The Office 365 Email Security Checklist

By Alex Fields, ITProMentor.com

Email is the number one attack vector that bad actors use to gain access to your data. And it is no surprise; anyone who has ever run phishing tests against a large group of email recipients will be shocked to learn how many people can be so easily manipulated into clicking on something.

We can't rely on education and testing alone—we need a comprehensive approach to email security. Microsoft Office 365 has all of the bells and whistles imaginable for helping to mitigate email-based attacks, but unfortunately most of them are **not enabled by default** (and some of them require additional licensing). Therefore, it is up to you, the reader, to take the necessary steps to protect your users.

My goal is to make this workbook easy to follow—like a checklist—so that you can implement a good "baseline" level of security as you proceed through to the end.

A note about licensing

Be aware that some of the features we are going to discuss require additional subscriptions that might not be included with your base Office 365 plan. However, I am not going to recommend any additional products unless I truly believe that they are necessary or add significant value (there are quite a few "security add-ons" in the Microsoft ecosystem that will *not* be included in this workbook—and that is on purpose).

Impact on Secure Score

At the beginning of each section, I will include the Secure Score impact for implementing each item. However, you will notice that some very critical actions I have included here are not even evaluated by Secure Score, at all. Also, some actions included are not scored, or, they are "worth" far more in Secure Score points than what I think they actually add in terms of real-world value.

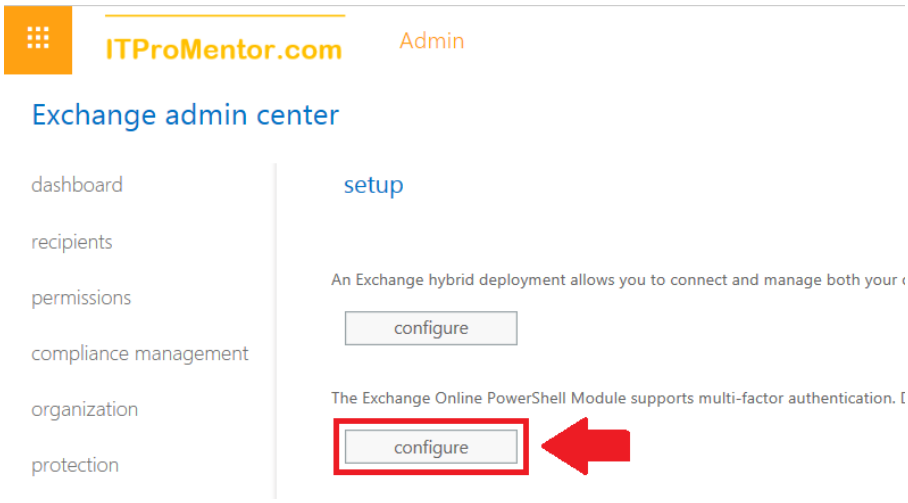
So take that tool with a grain of salt—Secure Score is as much (or more) of a sales device as it is an assessment device. Nevertheless, if you successfully implement 100% of this workbook you should easily bring your Secure Score to somewhere between 400 and 500 points.

Table of Contents

☐ Connecting to Exchange Online using PowerShell

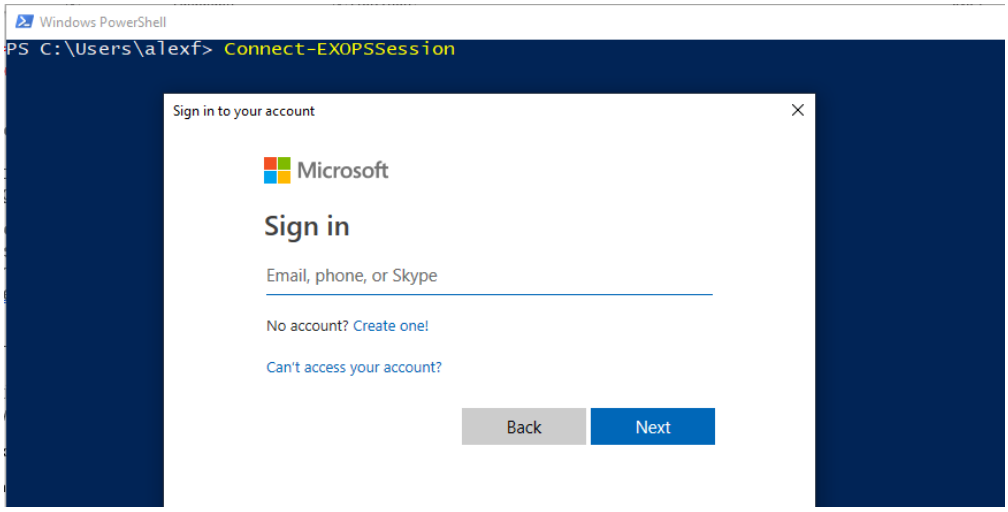
The [Exchange Online PowerShell Module] is going to make your life a lot easier.

