

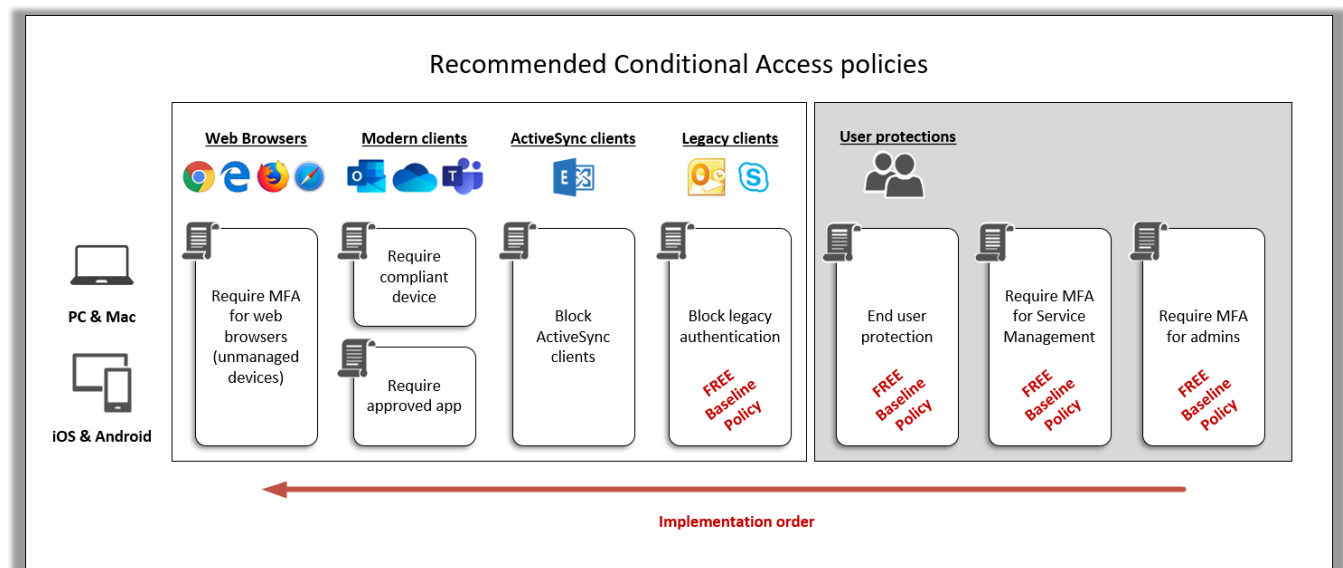
# Recommended Conditional Access policies for Microsoft 365 Business

By Alex Fields, ITProMentor.com

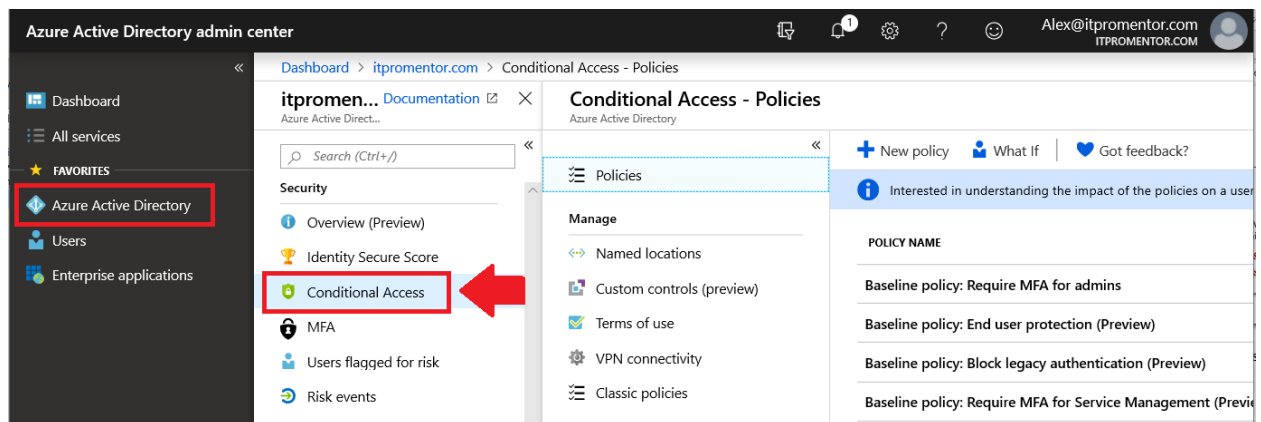
Microsoft 365 Business now includes a killer security control known as **Conditional Access**. This was previously available only with Azure AD Premium (part of Enterprise Mobility + Security). Separately, Microsoft also released “baseline” conditional access policies that are given free to all tenants, but with Microsoft 365 Business we can do a lot more.

