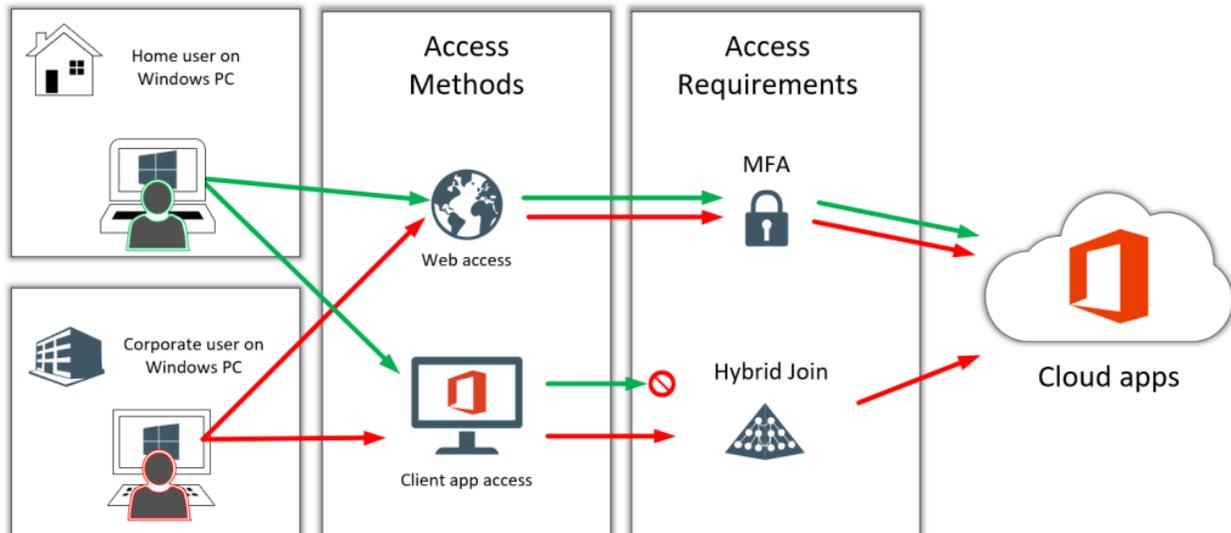


Boost your security with Hybrid Azure AD Join: From Zero to Conditional Access in one afternoon



"Alex, I work at a non-profit and I would love to take advantage of the better security in Microsoft 365 Business (we have Business Premium now), but it sounds like it is for "cloud-only" customers? Is that right?? We are using Office 365 for Exchange, but we can't go cloud-only with Active Directory and files because our vendor does not support their application in the cloud (has to be on LAN) [...] Do you recommend EM+S instead? ATP? [...] Also, how hard is it to do conditional access for hybrid??" Thanks, Gaylae

Good questions, Gaylae (not sure if I should pronounce that Gay-lay, or Gay-lee??), but in any event, I can tell you: Microsoft 365 Business **fully supports** hybrid environments, so you do not need to piecemeal your own SKU together. And have no fear, configuring Conditional Access for a hybrid environment is going to be a snap—I'll show you today!

Just because you are "stuck" on-premises doesn't mean you can't take advantage of what the cloud has to offer. Indeed, most small businesses have already made the move to services like Exchange Online, and are using the cloud for at least *some* of their critical workloads. File shares will most likely be the next mass exodus. But you can also start migrating your endpoint management & security operations into the cloud at any time—it's easier than you might think!

In this post I will demonstrate how simple it is to get your small or mid-sized organization connected to Azure Active Directory in order to enable strong security policies that will help prevent data leakage and unauthorized access to company data and resources.

