

# Recommended Conditional Access policies for Microsoft 365

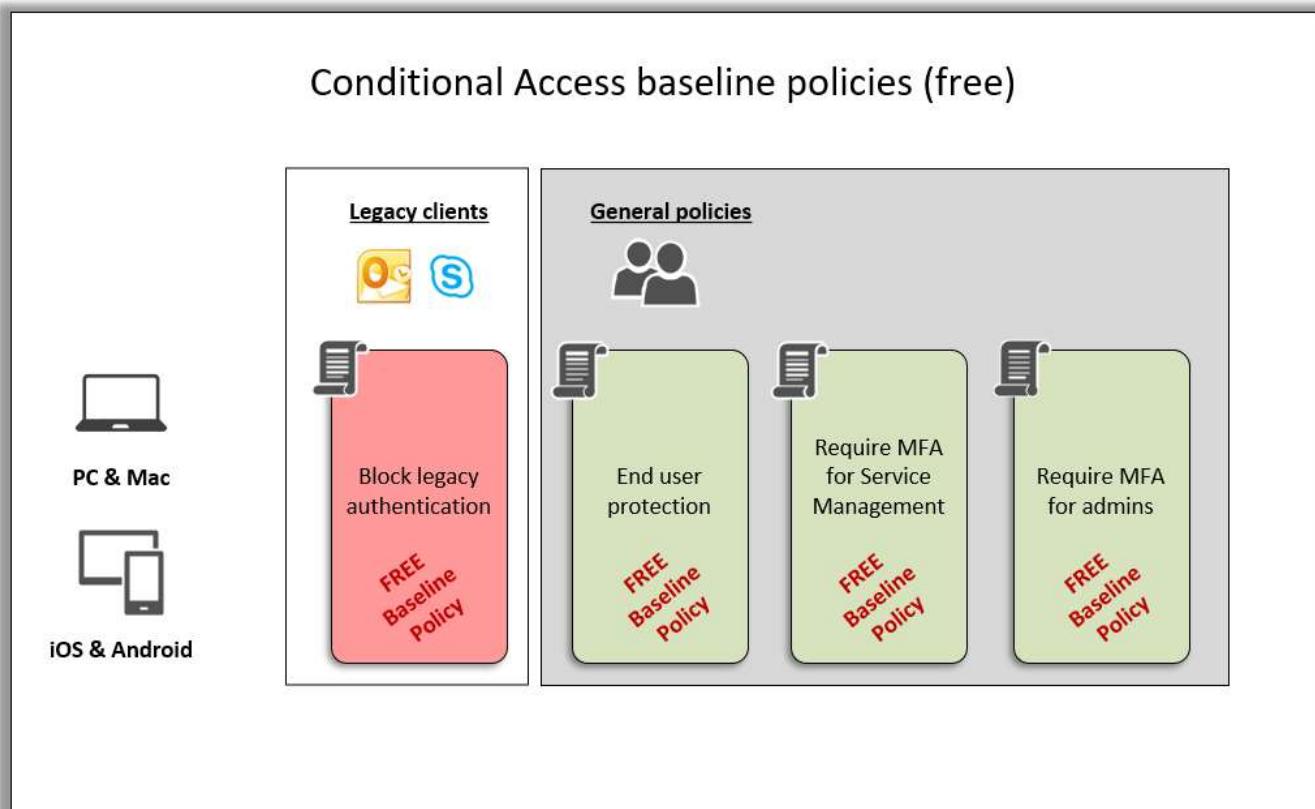
By Alex Fields, ITProMentor.com

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 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                         |
|---|---|--|--|
| <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**                        |

