

# Recommended Conditional Access policies for Microsoft 365

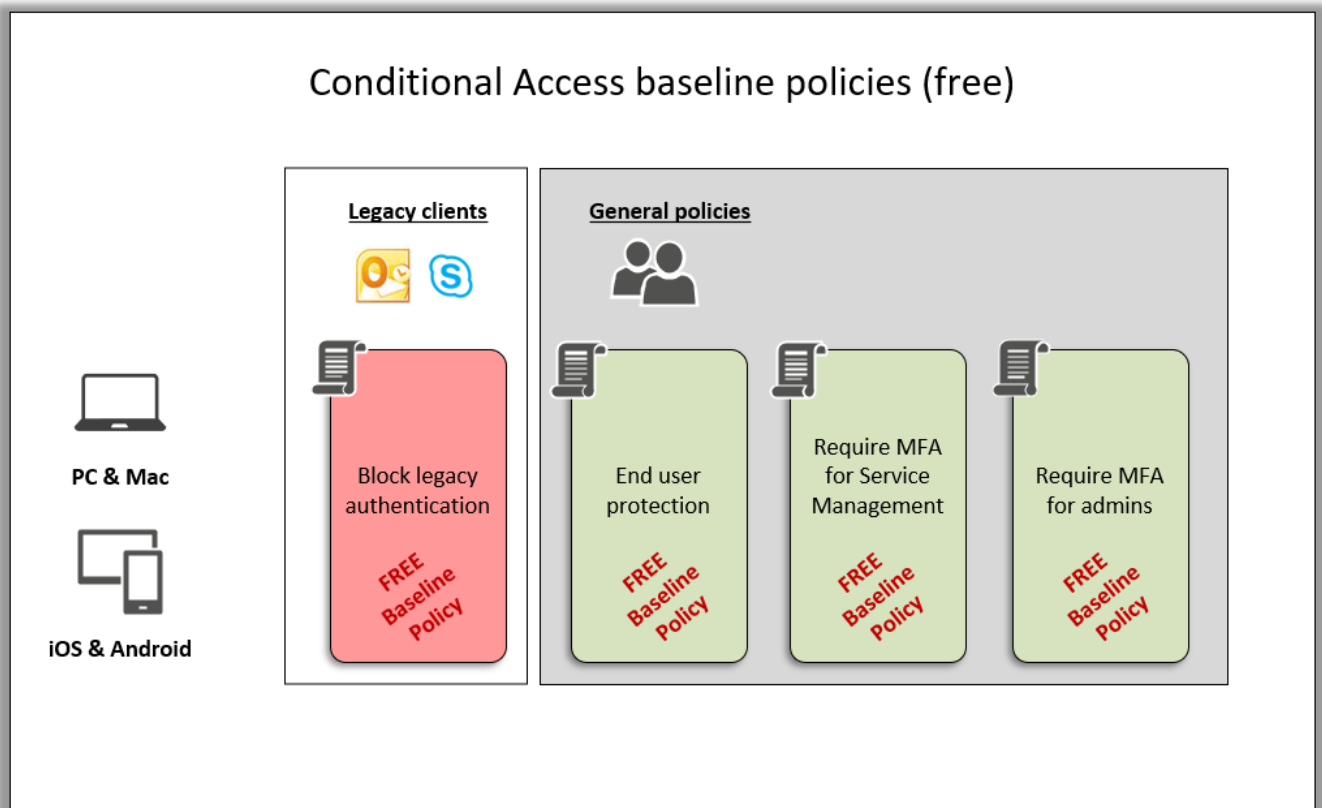
By Alex Fields, ITProMentor.com

Updated: 06/30/2019

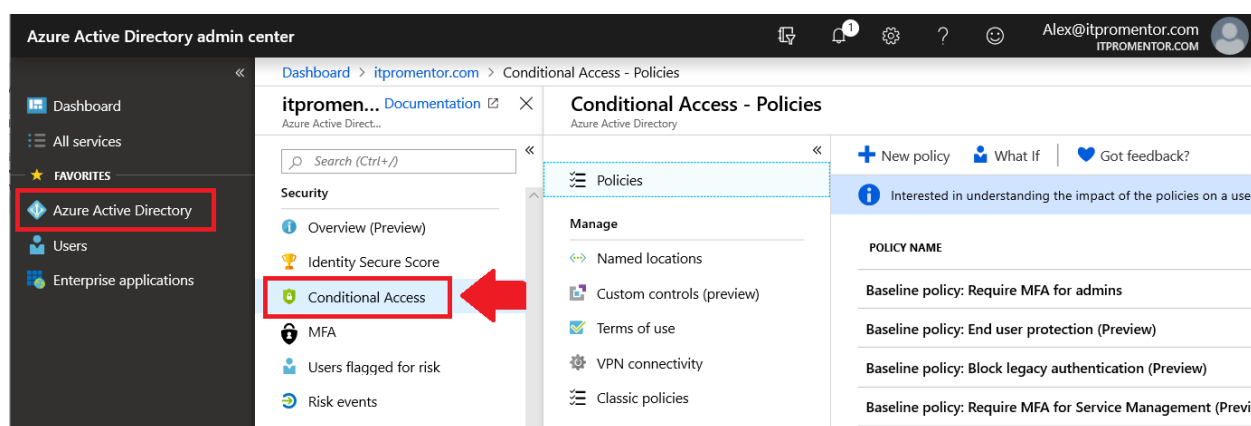
Conditional Access enables you to either block, allow or limit access under different circumstances that you define via policy. This document describes in detail setting up the policies detailed in [this resource](#).

## 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
<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 are required to use MFA	Admins must register for 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	No exclusions**
