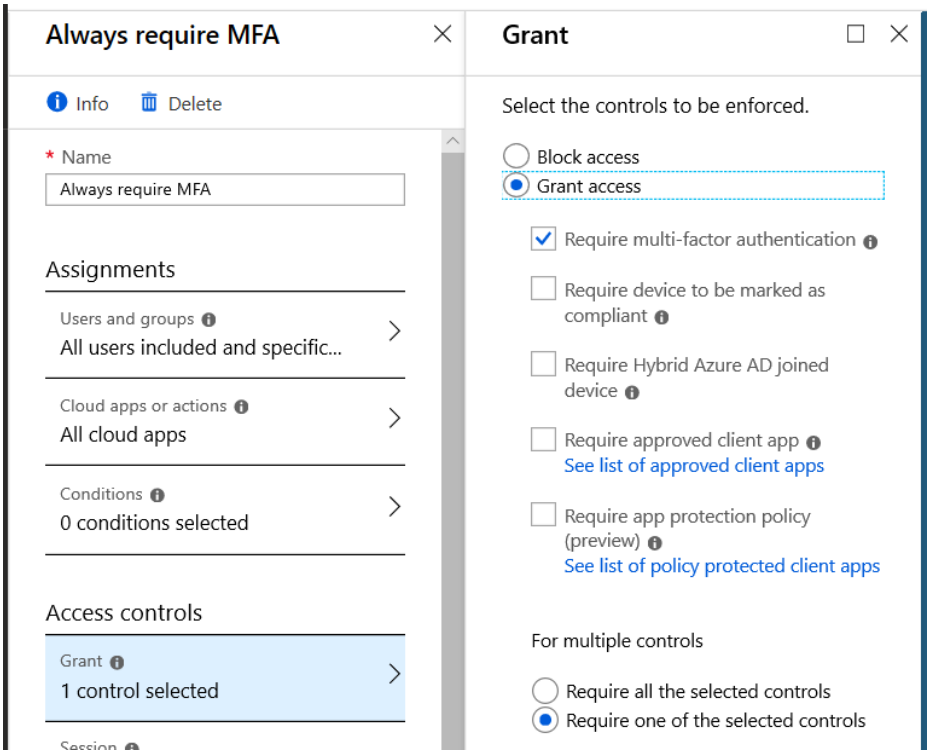
The following sections contain screenshots to assist with building these policies.

Always require MFA

Create a new policy, assign it to **All users** (exclude a "break glass" account) and **All cloud apps**.