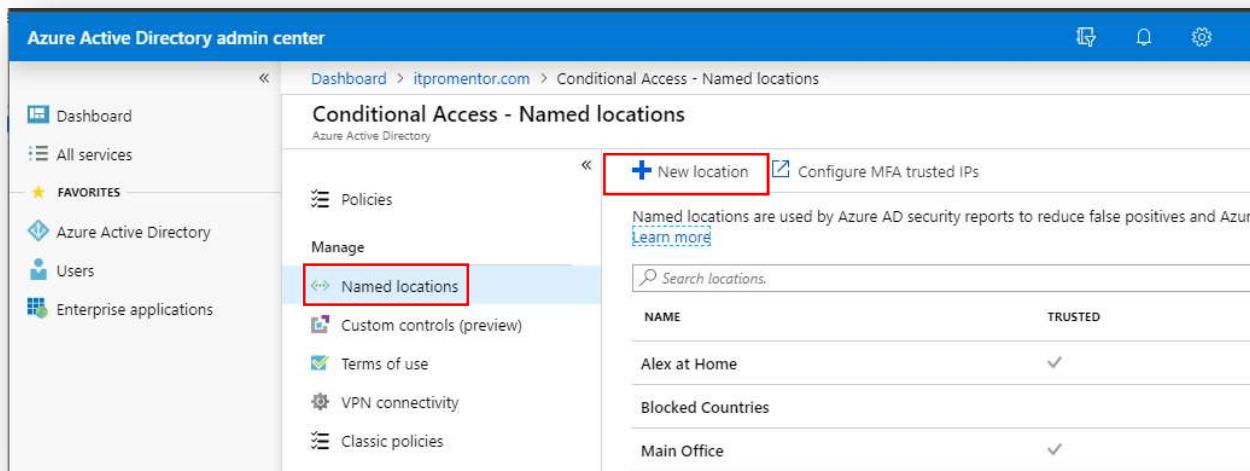
At the time of this writing, just know that the free baseline policies are still in “preview” which means that there could still be changes made to them before they are finalized. Also, Microsoft support may not be able to assist with preview items (though I find they usually make a best effort).

*\*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

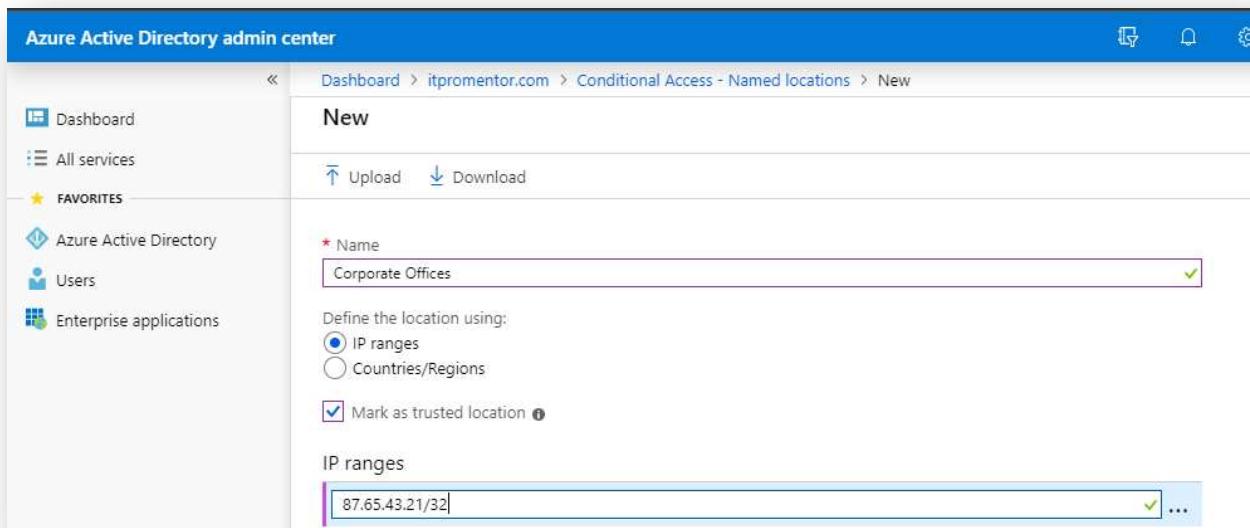
Before building any custom policies, go to **Azure Active Directory > Conditional access** and choose **Named locations**. Click **New location**.



The screenshot shows the Azure Active Directory admin center interface. In the top navigation bar, the URL is `itpromentor.com > Conditional Access - Named locations`. On the left sidebar, under the 'Manage' section, the 'Named locations' link is highlighted with a red box. At the top right of the main content area, there is a blue 'New location' button and a 'Configure MFA trusted IPs' link. Below these, a note states: 'Named locations are used by Azure AD security reports to reduce false positives and Azure Learn more'. A search bar labeled 'Search locations.' is present. The main table lists three named locations:

| NAME              | TRUSTED |
|-------------------|---------|
| Alex at Home      | ✓       |
| Blocked Countries |         |
| Main Office       | ✓       |

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.