To install the module, browse to your Exchange Online Admin Center, and navigate to **hybrid** from the left menu. Find the second button to **configure** the Exchange Online PowerShell Module (which supports MFA).



And then simply run:

```
Connect-EXOPSSession
```



Once you are connected for the first time, it may be necessary to enable organization customization (sometimes this has already been enabled via some other procedure, so if it errors out just ignore):

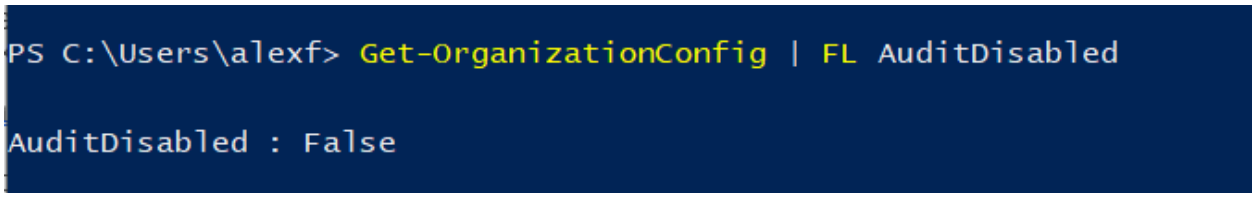
```
Enable-OrganizationCustomization
```

☐ Enable Mailbox auditing

Secure Score impact:
- Turn on audit data recording (+15)
- Turn on mailbox auditing for all users (+10)

Auditing is crucial. If there ever is a breach, you want logging enabled in order to understand what happened and when. Not to mention it is usually required for compliance with various laws and regulations. Check whether the tenant is enabled for auditing at all. Most tenants should have this enabled by default now, but even at the time of this writing, I still see instances where it is not. View the status like this (should return a value of **False** if it is enabled):

```
Get-OrganizationConfig | FL AuditDisabled
```



If it says True instead of False for some reason, and you need to change the value, simply use:

```
Set-OrganizationConfig -AuditDisabled $false
```

The other piece to this is that even if auditing is enabled globally, you still need to enable audit log search (so you can actually return data from a query against the audit logs), and on top of that, you need to enable auditing on every mailbox individually (because it's off by default).

To enable audit log search, run the command below. Note: it takes several hours before you can actually search the audit log (there is no data if auditing hasn't previously been enabled).

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

To enable auditing on all mailboxes with a log age limit of 365 days (1 year), and with audit actions enabled (including owner actions):

```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -AuditEnabled $true -AuditLogAgeLimit 365 -Audit
Admin Update, MoveToDeletedItems, SoftDelete, HardDelete, SendAs, SendOnBehalf, Create, Upda
teFolderPermission -AuditDelegate Update, SoftDelete, HardDelete, SendAs, Create, UpdateFolderP
ermissions, MoveToDeletedItems, SendOnBehalf -AuditOwner UpdateFolderPermission, MailboxLo
gin, Create, SoftDelete, HardDelete, Update, MoveToDeletedItems
```

Please note, any new mailboxes created also will not have this enabled, so it is a good idea to run the above command against any new mailbox (build this into your process).