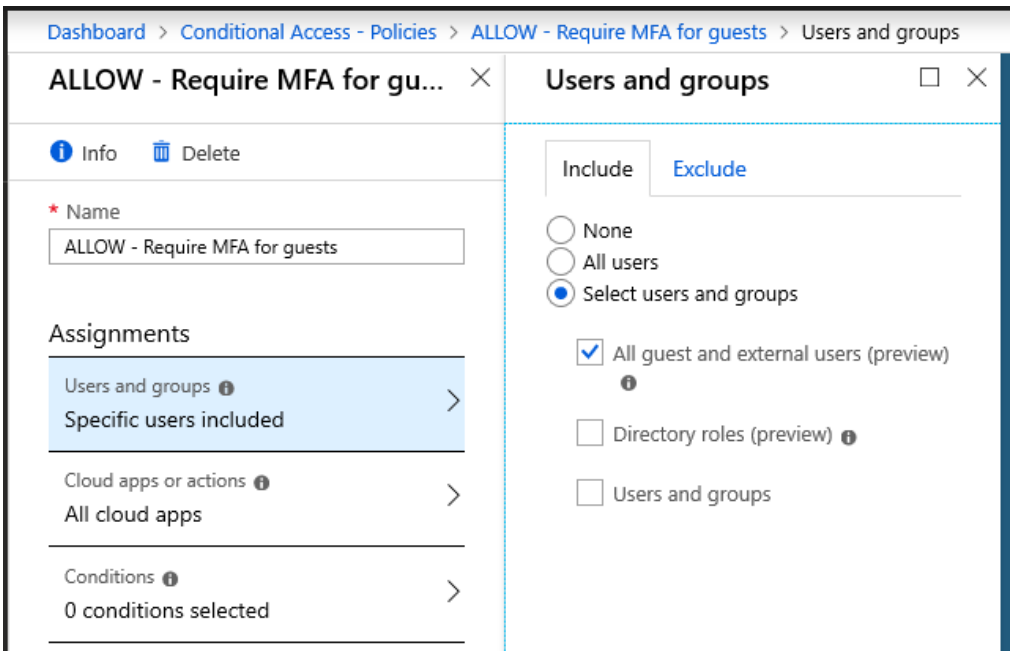


Do not select any conditions (we do not want to require MFA only under *certain* conditions but rather *any*). Therefore, move right into **Access controls**, choose **Grant access** and **Require multi-factor authentication**.



Require MFA for guest access

This policy will enforce MFA for guest and external users. **Under Assignments > Users and groups**, pick **Select users and groups > All guest and external users.** Next choose **Cloud apps or actions > All cloud apps**.

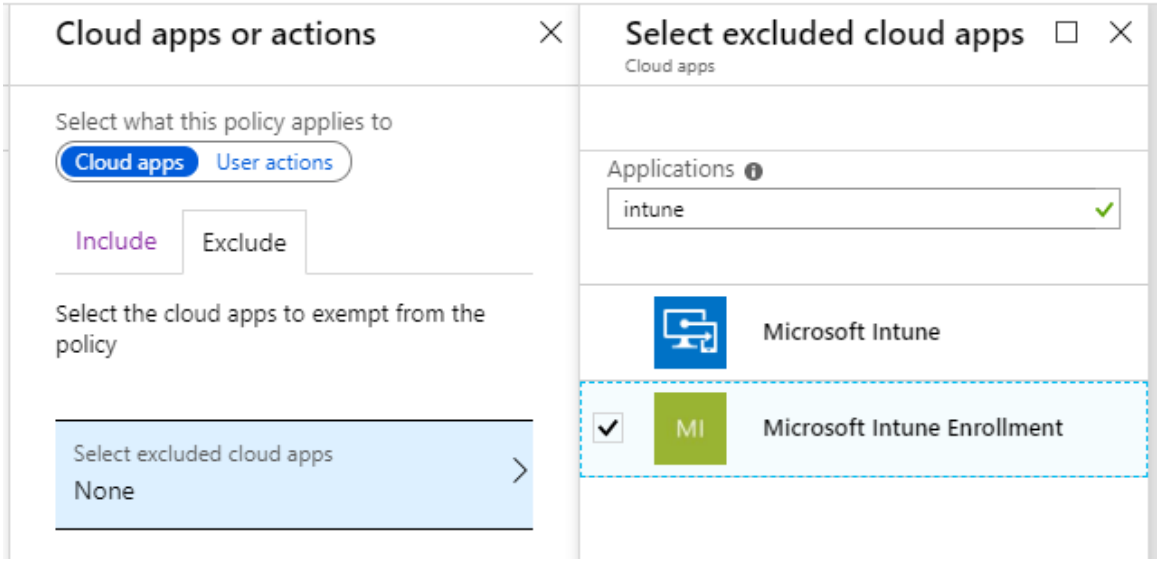


Last, skip all conditions again and enable the **Access control > Grant > Require multi-factor authentication**.