Pre-requisite

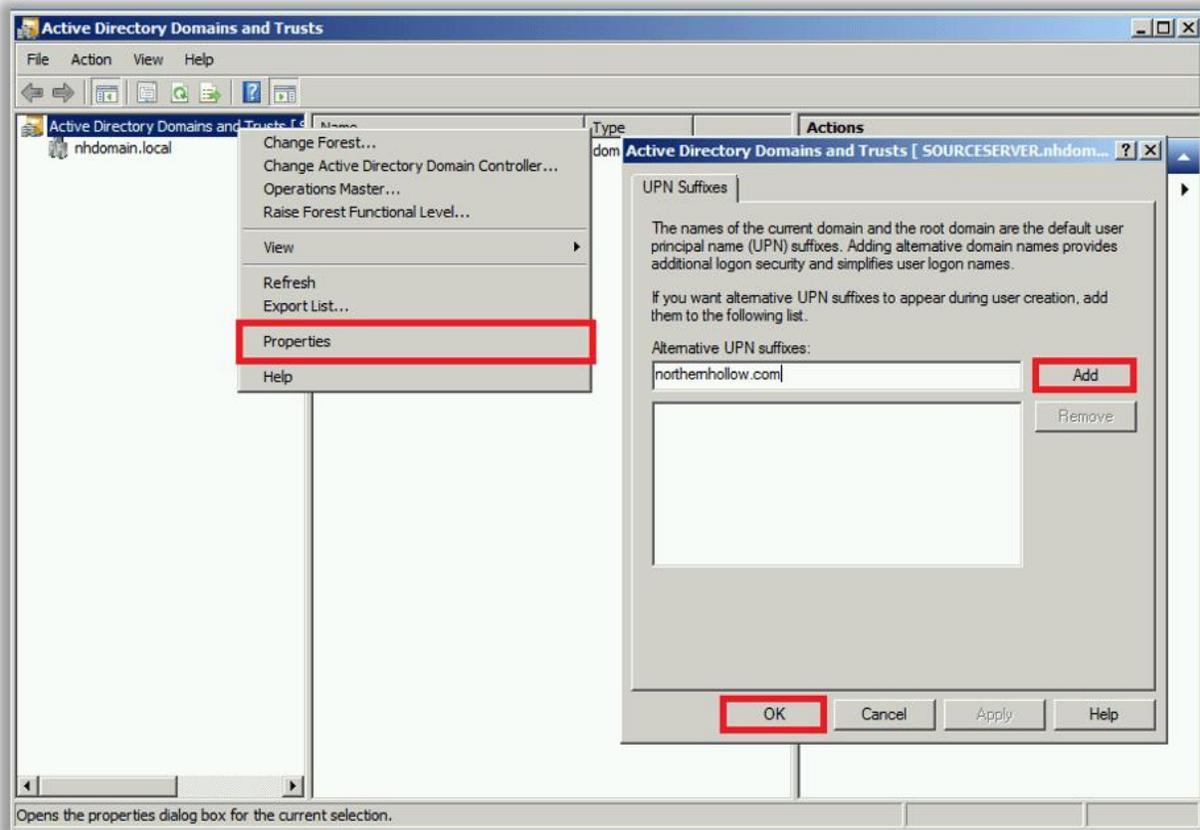
As Gaylae has noted, you will first of all need a subscription that supports Conditional Access. For the small and mid-sized business (under 300 seats) I recommend **Microsoft 365 Business**. Otherwise **Microsoft 365 Enterprise**, or the **Enterprise Mobility + Security** bundles will accomplish the same.

Step 1. Prepare for Azure AD Connect

If you already have synchronized your identities to Azure Active Directory you can skip this step and the next one. Some small orgs do have existing hybrid environments, while others may need to establish it.

Now especially in the SMB market, domains on-premises often have a ".local" or ".lan" suffix instead of something Internet-routable like ".com" or ".org." Non-routable domains are meaningless in the cloud, so this is the first thing we have to fix, and it's really easy to do. You can follow [this article from Microsoft](#).

Estimated time to complete: 15 minutes.