<b>Block legacy authentication</b>	Block legacy apps & protocols such as IMAP, POP and SMTP	Blocks basic auth (Outlook 2010 and any other legacy apps)	No exclusions**

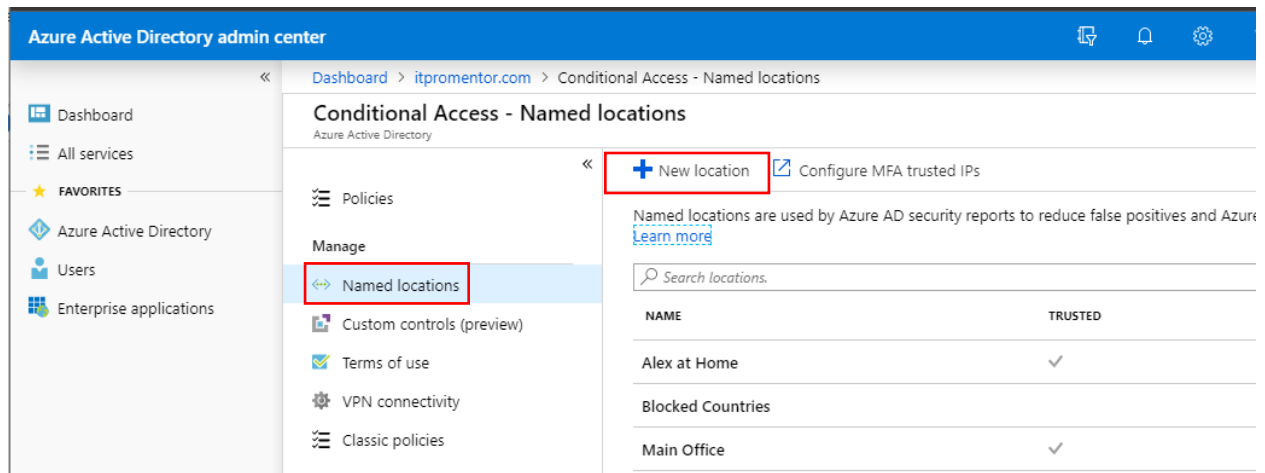
At the time of this writing, just know that the free baseline policies are still in “preview” which means that there could still be changes made to them before they are finalized. Also, Microsoft support may not be able to assist with preview items (though I find they usually make a best effort).