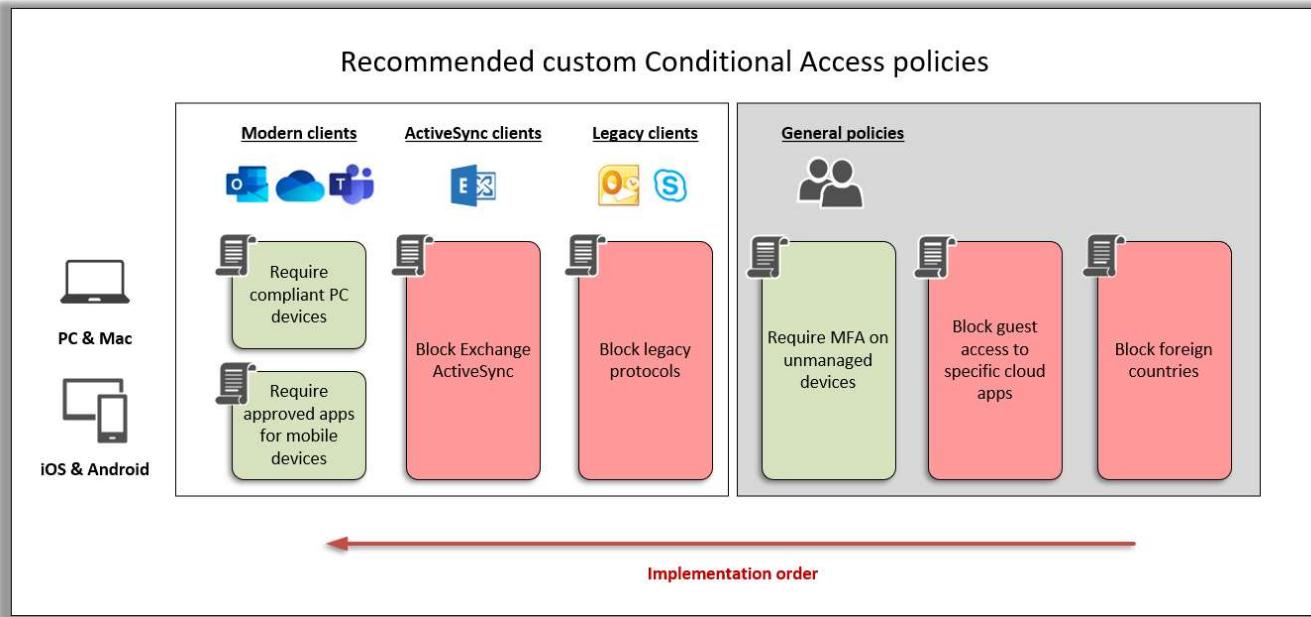


The screenshot shows the 'New' configuration page for a named location. The 'Name' field is filled with 'Corporate Offices'. Under 'Define the location using:', the 'IP ranges' radio button is selected. The 'Mark as trusted location' checkbox is checked. The 'IP ranges' input field contains '87.65.43.21/32'.

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>                   | Blocks 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<br><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<br><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<br><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<br><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<br><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<br><b>Apps:</b> All cloud apps  | <b>Device platforms:</b> iOS and Android<br><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<br><b>Apps:</b> All cloud apps  | <b>Device platforms:</b> Windows and macOS<br><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**.

Home > itpromentor.com > Conditional Access - Named locations

Conditional Access - Named locations

Azure Active Directory

Policies

Manage

New location

Configure MFA trusted IPs

Named locations

Custom controls (preview)

Terms of use

VPN connectivity

Classic policies

Troubleshooting + Support

Named locations

Search locations.

| NAME              | TRUSTED |
|-------------------|---------|
| Alex at Home      | ✓       |
| Blocked Countries | ...     |
| Main Office       | ✓       |

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.

Dashboard > Conditional Access - Named locations > New

New

\* Name

Allowed countries

Define the location using:

IP ranges

Countries/Regions

United States

United Arab Emirates

United Kingdom

United States

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**.