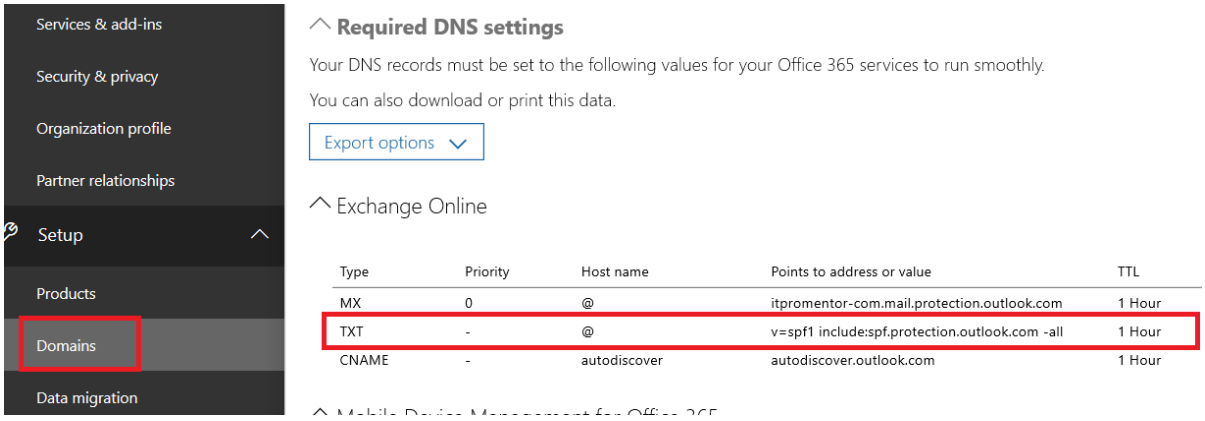
☐ Email authentication: SPF, DKIM and DMARC

Secure Score impact:
- None (which is crazy)

Email authentication is a means of using DNS records to validate or prove that your email is coming from a trusted source. Therefore, it is important that you also protect access to your DNS hosting provider, where these changes can be made. There are three record types in total that we need to configure.

☐ Sender Policy Framework

An SPF record is a DNS "TXT" type record. It is one of the records that Office 365 has you provision when you first setup and configure mail flow to Office 365. Navigate in the Microsoft 365 admin center to **Setup > Domains**.



The function of the SPF record is to advertise to the world who is allowed to send email on behalf of your domain. When you build this TXT record, you should try to include as many

"legitimate" sources of email as you can. For example, for email that is hosted at Office 365, with no other possible senders, then you only need the following:

Host name:
@ <or your domain name>

TXT value:
v=spf1 include:spf.protection.outlook.com -all

For third-party software such as Mail Chimp, Constant Contact, etc., you can usually find their SPF information using a quick Google search, or by contacting their support. For your own on-premises apps or scan to email devices, you may want to include an ip4 entry for your company's external IP addresses.

Let's say you had a combination of Office 365 for hosted email, Constant Contact for bulk mailing/marketing emails, and an on-premises copier/scanner internally, with your organization's external IP being 87.65.43.21. Then you would have this SPF to publish:

Host name:
@ <or your domain name>

TXT value:
v=spf1 include:spf.protection.outlook.com include:spf.constantcontact.com ip4:87.65.43.21 -all

☐ Domain Keys Identified Mail

DKIM is an authentication system based on an asymmetric cryptographic key pair–a private and public key. When a message leaves Office 365, it is digitally signed with the private key. The public key is published via a DNS CNAME record, so that recipient servers can validate the signature. Using this with SPF is a much stronger form of authentication, since your digital signature proves to recipient servers that individual messages really did come from the "right place."

By default, your "OnMicrosoft" domain already has DKIM configured and working. But if you are bringing a "vanity" domain name such as contoso.com (most organizations are), then you will need to setup DNS records for your domain(s), and then enable DKIM message signing in Exchange Online.

You will need to build two CNAME records per domain for DKIM. How these records are built is as follows:

Host name:
selector1._domainkey

Points to:
selector1-**CompanyDomainName-com**._domainkey.**TenantName**.onmicrosoft.com

Host name:
selector2._domainkey

Points to:
selector2-**CompanyDomainName-com**._domainkey.**TenantName**.onmicrosoft.com

Note: Under "**Points to**," the hyphenated version of your domain name that comes after selector1- or selector2- should match the domain as depicted in the MX record that is given to you by Office 365 (e.g.: **contoso-com**.mail.protection.outlook.com). So just make sure those values match. Also, the tenant name (**TenantName**.onmicrosoft.com) can be found under **Setup > Domains** in the 365 admin center.