## Baseline Conditional Access policies (for everyone)

There are several recommended policies, both baseline and custom-built, which are appropriate for *most* businesses that are just starting out in Microsoft 365.



Every organization 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
<b>Require MFA for Service Management</b>	Access to Azure services require MFA	Azure Portal, Azure PowerShell, etc. will require MFA	Exclude one break glass admin account*
<b>Require MFA for admins</b>	Admin accounts will be required to perform MFA	Admins must register for and perform MFA	Exclude one break glass admin account*
<b>End user protection</b>	Require MFA for risky sign-ins; require password reset for leaked credentials	Users must register for MFA	Exclude service accounts that cannot do MFA
<b>Block legacy authentication</b>	Block legacy apps & protocols such as IMAP, POP and SMTP	Blocks Outlook 2010 and any other legacy app relying on basic auth	Exclude service accounts that rely on IMAP, SMTP, etc.

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).

*Note: 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.*

### Recommended custom Conditional Access policies

The table below lists settings contained within the recommended custom policies, below. Following that we will provide screen shots to assist with the creation of each of these policies.

Conditional access policy	Assignments	Conditions	Access Control
<b>Block ActiveSync clients</b>	<b>Users:</b> All users <b>Apps:</b> Exchange Online	<b>Client apps:</b> Exchange ActiveSync clients	<b>Block access</b>
<b>Require compliant devices (PC &amp; Mac)</b>	<b>Users:</b> All users <b>Apps:</b> Exchange Online, SharePoint Online	<b>Device platforms:</b> Windows and macOS <b>Client apps:</b> Modern authentication clients	<b>Grant access:</b> Require device to be marked as compliant
<b>Require approved app (iOS &amp; Android)</b>	<b>Users:</b> All users <b>Apps:</b> Exchange Online, SharePoint Online	<b>Device platforms:</b> iOS and Android <b>Client apps:</b> Modern authentication clients	<b>Grant access:</b> Require approved client app
<b>Require MFA for web browsers (unmanaged devices)</b>	<b>Users:</b> All users <b>Apps:</b> All cloud apps	<b>Client apps:</b> Browser <b>Device state:</b> Exclude Device marked as compliant	<b>Grant access:</b> Require multi-factor authentication

## 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.

Dashboard > Conditional Access - Policies > Block ActiveSync clients > Cloud apps or actions

### Block ActiveSync clients

Info Delete

\* Name  
Block Exchange ActiveSync clients ✓

#### Assignments

Users and groups ⓘ  
All users >

Cloud apps or actions ⓘ  
1 app included >

Conditions ⓘ  
1 condition selected >

### Cloud apps or actions

Select what this policy applies to  
Cloud apps User actions

Include Exclude

☐ None  
☐ All cloud apps  
☒ Select apps

Select >  
Office 365 Exchange Online >

Office 365 Exchange Onli... ...

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

### Conditions

Info

Sign-in risk ⓘ  
Not configured >

Device platforms ⓘ  
Not configured >

Locations ⓘ  
Not configured >

Client apps (preview) ⓘ  
1 included >

Device state (preview) ⓘ  
Not configured >

### Client apps (preview)

Configure ⓘ  
Yes No

Select the client apps this policy will apply to

☐ Browser  
☒ Mobile apps and desktop clients  
☐ Modern authentication clients  
☒ Exchange ActiveSync clients  
☐ Apply policy only to supported platforms  
☐ Other clients ⓘ

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

**Block ActiveSync clients** [Close]

Info [Delete]

**Name**  
Block Exchange ActiveSync clients ✓

**Assignments**

Users and groups ⓘ  
All users >

Cloud apps or actions ⓘ  
1 app included >

Conditions ⓘ  
1 condition selected >

**Access controls**

Grant ⓘ  
Block access >

**Grant** [Close]

Select the controls to be enforced.