The screenshot shows the Microsoft Conditional Access Policies interface. A policy named "BLOCK - Foreign Countries" is selected. The "Conditions" tab is active, showing various configuration options like "Sign-in risk", "Device platforms", and "Locations". The "Locations" section is expanded, showing "Any location and 1 excluded". The "Exclude" tab is selected under "Locations". The "Access controls" tab is also visible, showing "Block access" is selected.

### 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.

The screenshot shows the Microsoft Conditional Access Policies interface for creating a new policy. The policy name is "LOCK - Guest access for specific cloud apps". The "Users and groups" tab is active, showing the "Include" tab selected. Under "Assignments", "All guest and external users (preview)" is checked. Other options like "Directory roles (preview)" and "Users and groups" are available but unchecked.

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.

**New**

**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 (selected), User actions

**Include** (selected)   **Exclude**

Select the cloud apps to exempt from the policy

Select excluded cloud apps: Office 365 SharePoint Online and... (includes Microsoft Teams and Office 365 SharePoint Online)

### 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**.

**ALLOW - Require MFA for unmanaged devices**

**Conditions**

**Device state (preview)**

**Configure**: Yes (selected), No

**Exclude**

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

Device Hybrid Azure AD joined

Device marked as compliant

**Assignments**

- Users and groups: All users included and specific users...
- Cloud apps or actions: All cloud apps
- Conditions: 1 condition selected

**Access controls**

- Grant: 1 control selected

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**.

The screenshot shows the configuration of a policy named "Block legacy authentication". The policy is set to target "All users" and includes conditions for "Device platforms" (Not configured) and "Client apps (preview)" (1 included). Under "Access controls", "Block access" is selected. The "Client apps (preview)" section is expanded, showing options for "Mobile apps and desktop clients" (selected), "Modern authentication clients" (unchecked), "Exchange ActiveSync clients" (unchecked), and "Other clients" (selected).

| Block legacy authentication  | Conditions   | Client apps (preview)   |
|--|--|---|
| <p>Info Delete</p> <p>* Name: Block legacy authentication</p> <p>Assignments</p> <ul style="list-style-type: none"><li>Users and groups: All users included and specific users...</li><li>Cloud apps or actions: 2 apps included</li><li>Conditions: 1 condition selected (highlighted with a red box)</li></ul> <p>Access controls</p> <ul style="list-style-type: none"><li>Grant: Block access (highlighted with a red box)</li></ul> | <p>Info</p> <p>Device platforms: Not configured</p> <p>Locations: Not configured</p> <p>Client apps (preview): 1 included (highlighted with a red box)</p> <p>Device state (preview): Not configured</p> | <p>Configure Yes No</p> <p>Select the client apps this policy will apply to</p> <ul style="list-style-type: none"><li>Browser (unchecked)</li><li>Mobile apps and desktop clients (checked)</li><li>Modern authentication clients (unchecked)</li><li>Exchange ActiveSync clients (unchecked)</li><li>Other clients (checked)</li></ul> |

### 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.

The screenshot shows the 'Conditional Access - Policies' section. A specific policy named 'Block Exchange ActiveSync clients' is selected. On the right, the 'Cloud apps or actions' configuration pane is open. It allows selecting what the policy applies to ('Cloud apps' or 'User actions'), choosing between 'Include' and 'Exclude' logic, and selecting specific apps ('None', 'All cloud apps', or 'Select apps'). Under 'Select apps', 'Office 365 Exchange Online' is listed, along with a thumbnail for 'Office 365 Exchange Onli...'. The left sidebar shows other policy sections like 'Assignments' and 'Conditions'.

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

The screenshot shows the 'Conditions' section with various configuration options like 'Sign-in risk', 'Device platforms', 'Locations', and 'Client apps (preview)'. The 'Client apps (preview)' section is selected and expanded. On the right, the 'Client apps (preview)' configuration pane is open. It includes a 'Configure' section with 'Yes' selected, followed by a list of client types to apply the policy to. The 'Mobile apps and desktop clients' and 'Exchange ActiveSync clients' checkboxes are checked, while others like 'Browser', 'Modern authentication clients', and 'Apply policy only to supported platforms' are unchecked.