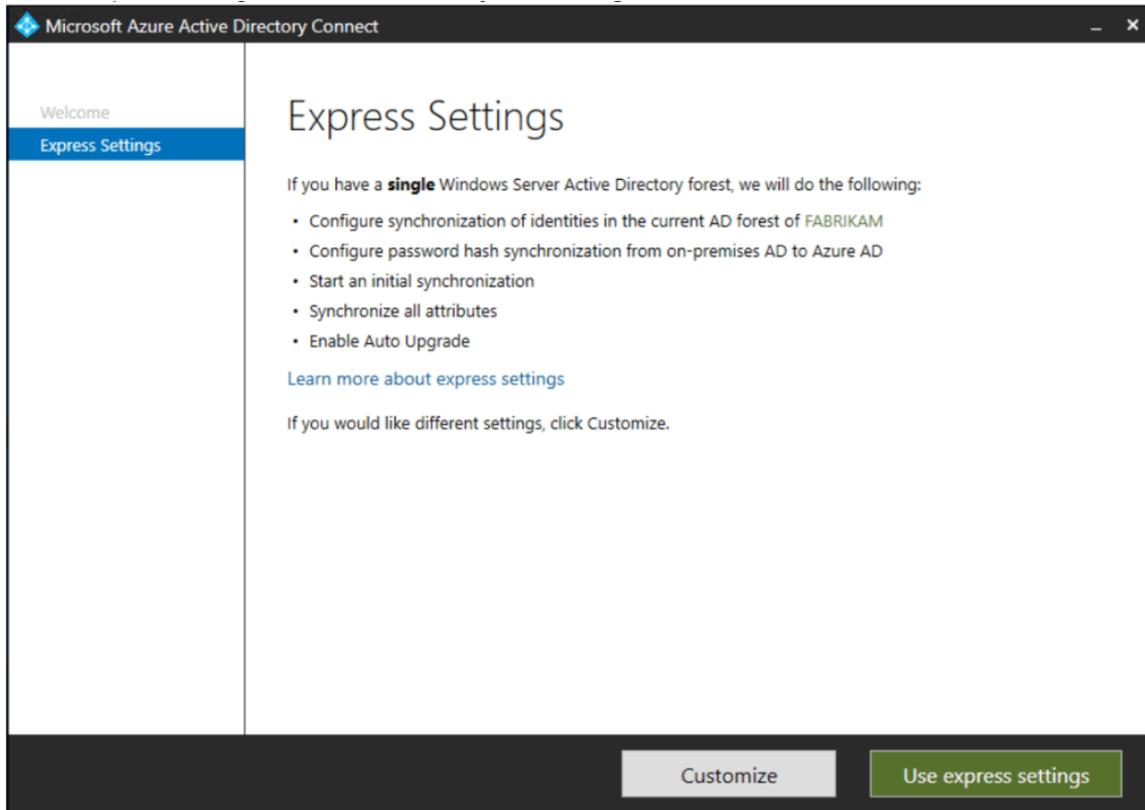


As well, you may need to import alias addresses that you have in Exchange Online. This means you need to have an on-premises Exchange Server in order to edit certain attributes that are specific to Exchange email. I have [written about this before](#), but just keep this in mind—if you have to install Exchange and add back the attributes, it can add 1-2 hours to your mini-project.

Step 2. Install Azure AD Connect

The next step is installing [Azure AD Connect](#); most small and mid-sized orgs will do just fine with the [Express installation](#). However, you can do a [Custom](#) installation if you want to constrain the scope of your synchronization to specific OU's, etc.—technically you only need to sync your active users and computers—I would not bring any distribution or security groups into the cloud as those are better managed using Office 365 Groups instead (which are cloud-only objects).