*\*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.*

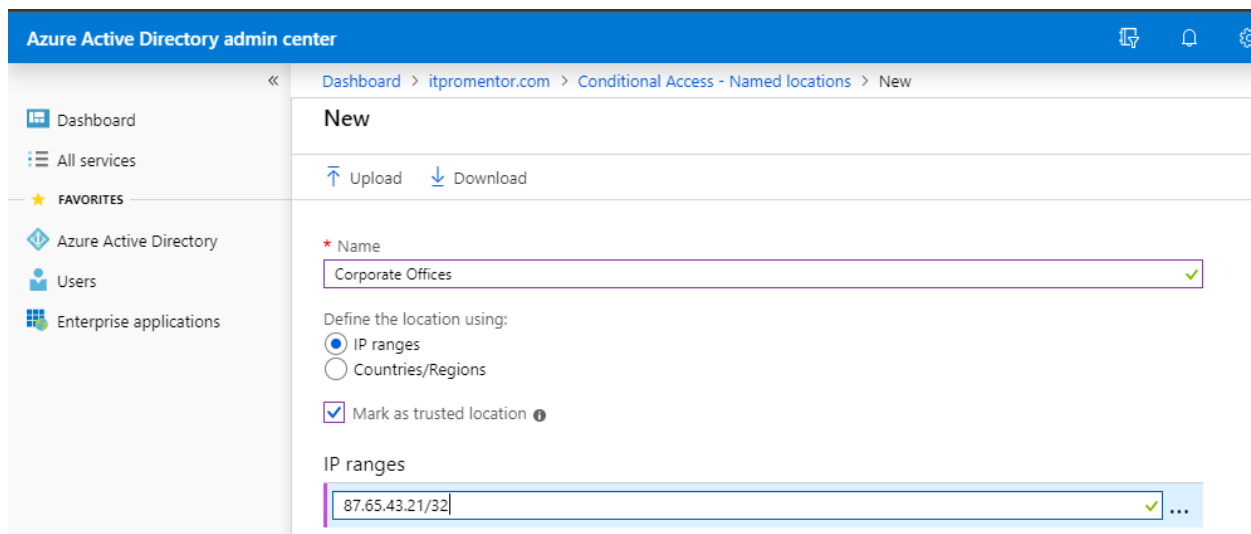
*\*\*At this time, it is not possible to exclude accounts from either **End user protection** or **Block legacy authentication**. If you have accounts that must continue to use basic authentication, then these policies are not for you!*

## Define trusted locations

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



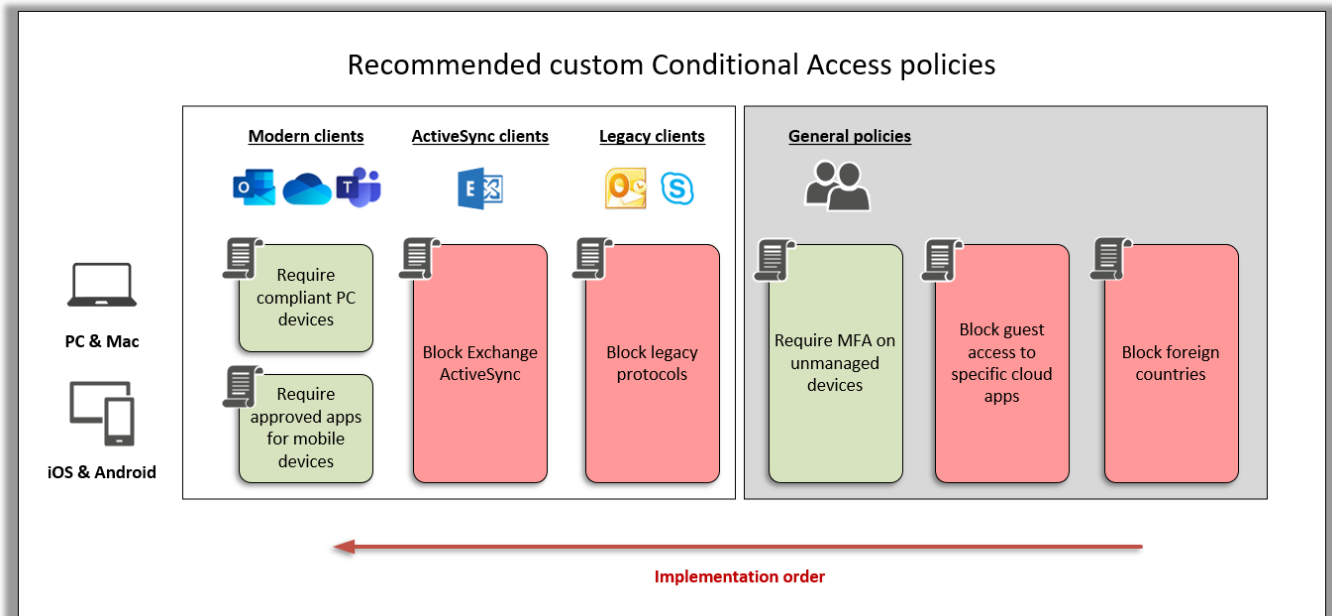
Fill out a **Name** such as *Corporate Offices*, choose **IP ranges** and **Mark as trusted location**. Type the CIDR IP address(es). These must be external addresses (not internal). Click **Create** to finish.