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

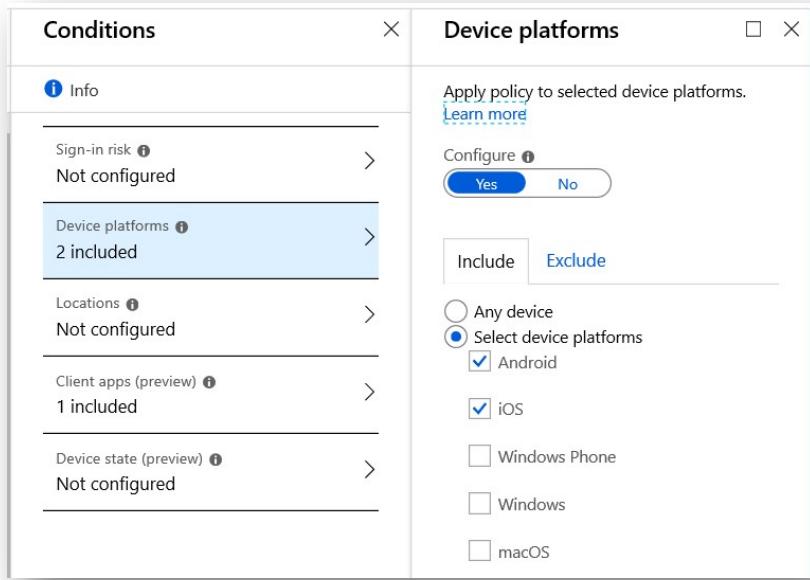
The screenshot shows two windows side-by-side. On the left is a policy configuration window titled 'Block ActiveSync clients'. It has sections for 'Info', 'Delete', 'Name' (set to 'Block Exchange ActiveSync clients'), 'Assignments' (targeted at 'All users'), 'Cloud apps or actions' (containing '1 app included'), and 'Conditions' (containing '1 condition selected'). Under 'Access controls', 'Block access' is selected. On the right is a 'Grant' dialog box titled 'Select the controls to be enforced'. It contains a radio button for 'Block access' (which is selected) and another for 'Grant access'. Below these are several optional controls: 'Require multi-factor authentication', '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'), 'Require app protection policy (preview)' (with a link to 'See list of policy protected client apps'), and two radio buttons for 'For multiple controls': 'Require all the selected controls' and '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.

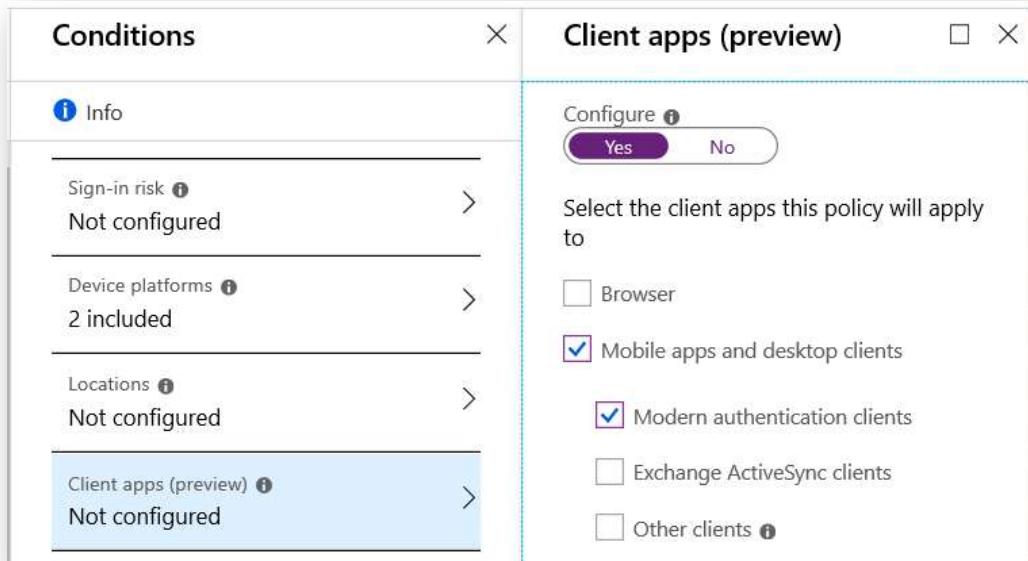
#### Require approved apps for mobile devices (iOS & Android)

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.



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 approved app (iOS and Android)**

**Grant**

Select the controls to be enforced.