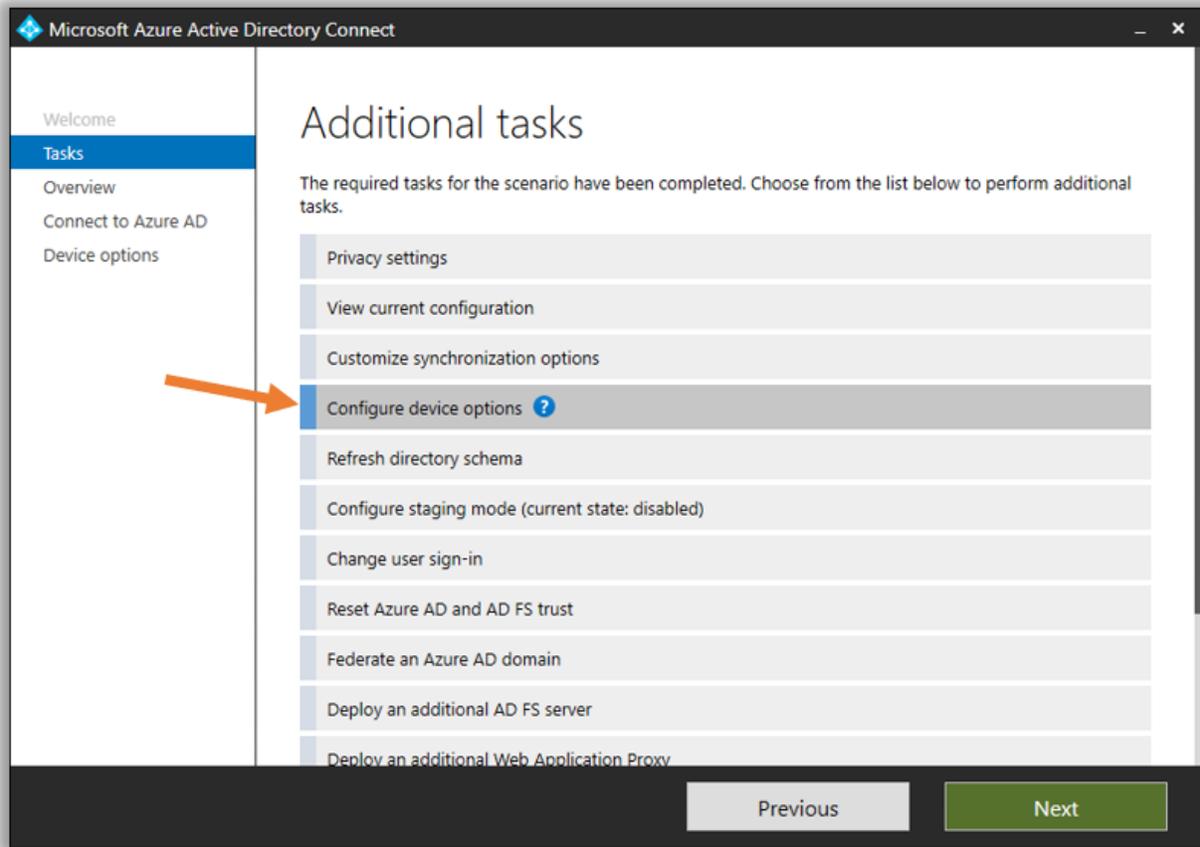
Estimated time to complete: 15 minutes



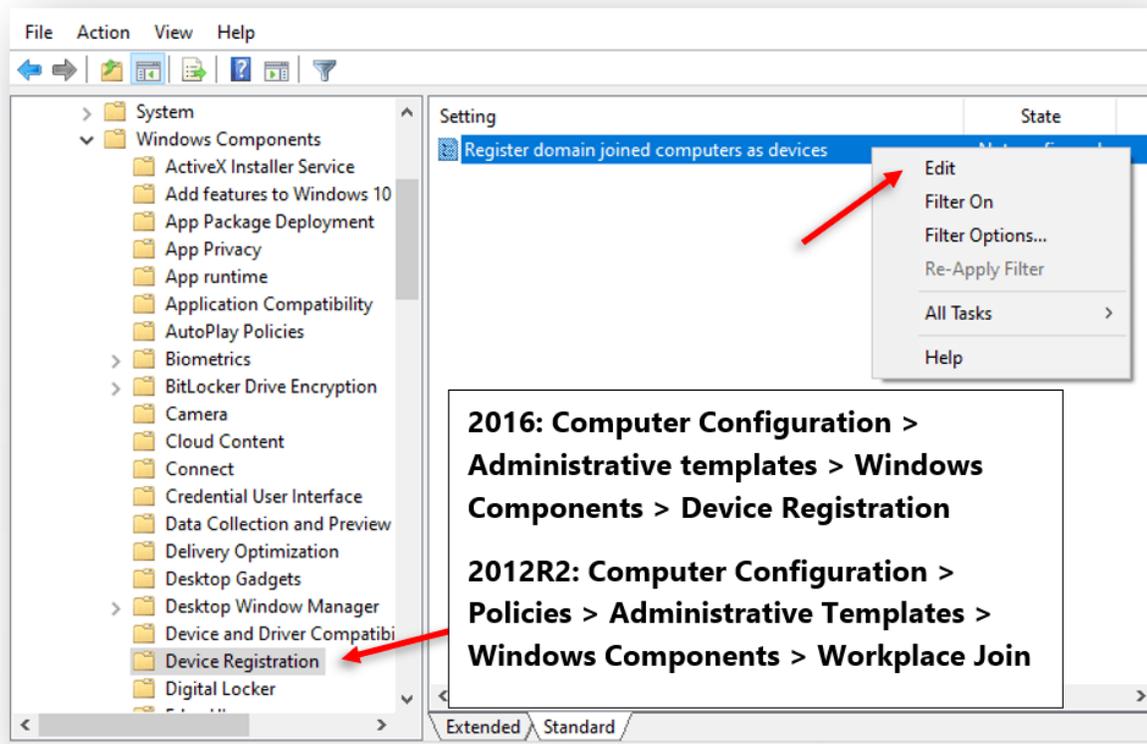
Step 3. Configure Hybrid Azure AD Join

Completing Hybrid Azure AD Join requires you to perform two more steps on-premises:

1. [Configure the SCP via Azure AD Connect](#), and
2. [Create a GPO to auto-register domain-joined computers](#)



Stepping through the wizard and deploying the GPO only takes a few clicks.



Optionally, you can also [deploy a GPO that will auto-enroll devices](#) with Microsoft Endpoint Manager (Intune). This extra step would allow you to put other policies against the domain-joined devices using MDM rather than GPO, but it is not a requirement to get Conditional Access working for Hybrid Azure AD Join.

Estimated time to complete: 20 minutes, although you may have to wait a while for all your domain-joined computers to get the new policy and be recognized as Hybrid Azure AD Joined machines in the cloud.

Step 4. Set up your Conditional Access policies

At this stage the cloud is now aware of the difference between Windows 10 devices that are joined to your corporate domain, and those which are not. That means you can decide to limit access on non-corporate computers in various ways.