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
<b>Block foreign countries</b>	Blocks sign-on from other countries	Traveling internationally can be difficult	Exclude an “International travelers” group
<b>Block guest access</b>	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
<b>Require MFA on unmanaged devices</b>	Prompts users for MFA on unmanaged devices	Device enrollment and web browser access requires MFA	Exclude service accounts that cannot do MFA
<b>Block legacy protocols</b>	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
<b>Block ActiveSync clients</b>	Blocks Exchange ActiveSync clients	Users should use the modern Outlook app	Alert users to this change before rolling it out
<b>Require approved apps for mobile devices</b>	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
<b>Require compliant devices</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

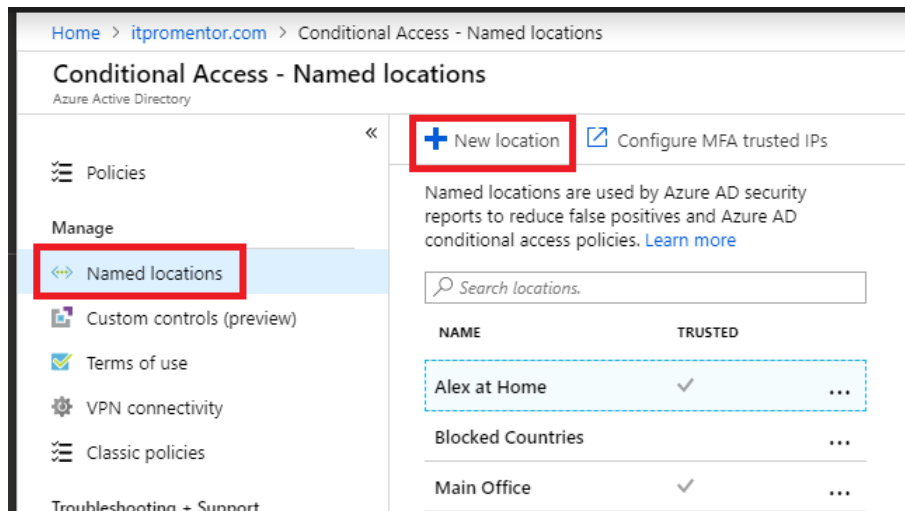
The following table lists all of the settings contained within the recommended custom policies. We will also provide screen shots to assist with the creation of each of these policies.