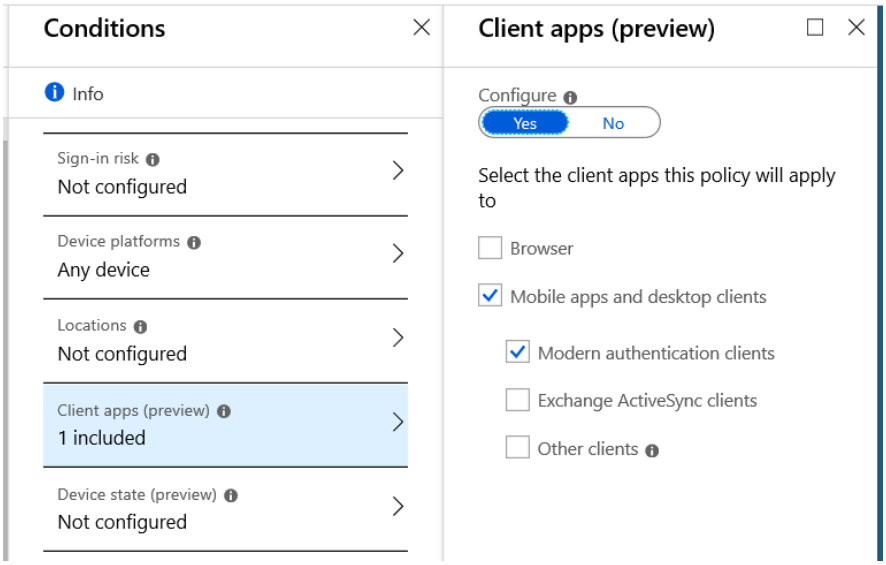
Require compliant PCs and mobile devices

This policy requires that devices be enrolled with Intune, meaning that device compliance policies must also be assigned, before enabling the corresponding conditional access policy.

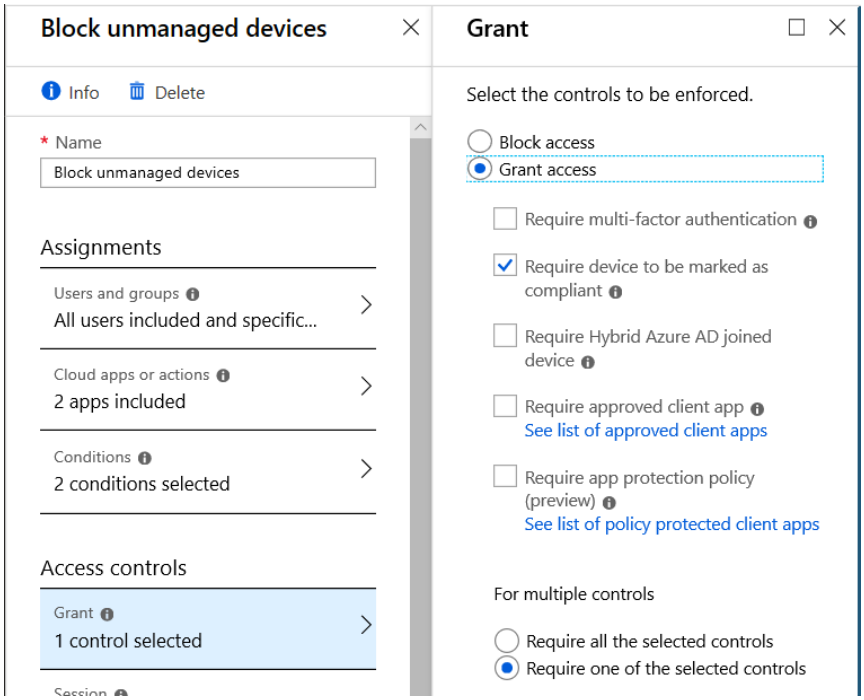
Create the new policy. Assign to **All users** and **All cloud apps**. Pick the **Exclude** tab, and choose **Microsoft Intune Enrollment**.



Under **Conditions**, specify **Client apps > Mobile apps and desktop clients** and **Modern authentication clients**.