☒ Block access  
☐ Grant access

☐ Require multi-factor authentication ⓘ  
☐ Require device to be marked as compliant ⓘ  
☐ Require Hybrid Azure AD joined device ⓘ  
☐ Require approved client app ⓘ  
[See list of approved client apps](#)  
☐ Require app protection policy (preview) ⓘ  
[See list of policy protected client apps](#)

For multiple controls

☐ Require all the selected controls  
☒ Require one of the selected controls

***Note:** 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.*

You are done creating this policy.

### Require compliant 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 the apps you want to protect for example **Office 365 Exchange Online** and **Office 365 SharePoint Online**.

**New** × **Cloud apps or actions** □ ×

**Info**

\* Name  
Require compliant device (PC & Mac) ✓

**Assignments**

Users and groups ⓘ  
All users >

Cloud apps or actions ⓘ  
No cloud apps or actions sele... >

Conditions ⓘ  
0 conditions selected >

**Access controls**

Select what this policy applies to  
**Cloud apps** User actions

**Include** **Exclude**

☐ None  
☐ All cloud apps  
☒ Select apps

Select  
Office 365 SharePoint Online a... >

Office 365 Exchange O... ...  
 Office 365 SharePoint ... ...

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

**Conditions** × **Device platforms** □ ×

**Info**

Sign-in risk ⓘ  
Not configured >

Device platforms ⓘ  
Not configured >

Locations ⓘ  
Not configured >

Client apps (preview) ⓘ  
Not configured >

Device state (preview) ⓘ  
Not configured >

Apply policy to selected device platforms.  
[Learn more](#)

Configure ⓘ  
**Yes** No

**Include** **Exclude**

☐ Any device  
☒ Select device platforms  
☐ Android  
☐ iOS  
☐ Windows Phone  
☒ Windows  
☒ 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.

**Conditions** ×

**Client apps (preview)** □ ×

**Info**

Sign-in risk ⓘ  
Not configured >

Device platforms ⓘ  
2 included >

Locations ⓘ  
Not configured >

Client apps (preview) ⓘ  
Not configured >

**Configure** ⓘ  
Yes No

Select the client apps this policy will apply to

☐ Browser

☒ Mobile apps and desktop clients

☒ Modern authentication clients

☐ Exchange ActiveSync clients

☐ Other clients ⓘ

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

**New** ×

**Grant** □ ×

**Info**

\* Name  
Require compliant device (PC & Mac) ✓

**Assignments**

Users and groups ⓘ  
All users >

Cloud apps or actions ⓘ  
2 apps included >

Conditions ⓘ  
2 conditions selected >

**Access controls**

Grant ⓘ  
0 controls selected >

Select the controls to be enforced.

☐ Block access

☒ Grant access

☐ Require multi-factor authentication ⓘ

☒ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy (preview) ⓘ  
[See list of policy protected client apps](#)

**For multiple controls**

☒ Require all the selected controls

☐ Require one of the selected controls

## Require approved app (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 the apps you wish to protect, for example **Office 365 Exchange Online** and **Office 365 SharePoint Online**.

Require approved app (iOS a... X

Info Delete

Name

Require approved app (iOS and Android)

Assignments

Users and groups ⓘ>

All users

Cloud apps or actions ⓘ>

2 apps included

Conditions ⓘ>

2 conditions selected

Access controls

Cloud apps or actions X

Select what this policy applies to

Cloud apps User actions

Include Exclude


☐ None


☐ All cloud apps

☒ Select apps

Select

Office 365 SharePoint Online a...>

 Office 365 Exchange O... ...

 Office 365 SharePoint ... ...

Under **Conditions > Device platforms**, choose only **Android** and **iOS**. The access control “*Require approved client app*” only applies to these mobile platforms.