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

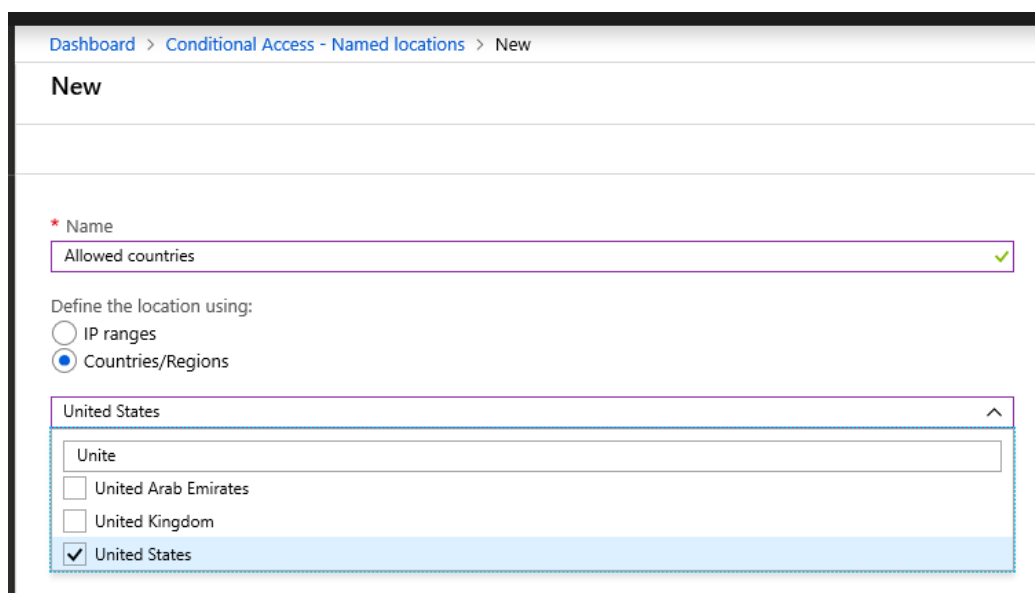
## Block foreign countries

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**.

Dashboard > Conditional Access - Policies > BLOCK - Foreign Countries > Conditions > Locations

**BLOCK - Foreign Countries** ×

Info Delete

\* Name  
BLOCK - Foreign Countries

Assignments

Users and groups ⓘ  
All users included and specific... >

Cloud apps or actions ⓘ  
All cloud apps >

Conditions ⓘ  
1 condition selected >

Access controls

Grant ⓘ  
Block access >

**Conditions** ×

Info

Sign-in risk ⓘ  
Not configured >

Device platforms ⓘ  
Not configured >

Locations ⓘ  
Any location and 1 excluded >

Client apps (preview) ⓘ  
Not configured >

Device state (preview) ⓘ  
Not configured >

**Locations** □ ×

Control user access based on their physical location. [Learn more](#)

Configure ⓘ  
**Yes** No

**Include** **Exclude**

Select the locations to exempt from the policy

☐ All trusted locations  
☒ Selected locations

Select  
Allowed countries >

Allowed countries ...

### 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.

Dashboard > Conditional Access - Policies > New > Users and groups

**New** ×

Info

\* Name  
LOCK - Guest access for specific cloud apps ✓

Assignments

Users and groups ⓘ  
Specific users included >

Cloud apps or actions ⓘ  
All cloud apps included and 2 ap... >

**Users and groups** □ ×

**Include** **Exclude**

☐ None  
☐ All users  
☒ Select users and groups

☒ All guest and external users (preview) ⓘ  
☐ Directory roles (preview) ⓘ  
☐ Users and groups

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.

Dashboard > Conditional Access - Policies > New > Cloud apps or actions

**New**

Info

\* Name

LOCK - Guest access for specific cloud apps ✓

Assignments

Users and groups ⓘ

Specific users included >

Cloud apps or actions ⓘ

No cloud apps or actions selected >

Conditions ⓘ

0 conditions selected >

**Cloud apps or actions**

Select what this policy applies to

Cloud apps User actions

Include Exclude

Select the cloud apps to exempt from the policy

Select excluded cloud apps

Office 365 SharePoint Online and... >

Microsoft Teams ...

Office 365 SharePoint On... ...

### Require MFA on unmanaged devices

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**.

Dashboard > Conditional Access - Policies > ALLOW - Require MFA for unmanaged devices > Conditions > Device state (preview)

**ALLOW - Require MFA for un...**

Info Delete

\* Name

ALLOW - Require MFA for unmanaged devices

Assignments

Users and groups ⓘ

All users included and specific us... >

Cloud apps or actions ⓘ

All cloud apps >

Conditions ⓘ

1 condition selected >

Access controls

Grant ⓘ

1 control selected >

**Conditions**

Info

Sign-in risk ⓘ

Not configured >

Device platforms ⓘ

Not configured >

Locations ⓘ

Not configured >

Client apps (preview) ⓘ

Not configured >

Device state (preview) ⓘ

All device state and exclude Devi... >

**Device state (preview)**

Info

Configure ⓘ

Yes No

Include Exclude

Select the device state condition used to exclude devices from policy.