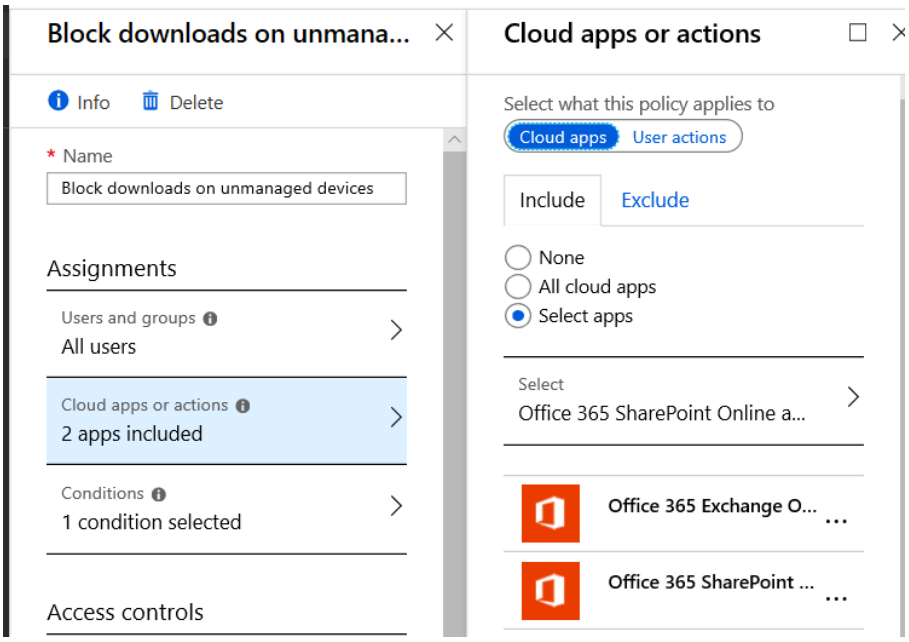
Last you must define: **Access controls > Grant access > Require device to be marked as compliant**.



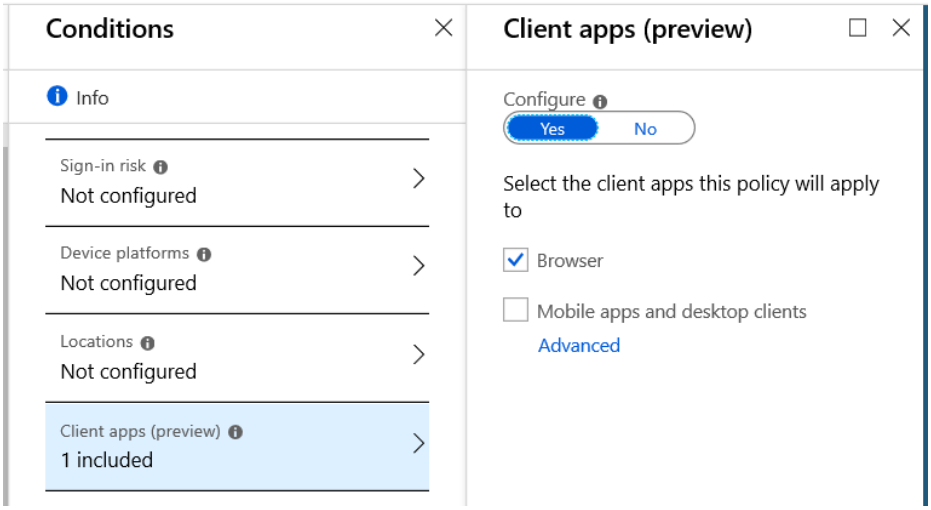
The effect of this policy is that unmanaged devices (of all types) are blocked from access; all devices must therefore be enrolled and compliant with Intune policy before connecting to resources. Do not enable this policy for the first time until all of your devices are enrolled.