Block access  
 Grant access

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

For multiple controls

Require all the selected controls  
 Require one of the selected controls

**Assignments**

- Users and groups i > All users
- Cloud apps or actions i > 2 apps included
- Conditions i > 2 conditions selected

**Access controls**

- Grant i > 1 control selected

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

**Conditions**

**Device platforms**

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

Configure i  
 Yes  No

**Include** **Exclude**

Any device  
 Select device platforms

- Android
- iOS
- Windows Phone
- Windows
- macOS

- Sign-in risk i > Not configured
- Device platforms i > Not configured
- Locations i > Not configured
- Client apps (preview) i > Not configured
- Device state (preview) i > Not configured

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

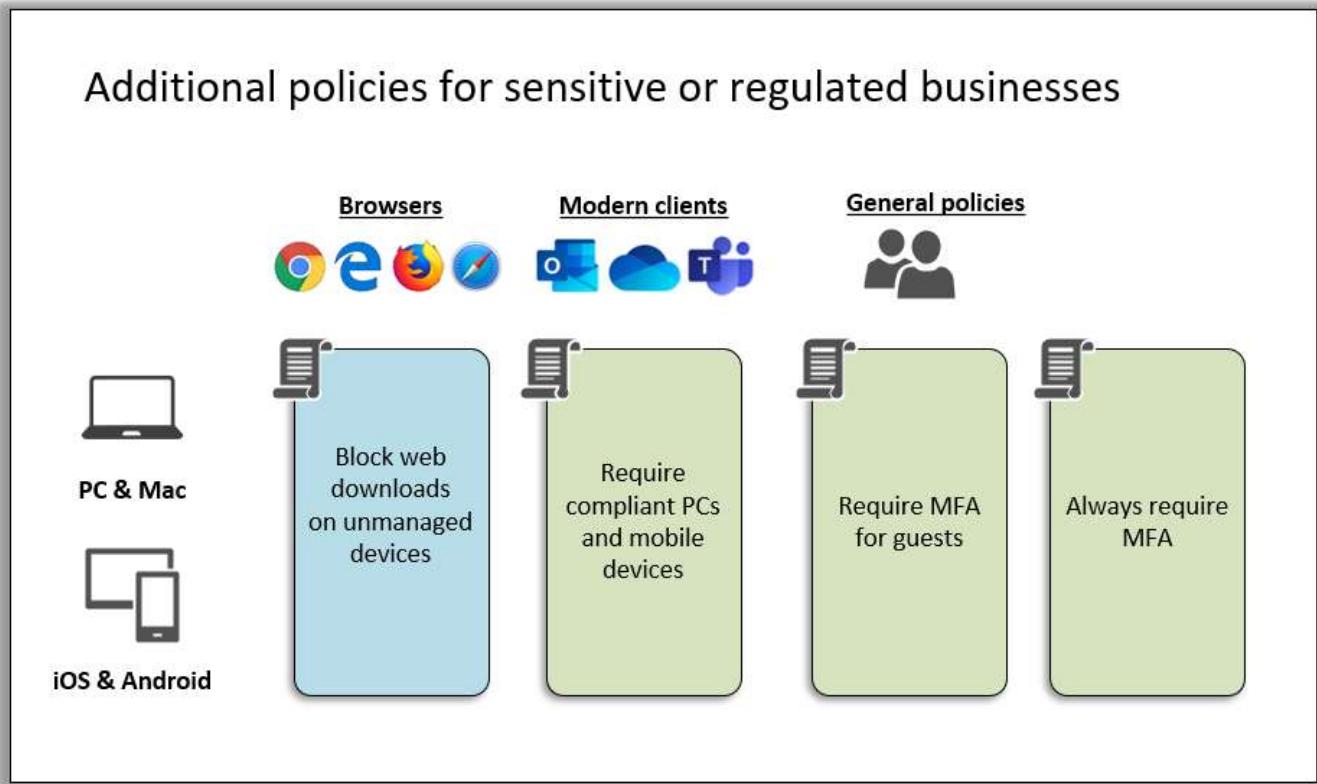
The screenshot shows two windows side-by-side. The left window is titled 'Conditions' and lists four items: 'Sign-in risk', 'Device platforms', 'Locations', and 'Client apps (preview)'. The 'Client apps (preview)' item is selected and highlighted in blue. The right window is titled 'Client apps (preview)' and contains a 'Configure' button with 'Yes' and 'No' options. Below it is a section titled 'Select the client apps this policy will apply to' with four 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 screenshot shows the 'Grant' access control configuration dialog. It has a 'Info' section with a name field containing 'Require compliant device (PC & Mac)' with a green checkmark. Below it are sections for 'Assignments' (with 'All users'), 'Cloud apps or actions' (with '2 apps included'), and 'Conditions' (with '2 conditions selected'). Under 'Access controls', there is a 'Grant' section with '0 controls selected'. On the right, the 'Grant' section is expanded, showing a radio button for 'Block access' (unchecked) and 'Grant access' (checked). A list of controls follows: '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), 'See list of approved client apps' (link), 'Require app protection policy (preview)' (unchecked), 'See list of policy protected client apps' (link), and 'For multiple controls' with radio buttons for '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                                      |
|---|---|--|---|
| 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    |