For example, perhaps your organization would like to allow web access from home PC's or personal laptops (as long as the user can pass an MFA challenge), but they would like to limit or block the ability to use thick client apps such as Outlook, Word and OneDrive, which can sync and cache company data on the local device.

To make this happen, create two policies: one for web access, and another for modern client access.

Estimated time to complete: 15 minutes.

Browser access: Require MFA

Go to **Azure AD > Security > Conditional Access**. Create a new policy:

- Name it **GRANT – Windows 10 Browser access**.
- Select **All users** and exclude at least one [emergency access account](#).
- Select the apps you want to protect for example **Office 365** (includes apps like Exchange, SharePoint, Teams, etc.)

center Alex@itpromentor.com
ITPROMENTOR.COM

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

New

Info

Name *
GRANT - Windows 10 Browser access ✓

Assignments

- Users and groups ①
All users included and specific... >
- Cloud apps or actions ①
No cloud apps or actions sele... >
- Conditions ①
0 conditions selected >
- Access controls

 - Grant ①
0 controls selected >
 - Session ①
0 controls selected >

Create

Cloud apps or actions

Select what this policy applies to

Cloud apps User actions

Include Exclude

None
 All cloud apps
 Select apps

Select
None >

Done

Select

Cloud apps

Applications ①
Office 365 ✓

- Office 365 (preview) ①
- Office 365 Exchange Online
- Office 365 SharePoint Online
- Office 365 Yammer

Selected
Office 365 (preview) >

Select

Select **Conditions**:

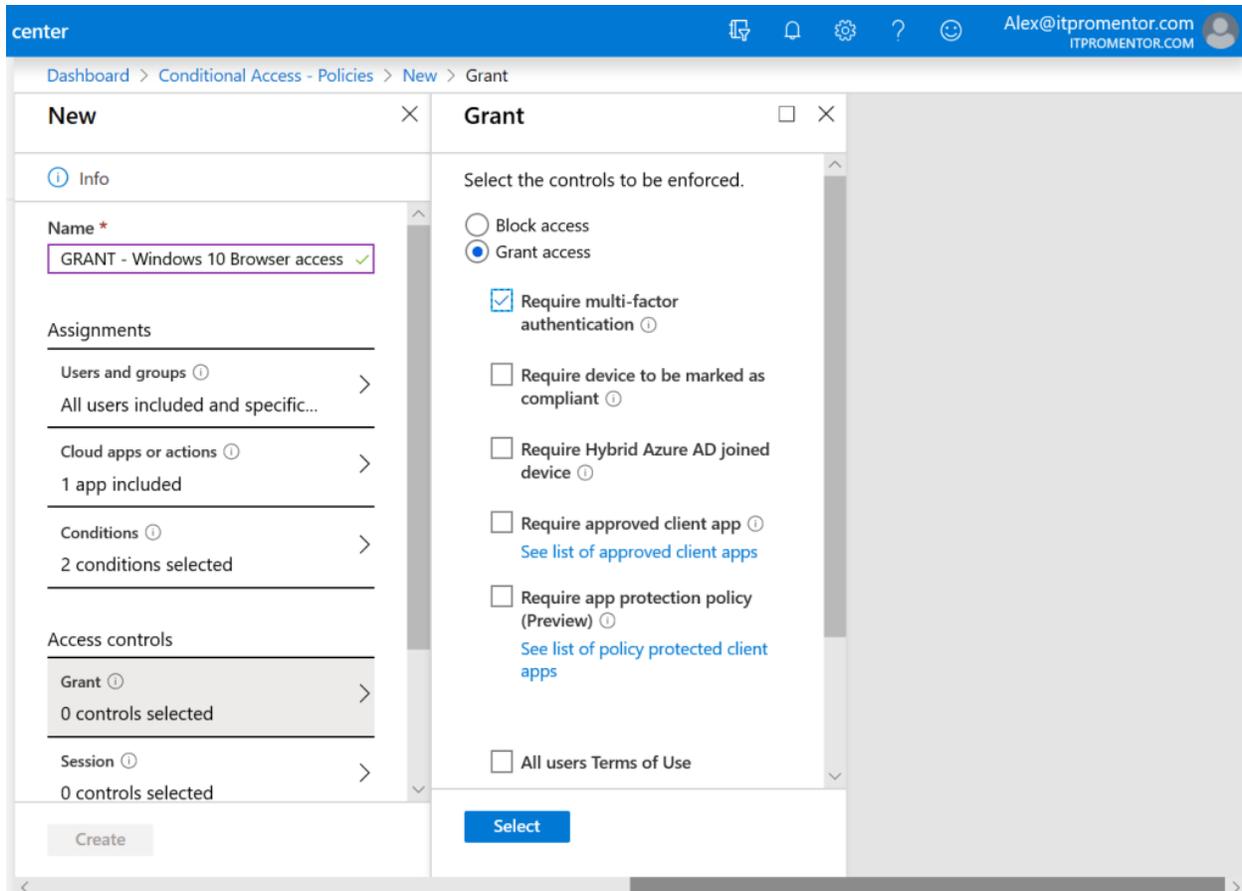
- Under **Device platforms** select only the **Windows** option
- Select **Client apps** and choose only the **Browser** option.