Block downloads on unmanaged devices

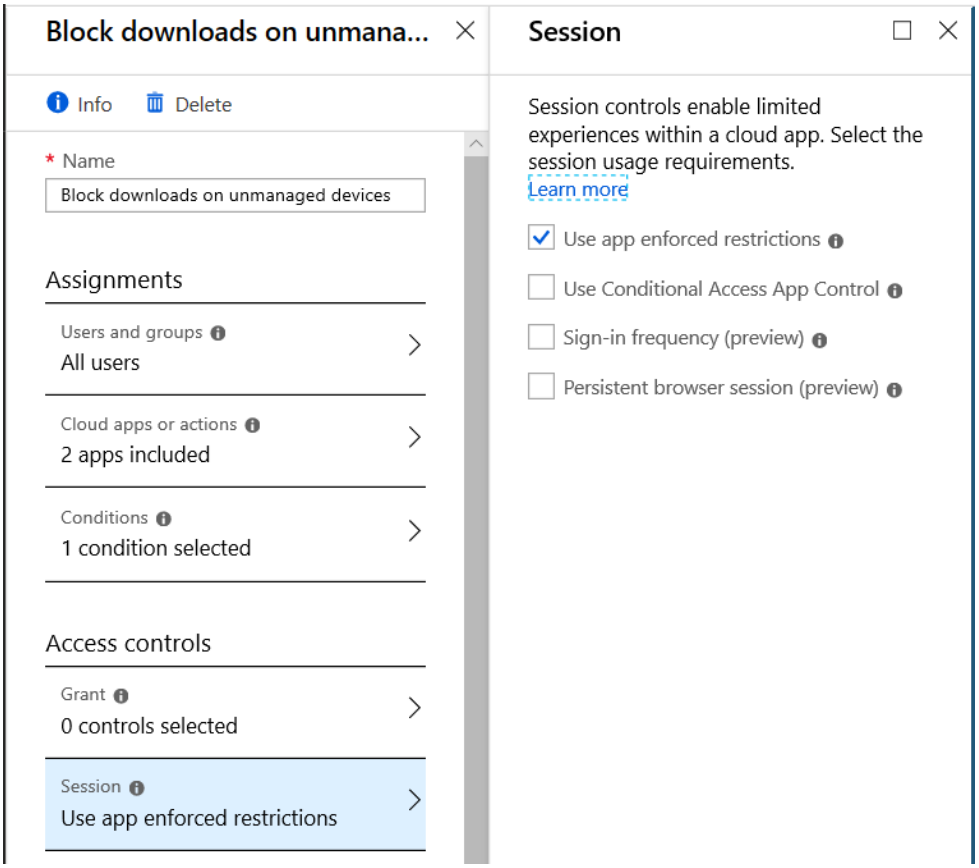
Create a new policy. Assign to **All users** and pick **Office 365 Exchange Online** and **Office 365 SharePoint Online**. Both of these cloud apps support the access control which will enforce app restrictions, limiting the browser session so that downloads are not possible from unmanaged devices.



Under conditions pick **Client app > Browser**.



Under **Access controls** pick **Session > Use app enforced restrictions** only.



You are not done implementing this policy. You will also need to enable these settings in Exchange Online and SharePoint Online.

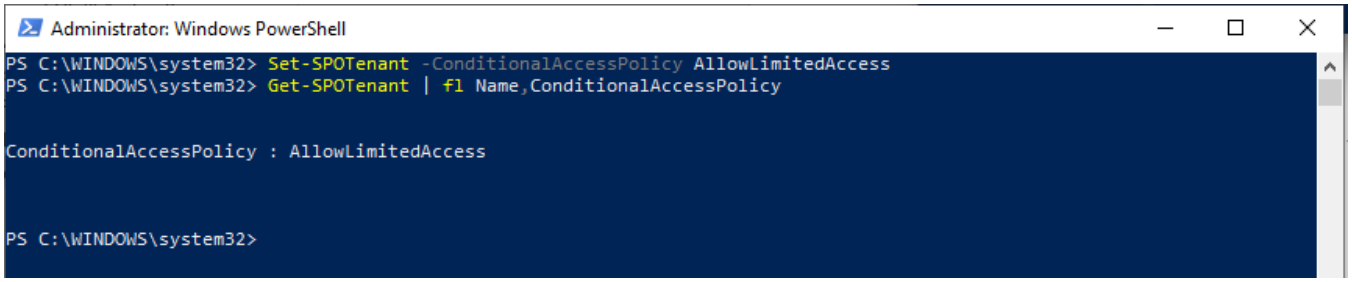
To enable for Exchange Online, connect to your tenant using the Exchange Online PowerShell module with MFA. Once connected, enable "ReadOnly" mode for Outlook on the Web:

```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -ConditionalAccessPolicy ReadOnly
```

```
PS C:\Users\alexf> Get-OwaMailboxPolicy | fl Name,ConditionalAccessPolicy

Name                    : OwaMailboxPolicy-Default
ConditionalAccessPolicy : Off



PS C:\Users\alexf> Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -ConditionalAccessPolicy ReadOnly
PS C:\Users\alexf>
```