The screenshot shows a two-pane interface. The left pane, titled 'Conditions', has a list of items: 'Sign-in risk' (Not configured), 'Device platforms' (2 included), 'Locations' (Not configured), 'Client apps (preview)' (1 included), and 'Device state (preview)' (Not configured). The 'Device platforms' item is selected and highlighted in blue. The right pane, titled 'Device platforms', contains the following configuration options: a 'Learn more' link, a 'Configure' section with 'Yes' and 'No' buttons (where 'Yes' is selected), an 'Include' and 'Exclude' toggle (where 'Include' is selected), and a list of device platforms with checkboxes: 'Any device' (unselected), 'Select device platforms' (selected), 'Android' (checked), 'iOS' (checked), 'Windows Phone' (unchecked), 'Windows' (unchecked), and 'macOS' (unchecked).

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

The screenshot shows a two-pane interface. The left pane, titled 'Conditions', has a list of items: 'Sign-in risk' (Not configured), 'Device platforms' (2 included), 'Locations' (Not configured), and 'Client apps (preview)' (Not configured). The 'Client apps (preview)' item is selected and highlighted in blue. The right pane, titled 'Client apps (preview)', contains the following configuration options: a 'Configure' section with 'Yes' and 'No' buttons (where 'Yes' is selected), a 'Select the client apps this policy will apply to' section with checkboxes: 'Browser' (unchecked), 'Mobile apps and desktop clients' (checked), 'Modern authentication clients' (checked), 'Exchange ActiveSync clients' (unchecked), and 'Other clients' (unchecked).



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 approved app (iOS and Android)**

Info Delete

Name  
Require approved app (iOS and Android)

Assignments

Users and groups  
All users

Cloud apps or actions  
2 apps included

Conditions  
2 conditions selected

Access controls  
Grant  
1 control selected

**Grant**

Select the controls to be enforced.

☐ Block access

☒ Grant access

☐ Require multi-factor authentication

☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☒ Require approved client app  
[See list of approved client apps](#)

☐ Require app protection policy (preview)  
[See list of policy protected client apps](#)

For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

### Require MFA for web browsers (unmanaged devices)

Create a new policy and assign **All users** (excluding your “break glass” admin account). Choose **All cloud apps**.

**Require MFA for web browser...**

Info Delete

Name  
Require MFA for web browsers (unmanaged)

Assignments

Users and groups  
All users included and specific...

Cloud apps or actions  
All cloud apps

Conditions  
2 conditions selected

Access controls

**Cloud apps or actions**

Select what this policy applies to

☒ Cloud apps ☐ User actions

Include Exclude

☐ None

☒ All cloud apps

☐ Select apps

Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

Under **Conditions**, pick **Client apps > Browser**.

The image shows two side-by-side configuration panels. The left panel, titled 'Conditions', has a sidebar with 'Info', 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), and 'Client apps (preview)' (1 included). The 'Client apps (preview)' item is selected. The right panel, titled 'Client apps (preview)', has a 'Configure' toggle set to 'Yes'. Below it, the text says 'Select the client apps this policy will apply to'. There are two checkboxes: 'Browser' (checked) and 'Mobile apps and desktop clients' (unchecked). A link labeled 'Advanced' is at the bottom.

Also choose another condition: **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.

The image shows two side-by-side configuration panels. The left panel, titled 'Conditions', has a sidebar with 'Info', 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), 'Client apps (preview)' (1 included), and 'Device state (preview)' (All device state and exclude Devi...). The 'Device state (preview)' item is selected. The right panel, titled 'Device state (preview)', has an 'Info' tab. Below it is a 'Configure' toggle set to 'Yes'. There are two tabs: 'Include' and 'Exclude' (selected). The text says 'Select the device state condition used to exclude devices from policy.' There are two checkboxes: 'Device Hybrid Azure AD joined' (unchecked) and 'Device marked as compliant' (checked).

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

### Require MFA for web browser...

Info Delete

**Name**  
Require MFA for web browsers (unmanaged devices)

**Assignments**

Users and groups  
All users included and specific...