☐ Device Hybrid Azure AD joined ⓘ

☒ Device marked as compliant ⓘ



Under **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.

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 **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

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

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)

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.*

#### 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.

Conditions

Info

Sign-in risk

Not configured

Device platforms

2 included

Locations

Not configured

Client apps (preview)

1 included

Device state (preview)

Not configured

Device platforms

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** & **Modern authentication clients**. All other client types are being blocked by other policies.

Conditions

Info

Sign-in risk

Not configured

Device platforms

2 included

Locations

Not configured

Client apps (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

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.



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

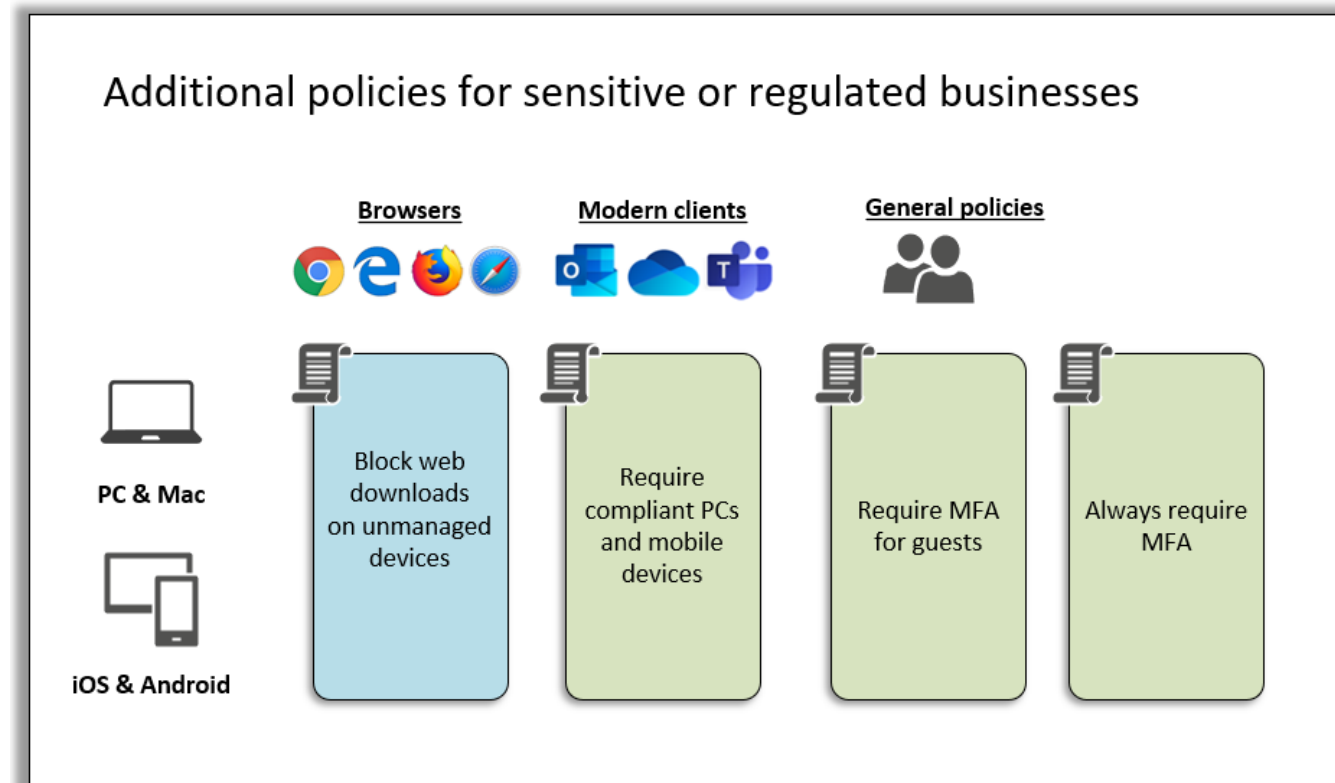
The image shows two side-by-side configuration panels. The left panel, titled 'Conditions', has an 'Info' icon and lists four items: 'Sign-in risk' (Not configured), 'Device platforms' (2 included), 'Locations' (Not configured), and 'Client apps (preview)' (Not configured). The 'Client apps (preview)' item is highlighted in blue. The right panel, titled 'Client apps (preview)', has a 'Configure' toggle set to 'Yes' and a section 'Select the client apps this policy will apply to'. It contains five checkboxes: 'Browser' (unchecked), 'Mobile apps and desktop clients' (checked), 'Modern authentication clients' (checked), 'Exchange ActiveSync clients' (unchecked), and 'Other clients' (unchecked).