To enable for SharePoint Online, connect to SharePoint Online Management Shell using MFA. Run:

```
Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess
```

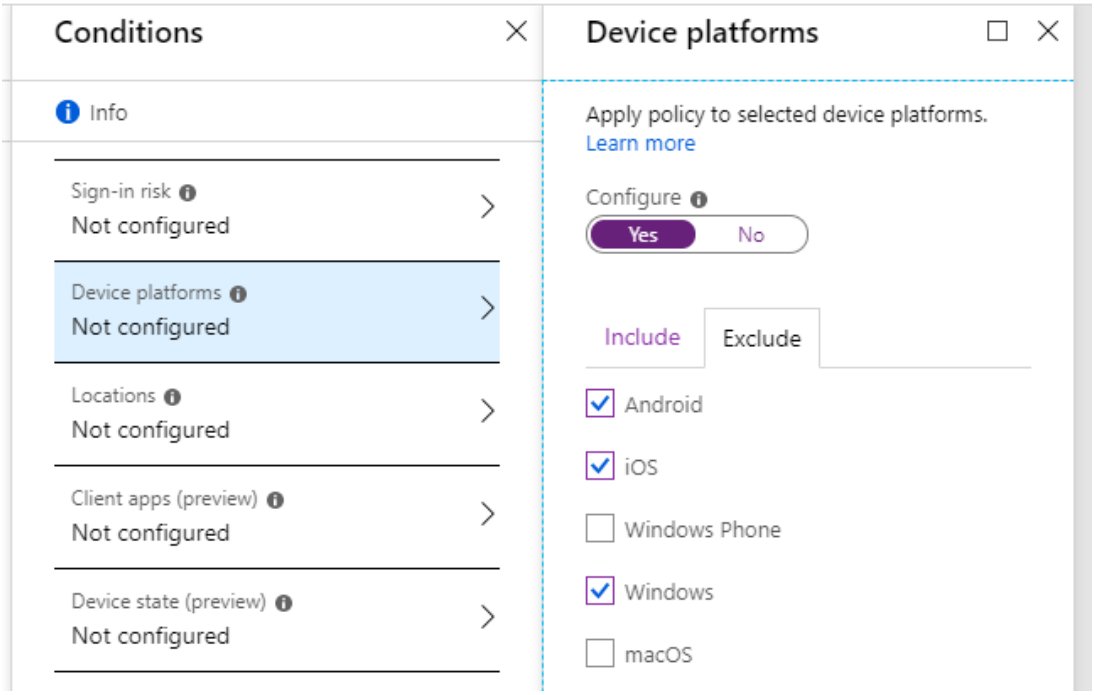


Note: this action will automatically create Conditional access policies labeled as [SharePoint admin center]. You can safely disable or even delete these policies, as they will be redundant to what we have already created.

Block unsupported devices

This policy will block devices that you do not specifically intend to support in your environment. For example, if you do not expect or do not want to support other platforms like Linux, Chromebook, and so forth, then you can use this policy to block non-supported device platforms from connecting to your services.

Create a new policy, name it and target **All users**, and **All cloud apps**. Under **Conditions**, pick **Device platforms**, and pick **Any device**, but then also select the **Exclude** tab and choose any platforms that you do intend to support, such as Windows, iOS, Android, etc.



Finally, under **Access controls**, choose **Block access**.

This concludes guidance on the recommended conditional access policies.