Cloud apps or actions  
All cloud apps

Conditions  
2 conditions selected

**Access controls**

Grant  
1 control selected

### Grant

Select the controls to be enforced.

☐ Block access

☒ Grant access

☒ Require multi-factor authentication

☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☐ Require approved client app  
[See list of approved client apps](#)

☐ Require app protection policy (preview)  
[See list of policy protected client apps](#)

For multiple controls

☐ Require all the selected controls

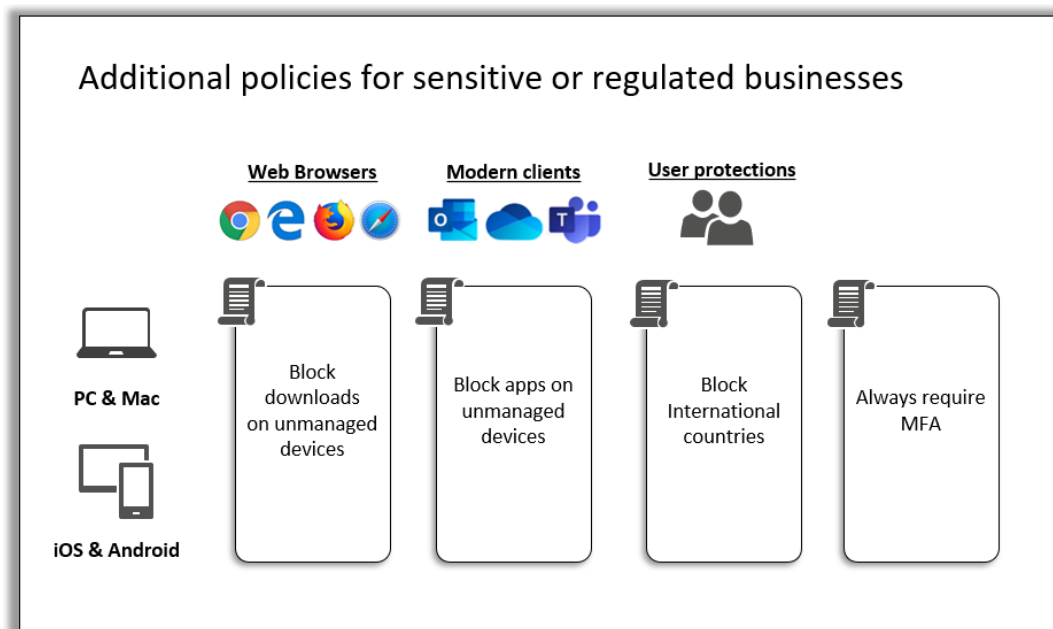
☒ Require one of the selected controls

Now that we have the policies in place, and before you turn them on, we will describe their impacts and considerations, again in a table as we did before.

Conditional access policy	Description	Impact	Considerations
<b>Block ActiveSync clients</b>	Blocks legacy Exchange ActiveSync clients from connecting	Users should use the modern Outlook app	Alert users to this change before rolling it out
<b>Require compliant devices (PC &amp; Mac)</b>	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
<b>Require approved app (iOS &amp; Android)</b>	This policy blocks apps such as the native mail app for iOS or Android	Users must use modern apps like Outlook and OneDrive	Alert users to this change before rolling it out
<b>Require MFA for web browsers (unmanaged devices)</b>	Prompts users in web browsers for MFA on unmanaged devices	Unmanaged devices cannot gain access over the web without MFA	Exclude service accounts that cannot do MFA

## 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 additional custom policy set is as follows:

- Always require MFA
- Block International countries
- Block apps on unmanaged devices
- Block downloads on unmanaged devices

The following table describes how to build out the policies.