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

The image shows two side-by-side configuration panels. The left panel, titled 'New', has an 'Info' icon and includes a 'Name' field with the value 'Require compliant device (PC & Mac)' and a green checkmark. Below are sections for 'Assignments' (Users and groups: All users; Cloud apps or actions: 2 apps included; Conditions: 2 conditions selected) and 'Access controls' (Grant: 0 controls selected). The 'Grant' item is highlighted in blue. The right panel, titled 'Grant', has a section 'Select the controls to be enforced.' with two radio buttons: 'Block access' (unchecked) and 'Grant access' (checked). Below are five checkboxes: 'Require multi-factor authentication' (unchecked), 'Require device to be marked as compliant' (checked), 'Require Hybrid Azure AD joined device' (unchecked), 'Require approved client app' (unchecked), and 'Require app protection policy (preview)' (unchecked). At the bottom, under 'For multiple controls', there are two radio buttons: 'Require all the selected controls' (checked) and 'Require one of the selected controls' (unchecked).

## 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
<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>Require MFA for guests</b>	Multi-factor challenge required for guest access	Guests required to perform MFA	Alert users to this change before rolling it out
<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

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>Require MFA for guests</b>	<b>Users:</b> All guest and external users <b>Apps:</b> All cloud apps	<b>None</b>	<b>Grant access:</b> Require multi-factor authentication
<b>Require compliant PCs and mobile devices</b>	<b>Users:</b> All users <b>Apps:</b> All cloud apps	<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**.

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**.



## Always require MFA

Info

Delete

Name

Always require MFA

Assignments

Users and groups

All users included and specific...

Cloud apps or actions

All cloud apps

Conditions

0 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

### 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**.

Dashboard > Conditional Access - Policies > ALLOW - Require MFA for guests > Users and groups

## ALLOW - Require MFA for gu...

Info

Delete

Name

ALLOW - Require MFA for guests

Assignments

Users and groups

Specific users included

Cloud apps or actions

All cloud apps

Conditions

0 conditions selected

## Users and groups

Include

Exclude

None

All users

Select users and groups

All guest and external users (preview)

Directory roles (preview)

Users and groups

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

The screenshot displays the 'Client apps (preview)' configuration window. The left pane, titled 'Conditions', lists several criteria: 'Sign-in risk' (Not configured), 'Device platforms' (Any device), 'Locations' (Not configured), 'Client apps (preview)' (1 included), and 'Device state (preview)' (Not configured). The 'Client apps (preview)' condition is selected. The right pane, titled 'Client apps (preview)', shows a 'Configure' section with 'Yes' and 'No' buttons. Below this, it asks to 'Select the client apps this policy will apply to' and provides four checkboxes: 'Browser' (unchecked), 'Mobile apps and desktop clients' (checked), 'Modern authentication clients' (checked), 'Exchange ActiveSync clients' (unchecked), and 'Other clients' (unchecked).

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 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.

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

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 pick **Client app > Browser**.