center Alex@itpromentor.com
ITPROMENTOR.COM

Dashboard > Conditional Access - Policies > New > Conditions > Client apps (Preview)

New	Conditions	Client apps (Preview)
<p>Info</p> <p>Name *</p> <p>GRANT - Windows 10 Browser access ✓</p> <p>Assignments</p> <p>Users and groups ① ></p> <p>All users included and specific...</p> <p>Cloud apps or actions ① ></p> <p>1 app included</p> <p>Conditions ① ></p> <p>0 conditions selected</p> <p>Access controls</p> <p>Grant ① ></p> <p>0 controls selected</p> <p>Session ① ></p> <p>0 controls selected</p> <p>Create</p>	<p>Info</p> <p>Sign-in risk ① ></p> <p>Not configured</p> <p>Device platforms ① ></p> <p>1 included</p> <p>Locations ① ></p> <p>Not configured</p> <p>Client apps (Preview) ① ></p> <p>Not configured</p> <p>Device state (Preview) ① ></p> <p>Not configured</p> <p>Done</p>	<p>Configure ①</p> <p>Yes No</p> <p>Select the client apps this policy will apply to</p> <p><input checked="" type="checkbox"/> Browser</p> <p><input type="checkbox"/> Mobile apps and desktop clients</p> <p>Advanced</p> <p>Done</p>

Under Access controls > Grant pick **Require Multi-factor Authentication**.



Create and **Enable** the policy when you're ready. Users will be required to register for MFA and complete the MFA challenge moving forward, when accessing Office 365 apps on the web.

Windows 10 client access: Require Hybrid Azure AD Joined device

Complete the same steps to begin building your policy, naming it **GRANT – Windows 10 client app access**, then selecting the same users and apps as before.

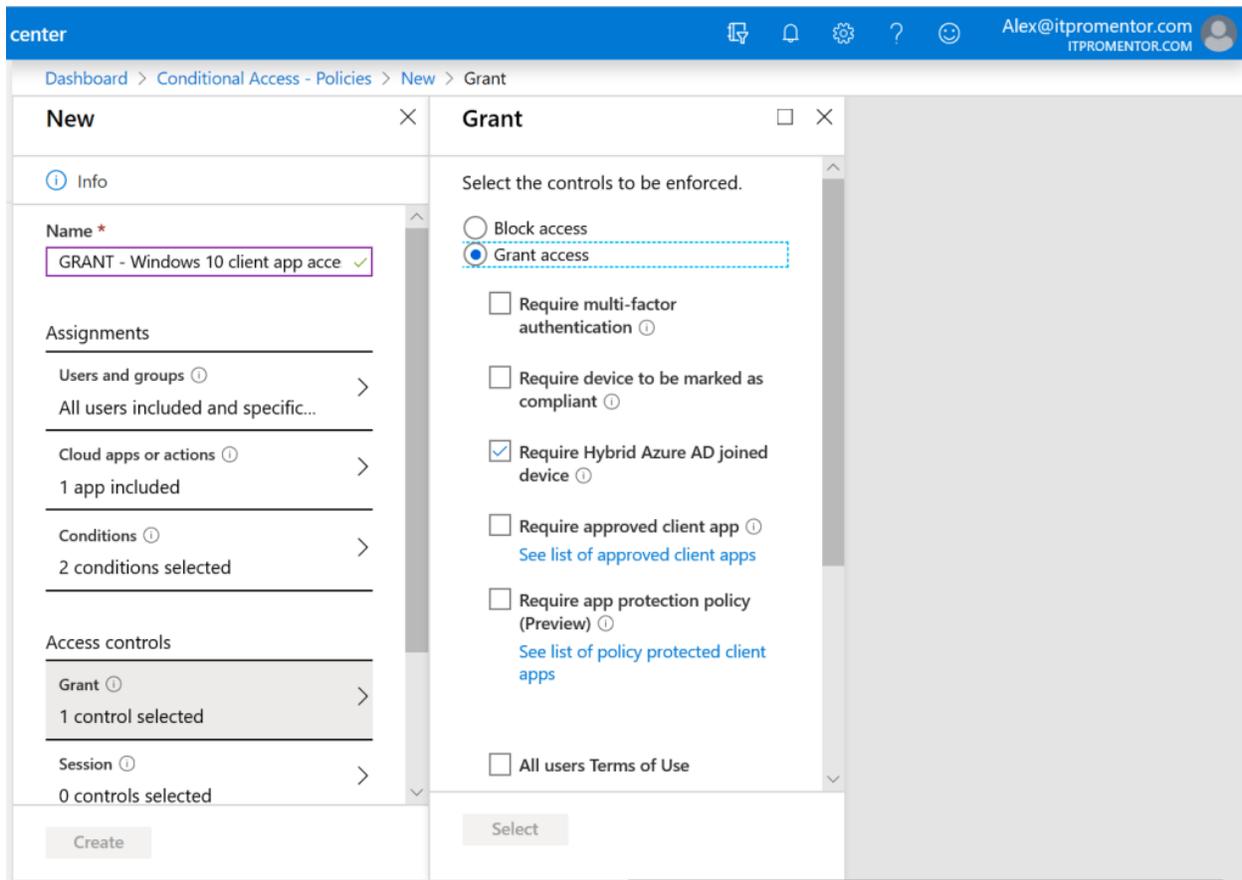
Then under **Conditions**, again selecting **Windows 10** as the **Device platform**, this time target **Client apps > Mobile apps and desktop clients > Modern authentication clients**.