Conditional access policy	Assignments	Conditions	Access Control
<b>Always require MFA</b>	<b>Users:</b> All users <b>Apps:</b> All cloud apps	<b>None</b>	<b>Grant access:</b> Require multi-factor authentication
<b>Block international countries</b>	<b>Users:</b> All users <b>Apps:</b> All cloud apps	<b>Location:</b> Pick named location with blocked country list	<b>Block access</b>
<b>Block apps on unmanaged devices</b>	<b>Users:</b> All users <b>Apps:</b> Exchange Online, SharePoint Online	<b>Device platforms:</b> Any device <b>Client apps:</b> Modern authentication clients	<b>Grant access:</b> Require device to be marked as compliant
<b>Block downloads on unmanaged devices</b>	<b>Users:</b> All users <b>Apps:</b> Exchange Online, SharePoint Online	<b>Client apps:</b> Browser	<b>Session:</b> Use app enforced restrictions

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**.

The screenshot shows the 'Always require MFA' policy configuration window with the 'Users and groups' tab selected. The left pane shows the policy name 'Always require MFA' and two assignment categories: 'Users and groups' (with 'All users included and specific...' selected) and 'Cloud apps or actions' (with 'All cloud apps' selected). The right pane shows the 'Include' tab with radio buttons for 'None', 'All users' (selected), and 'Select users and groups'. Below these are checkboxes for 'All guest and external users (preview)', 'Directory roles (preview)', and 'Users and groups'.

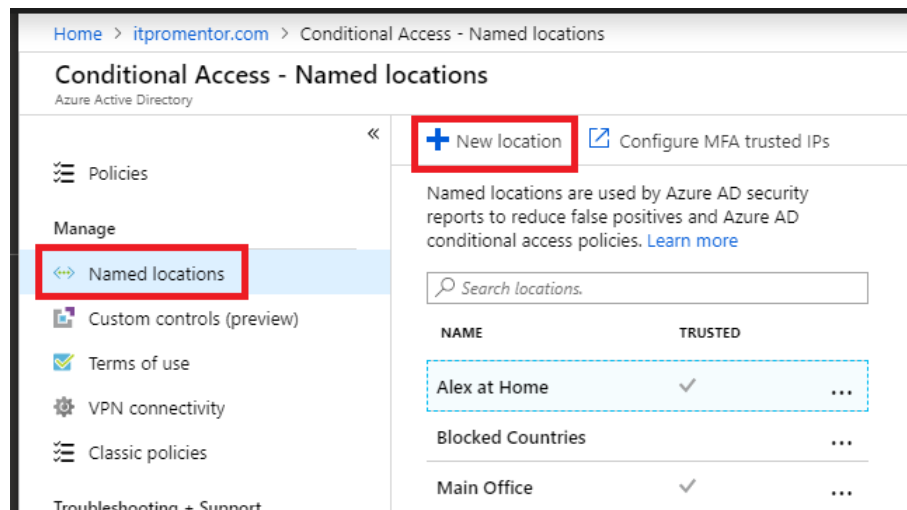
Do not select any conditions (we do not want to require MFA only under *certain* conditions but rather *all*). Therefore, move right into **Access controls**, choose **Grant access** and **Require multi-factor authentication**.

The screenshot shows the 'Always require MFA' policy configuration window with the 'Grant' tab selected. The left pane shows the policy name 'Always require MFA' and three assignment categories: 'Users and groups' (with 'All users included and specific...' selected), 'Cloud apps or actions' (with 'All cloud apps' selected), and 'Conditions' (with '0 conditions selected'). The 'Access controls' section shows 'Grant' selected with '1 control selected'. The right pane shows the 'Select the controls to be enforced.' section with radio buttons for 'Block access' and 'Grant access' (selected). Below are checkboxes for 'Require multi-factor authentication' (checked), 'Require device to be marked as compliant', 'Require Hybrid Azure AD joined device', 'Require approved client app' (with a link to 'See list of approved client apps'), and 'Require app protection policy (preview)' (with a link to 'See list of policy protected client apps'). The 'For multiple controls' section has radio buttons for 'Require all the selected controls' and 'Require one of the selected controls' (selected).