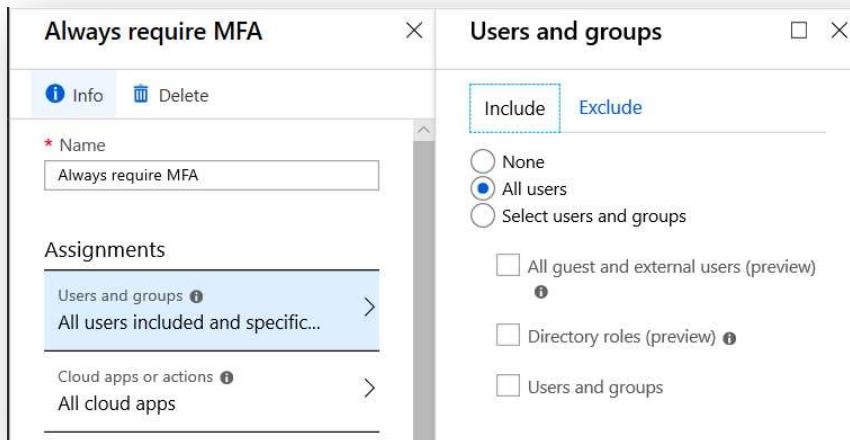
The following table describes how to build out the policies.

| Conditional access policy                | Assignments  | Conditions  | Access Control   |
|--|--|---|--|
| Always require MFA                       | <b>Users:</b> All users<br><b>Apps:</b> All cloud apps                     | <b>None</b>                                       | <b>Grant access:</b><br>Require multi-factor authentication      |
| Require MFA for guests                   | <b>Users:</b> All guest and external users<br><b>Apps:</b> All cloud apps  | <b>None</b>                                       | <b>Grant access:</b><br>Require multi-factor authentication      |
| Require compliant PCs and mobile devices | <b>Users:</b> All users<br><b>Apps:</b> All cloud apps                     | <b>Client apps:</b> Modern authentication clients | <b>Grant access:</b><br>Require device to be marked as compliant |
| Block downloads on unmanaged devices     | <b>Users:</b> All users<br><b>Apps:</b> Exchange Online, SharePoint Online | <b>Client apps:</b> Browser                       | <b>Session:</b><br>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**.

The screenshot shows the 'Always require MFA' policy configuration. On the left, under 'Assignments', 'Users and groups' is selected, showing 'All users included and specific...'. Under 'Access controls', 'Grant' is selected, showing '1 control selected'. A modal window titled 'Grant' is open, prompting to 'Select the controls to be enforced'. It offers two options: 'Block access' (radio button) and 'Grant access' (radio button, selected). Below these are several checkboxes for controls: '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'), 'Require app protection policy (preview)' (with a link to 'See list of policy protected client apps'), 'Require all the selected controls' (radio button), and 'Require one of the selected controls' (radio button, selected).