center Alex@itpromentor.com ITPROMENTOR.COM

Dashboard > Conditional Access - Policies > New > Conditions > Client apps (Preview)

New	Conditions	Client apps (Preview)
<p>Info</p> <p>Name *</p> <p>GRANT - Windows 10 client app acce ✓</p> <p>Assignments</p> <p>Users and groups ⓘ All users included and specific... ></p> <p>Cloud apps or actions ⓘ 1 app included ></p> <p>Conditions ⓘ 2 conditions selected ></p> <p>Access controls</p> <p>Grant ⓘ 1 control selected ></p> <p>Session ⓘ 0 controls selected ></p> <p>Create</p>	<p>Info</p> <p>Sign-in risk ⓘ Not configured ></p> <p>Device platforms ⓘ 1 included ></p> <p>Locations ⓘ Not configured ></p> <p>Client apps (Preview) ⓘ 1 included ></p> <p>Device state (Preview) ⓘ Not configured ></p> <p>Done</p>	<p>Configure ⓘ</p> <p>Yes No</p> <p>Select the client apps this policy will apply to</p> <p><input type="checkbox"/> Browser</p> <p><input checked="" type="checkbox"/> Mobile apps and desktop clients</p> <p><input checked="" type="checkbox"/> Modern authentication clients</p> <p><input type="checkbox"/> Exchange ActiveSync clients</p> <p><input type="checkbox"/> Other clients ⓘ</p> <p>Done</p>

Moving to **Access controls**, pick **Require Hybrid Azure AD joined device**. This means non-corporate, non-domain joined PC's cannot get access to Office 365 using desktop applications.



The screenshot shows the 'New Grant' configuration page in the Azure portal. The left sidebar contains the following sections:

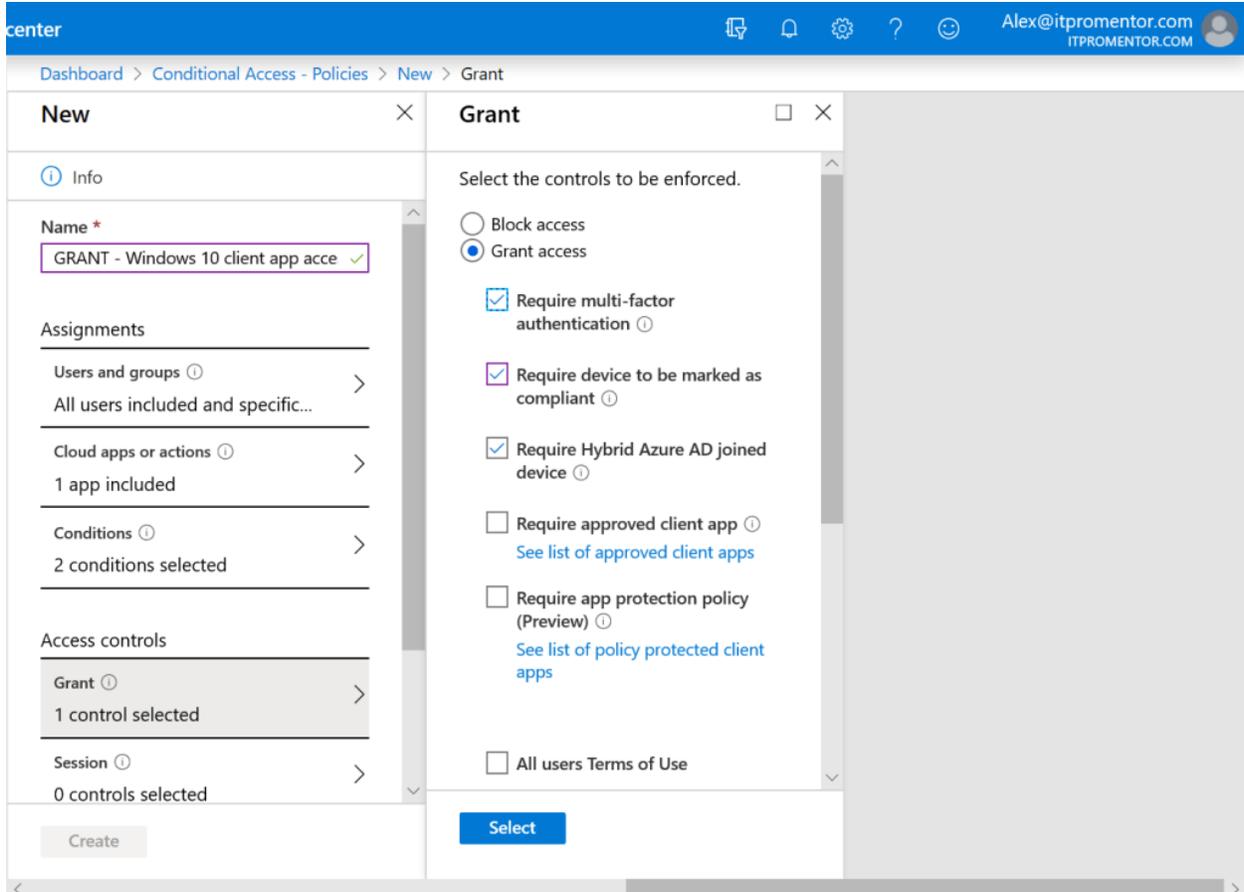
- Info:** Name * (GRANT - Windows 10 client app acce ✓)
- Assignments:**
 - Users and groups ⓘ: All users included and specific...
 - Cloud apps or actions ⓘ: 1 app included
 - Conditions ⓘ: 2 conditions selected
- Access controls:**
 - Grant ⓘ: 1 control selected
 - Session ⓘ: 0 controls selected

The main area is titled 'Grant' and contains the following controls:

- 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](#)
 - All users Terms of Use

Buttons at the bottom: 'Create' (disabled) and 'Select'.

It would be your choice whether to also require MFA for this access scenario, depending on your needs. Or you could go even further with **Require device to be marked as compliant**—for instance if you are going to be enforcing [device compliance](#) using Intune policies as well.



The controls can be as strong or as relaxed as you need them to be for each unique access scenario.

Conclusion

See, not so hard was it? Conditional Access with Microsoft 365 Business works no matter where you are at in your cloud journey.

The cloud enables you to go faster, and further, than you ever have before, and with better security than what you have been able to offer on-premises in the past.

Layering “device aware” Conditional Access rules into your security architecture is one of the primary reasons I recommend that organizations upgrade from Office 365 to Microsoft 365, whether they are hybrid or cloud-only. Once you can actually distinguish between corporate and non-corporate contexts, you can start taking advantage of some pretty amazing security controls, and you can choose just how much access personal / unmanaged devices are allowed to get.

And there is so much more—MAM policies for personal mobile devices, Office 365 ATP for better anti-phishing and anti-malware protection, Sensitivity labels, Retention labels and policies, DLP—the list goes on!

Every organization can benefit from these capabilities, especially those that work with sensitive data, or customer data that might be subject to regulations like GDPR or the new California Consumer Privacy Act. Eventually I think it is safe to say that every business is going to be responsible for better data stewardship and more compliance with laws and regulations, so it is best if you can get started as soon as possible.

And hey, Gaylae, did you know that non-profits can redeem 10 *free* licenses of Microsoft 365 Business to get started? This should be enough for you to demonstrate a Proof of Concept to management, and see if they will open the budget a tiny bit more for that upgrade from Office 365 Business Premium!



我们传递价值 | We Deliver Values

 联系我们

上海 +86 021-22065380

北京 +86 010-53605669

香港 +852 94019304