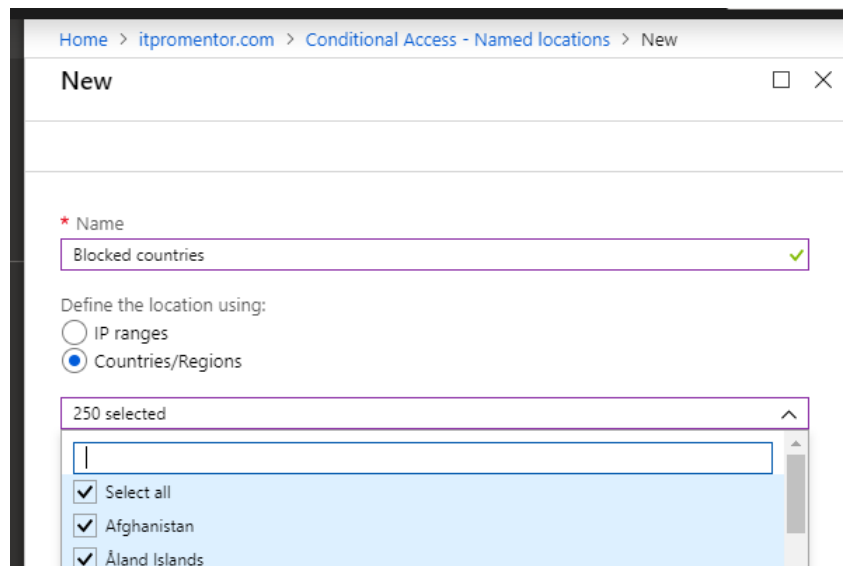
## Block International countries

This policy is used to block sign-in from foreign countries; recommended for sensitive or highly regulated industries, and especially when there is no reason one of your users should be authenticating from foreign locations. Note, this does not prevent users from communicating or doing business with those other countries.

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



Name the location **Blocked countries**. Pick the **Countries/Regions** option, then **Select all** the countries at first.



You can then filter this list by any country or countries you wish to exclude from the policy. For example, I live in the United States, and let's say my company also has offices in Canada. I might only deselect those two countries from this list.

The screenshot shows the 'New' location configuration page in the Azure AD portal. The breadcrumb trail is 'Home > itpromentor.com > Conditional Access - Named locations > New'. The page title is 'New'. There is a text input field for 'Name' containing 'Blocked countries' with a green checkmark. Below this, it says 'Define the location using:' with two radio buttons: 'IP ranges' and 'Countries/Regions'. The 'Countries/Regions' radio button is selected. Below the radio buttons is a dropdown menu showing '249 selected'. A search bar contains the text 'unit'. Below the search bar, there is a list of countries with checkboxes: 'United Arab Emirates' (checked), 'United Kingdom' (checked), and 'United States' (unchecked).

**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**, pick **Locations** then **Selected locations** and choose **Blocked countries**. Under **Access controls**, choose **Block access**.

The screenshot shows the Azure AD Conditional Access policy configuration page. The breadcrumb trail is 'Home > itpromentor.com > Conditional Access - Policies > Block International Sign-in > Conditions > Locations'. The page is divided into three main sections: 'Block International Sign-in', 'Conditions', and 'Locations'. In the 'Block International Sign-in' section, the 'Name' field contains 'Block International Sign-in'. Under 'Assignments', 'Users and groups' is set to 'All users included and specific us...', 'Cloud apps or actions' is set to 'All cloud apps', and 'Conditions' is set to '1 condition selected'. Under 'Access controls', the 'Grant' section is expanded, showing 'Block access' selected. In the 'Conditions' section, 'Locations' is selected, showing '1 included and all trusted locatio...'. In the 'Locations' section, 'Configure' is set to 'Yes', 'Include' is selected, and 'Selected locations' is chosen. Below this, a search bar shows 'Blocked Countries' and a list of countries is visible.

## Block apps on unmanaged devices

This policy requires that devices be enrolled with Intune, and Compliance policies be assigned, before enabling the corresponding Conditional access policy.

Create the new policy. Assign to **All users** and pick **Office 365 Exchange Online** and **Office 365 SharePoint Online**. Both of these cloud apps contain storage locations with sensitive company data, which could be synced to a device using a modern client application like Outlook or OneDrive.

The screenshot displays the configuration interface for a Conditional Access policy named "Block unmanaged devices".