## 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**.

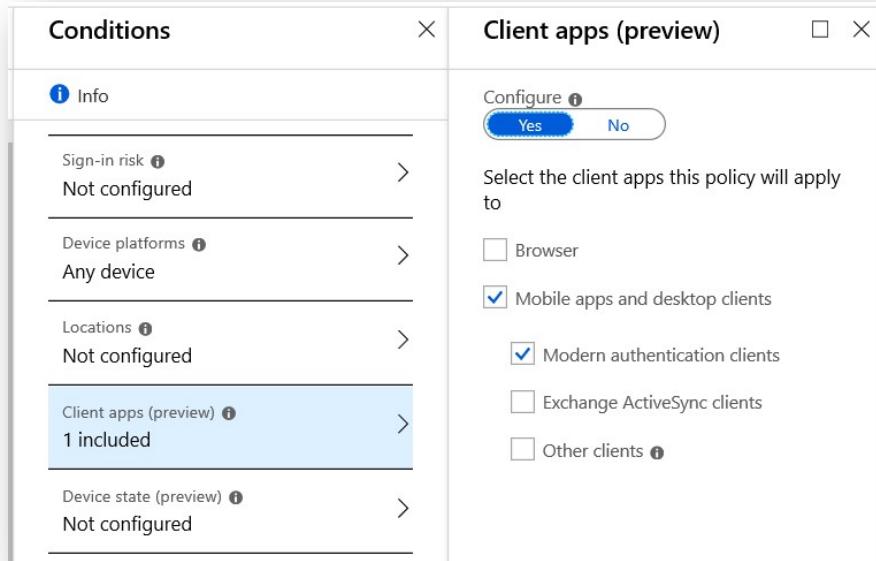
The screenshot shows the 'ALLOW - Require MFA for guests' policy configuration. Under 'Assignments', 'Users and groups' is selected, showing 'Specific users included'. Under 'Access controls', 'Grant' is selected, showing '1 control selected'. A modal window titled 'Users and groups' is open, showing the 'Exclude' tab selected. It offers three options: 'None', 'All users', and 'Select users and groups' (selected). Below these are checkboxes for 'All guest and external users (preview)' (checked), 'Directory roles (preview)', and '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**.



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

The screenshot shows the 'Grant' configuration dialog for a policy named 'Block unmanaged devices'. The 'Grant' tab is selected, showing options to 'Select the controls to be enforced'. The 'Grant access' radio button is selected. Under 'For multiple controls', the 'Require one of the selected controls' radio button is selected. Other options listed include 'Block access', 'Require multi-factor authentication', 'Require device to be marked as compliant' (which is checked), '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 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.

The screenshot shows the 'Cloud apps or actions' policy configuration screen. At the top, it says 'Select what this policy applies to' with tabs for 'Cloud apps' (selected) and 'User actions'. Below that are 'Include' and 'Exclude' buttons. Under 'Include', the 'Select apps' option is selected. A list of apps follows, with 'Office 365 SharePoint Online a...' and 'Office 365 Exchange O...' visible. The left sidebar shows the policy's structure: 'Name' is 'Block downloads on unmanaged devices'; 'Assignments' includes 'All users' and 'Cloud apps or actions' (which is currently selected); 'Conditions' shows '1 condition selected'; and 'Access controls' is listed.

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

The screenshot shows the 'Client apps (preview)' policy configuration screen. It has a 'Configure' button with 'Yes' (selected) and 'No' options. Below it, it says 'Select the client apps this policy will apply to' with a checked checkbox for 'Browser' and an unchecked checkbox for 'Mobile apps and desktop clients'. The left sidebar shows the policy's structure: 'Conditions' includes 'Sign-in risk', 'Device platforms', and 'Locations'; 'Client apps (preview)' is selected and shows '1 included'.

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

The screenshot shows the 'Block downloads on unmanaged devices' policy in the Microsoft Conditional Access portal. On the left, under 'Assignments', there are sections for 'Users and groups', 'Cloud apps or actions', and 'Conditions'. Under 'Access controls', there is a 'Grant' section and a 'Session' section which is currently selected. In the 'Session' tab on the right, it says: 'Session controls enable limited experiences within a cloud app. Select the session usage requirements.' Below this, there are four checkboxes: 'Use app enforced restrictions' (checked), 'Use Conditional Access App Control', 'Sign-in frequency (preview)', and 'Persistent browser session (preview)'. The 'Use app enforced restrictions' checkbox is checked.

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\alexfr> Get-OwaMailboxPolicy | fl Name,ConditionalAccessPolicy

Name          : OwaMailboxPolicy-Default
ConditionalAccessPolicy : off

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

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

## Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows the following command sequence:

```
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.