Conditions X

Info

Sign-in risk ⓘ

Not configured >

Device platforms ⓘ

Not configured >

Locations ⓘ

Not configured >

Client apps (preview) ⓘ

1 included >

Client apps (preview) □ X

Configure ⓘ

Yes

No

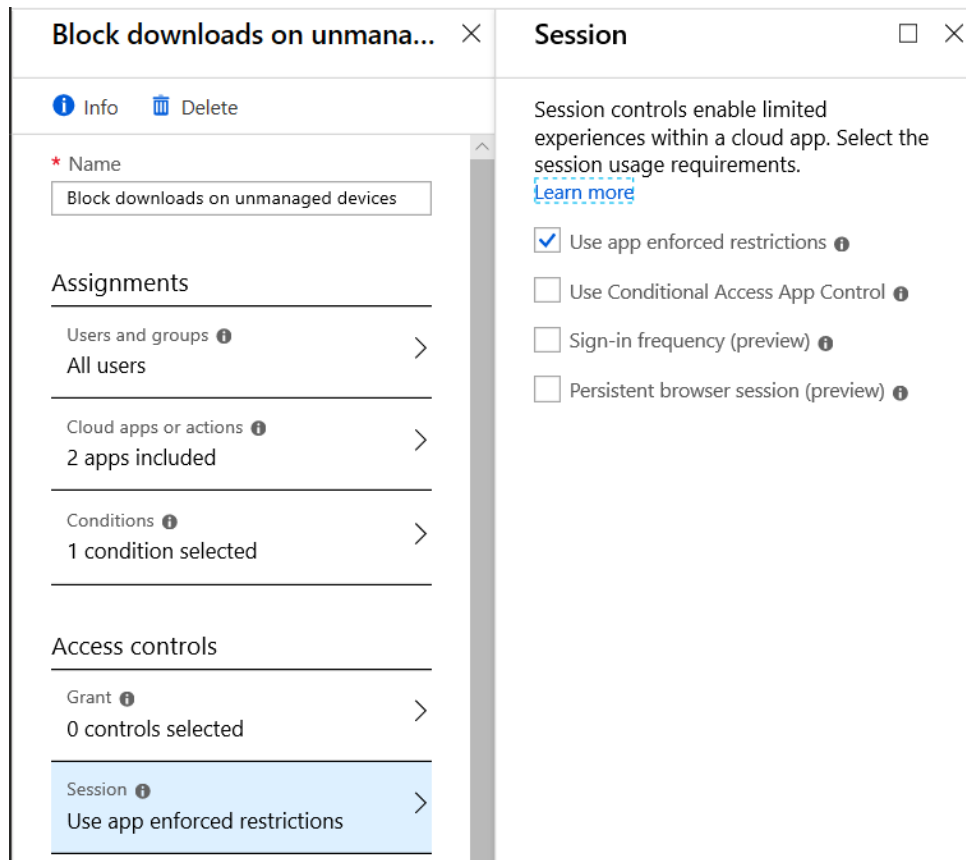
Select the client apps this policy will apply to

☒ Browser

☐ Mobile apps and desktop clients

Advanced

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



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
```

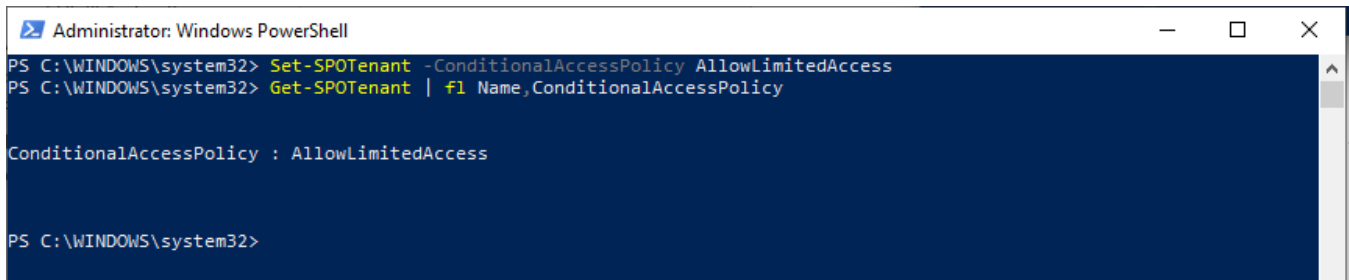
```
PS C:\Users\alex> Get-OwaMailboxPolicy | fl Name,ConditionalAccessPolicy

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.*

This concludes guidance on the recommended conditional access policies.