**Left Pane (Policy Overview):**

- Name:** Block unmanaged devices
- Assignments:**
  - Users and groups: All users included and specific...
  - Cloud apps or actions:** 2 apps included (highlighted)
  - Conditions: 2 conditions selected
- Access controls:**

**Right Pane (Cloud apps or actions configuration):**

- Select what this policy applies to:** Cloud apps (selected), User actions
- Include/Exclude:** Include (selected), Exclude
- Options:**
  - ☐ None
  - ☐ All cloud apps
  - ☒ Select apps
- Select:** Office 365 SharePoint Online a... (with a chevron icon)
- App List:**
  - Office 365 Exchange O... (with a chevron icon)
  - Office 365 SharePoint ... (with a chevron icon)

Under **Conditions**, specify **Device platforms > Any device** as well as **Client apps > Mobile apps and desktop clients** and **Modern authentication clients**. Modern clients tend to store company data on the local device (e.g. Outlook .ost file, OneDrive sync client, etc.). All other client types are being targeted by other policies.



Conditions

Info

Sign-in risk

Not configured

Device platforms

Any device

Locations

Not configured

Client apps (preview)

1 included

Device state (preview)

Not configured

Client apps (preview)

Configure

Yes No

Select the client apps this policy will apply to

Browser

Mobile apps and desktop clients

Modern authentication clients

Exchange ActiveSync clients

Other clients

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

Block unmanaged devices

Info Delete

Name

Block unmanaged devices

Assignments

Users and groups

All users included and specific...

Cloud apps or actions

2 apps included

Conditions

2 conditions selected

Access controls

Grant

1 control selected

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

Require app protection policy (preview)

See list of approved client apps

See list of policy protected client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

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 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 contain storage locations with sensitive company data.

**Block downloads on unmanaged devices** ✕

Info Delete

\* Name  
Block downloads on unmanaged devices

**Assignments**

Users and groups ⓘ  
All users >

Cloud apps or actions ⓘ  
2 apps included >

Conditions ⓘ  
1 condition selected >

**Access controls**

**Cloud apps or actions** □ ✕

Select what this policy applies to  
**Cloud apps** User actions

Include Exclude

☐ None  
☐ All cloud apps  
☒ Select apps

Select  
Office 365 SharePoint Online a... >

Office 365 Exchange O... ...  
 Office 365 SharePoint ... ...

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

**Conditions** ✕

Info

Sign-in risk ⓘ  
Not configured >

Device platforms ⓘ  
Not configured >

Locations ⓘ  
Not configured >

Client apps (preview) ⓘ  
1 included >

**Client apps (preview)** □ ✕

Configure ⓘ  
**Yes** No

Select the client apps this policy will apply to

☒ Browser  
☐ Mobile apps and desktop clients  
[Advanced](#)

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

Block downloads on unmana... X

Info Delete

Name

Block downloads on unmanaged devices

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

2 apps included

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

Use app enforced restrictions

Session X

Session controls enable limited experiences within a cloud app. Select the session usage requirements.

Learn more

☒ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

☐ Sign-in frequency (preview) ⓘ

☐ Persistent browser session (preview) ⓘ

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\alex> Get-OwaMailboxPolicy | fl Name,ConditionalAccessPolicy

Name                : OwaMailboxPolicy-Default
ConditionalAccessPolicy : Off

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

To enable for SharePoint Online, connect to [SharePoint Online Management Shell using MFA](#). Run:

## Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess
PS C:\WINDOWS\system32> Get-SPOTenant | fl Name,ConditionalAccessPolicy

ConditionalAccessPolicy : AllowLimitedAccess

PS C:\WINDOWS\system32>
```

*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.*

Now that we have the policies in place, and before you turn them on, we will describe their impacts and considerations, again in a table as we did before.

Conditional access policy	Description	Impact	Considerations
<b>Always require MFA</b>	Multi-factor challenge required for access	Users required to perform MFA more frequently	Alert users to this change before rolling it out
<b>Block International countries</b>	Sign-in blocked from specified foreign countries	Traveling internationally can be difficult	Excluding a group: "Traveling users"
<b>Block access from apps on unmanaged devices</b>	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
<b>Block downloads on unmanaged devices</b>	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