Therefore, contoso.com looks like this:

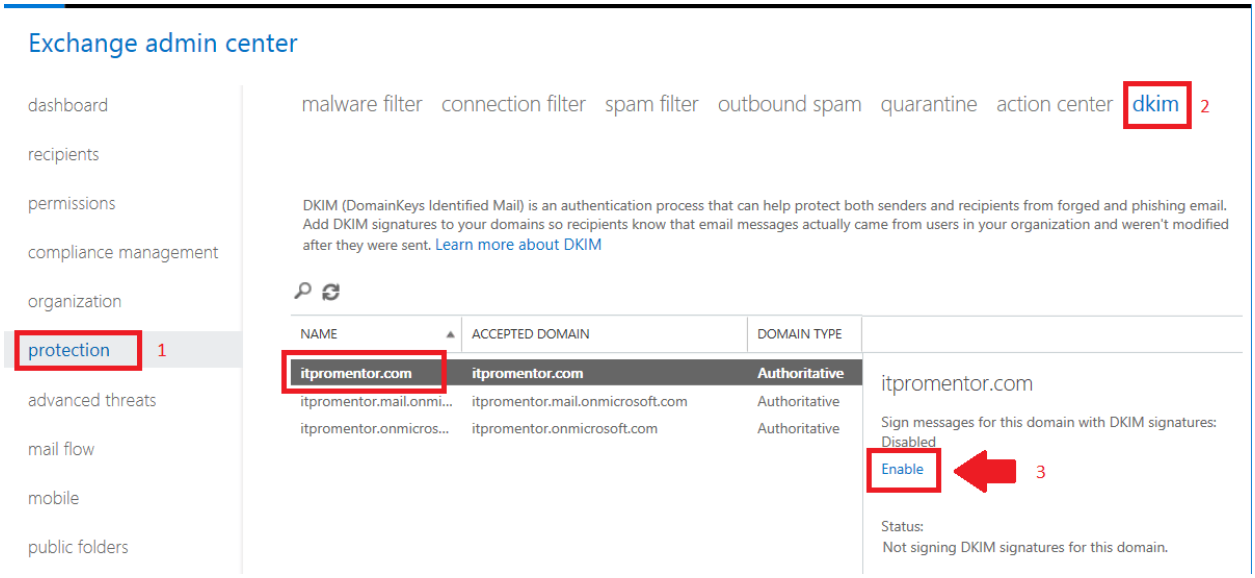
Host name: selector1._domainkey
Points to: selector1-**contoso-com**._domainkey.**contoso**.onmicrosoft.com

Host name: selector2._domainkey
Points to: selector2-**contoso-com**._domainkey.**contoso**.onmicrosoft.com

You can use PowerShell to retrieve the "Points to" value of the CNAME record (just remember that you have to specify the host names *selector1._domainkey* and *selector2._domainkey* as well, for each):

```
Get-DkimSigningConfig <DomainName.com> | fl *cname
```

Next, in the Exchange admin center, go to **protection > dkim**, pick the domain that you want to enable for DKIM signing. On the right pane, click **Enable**. If you haven't configured your DNS records, this operation will fail out, so be sure to allow enough time for DNS to propagate.



In PowerShell, this accomplished as follows (example is for contoso.com):

```
New-DkimSigningConfig -DomainName contoso.com -Enabled $true
```

NOTE: You should also have third-party senders get their DKIM information to you, so that you can add the necessary records following their direction, and have them enable signing as well.

☐ Domain-based Message Authentication, Reporting & Conformance

DMARC is a DNS record that tells recipient servers how to treat unauthenticated messages that come from your domain, based on policy. It can also communicate where to send reports about mail from your domain.

By way of example, here is what DMARC could look like for contoso.com:

```
TXT Name: _dmarc.contoso.com
Value: "v=DMARC1; p=none; ruf=mailto:spoofalert@contoso.com; fo=1"
```

Walking through the logic of the text record:

- **v=DMARC1;** = This just indicates the version (1) that is being used for DMARC
- **p=none;** = The policy is set to “none” in this case, meaning that recipient servers need take no special action on your messages if they fail authentication (you can also choose to advertise **quarantine** or **reject**)
- **ruf=mailto:<spoofalert@contoso.com>;** = this is where you can specify a place to send failure reports

- **fo=1** = this indicates that a DMARC failure report should be produced for anything other than a "pass" result on either DKIM *or* SPF; other options are **0** (report only if both mechanisms fail), **d** (DKIM failures only), or **s** (SPF failures only)

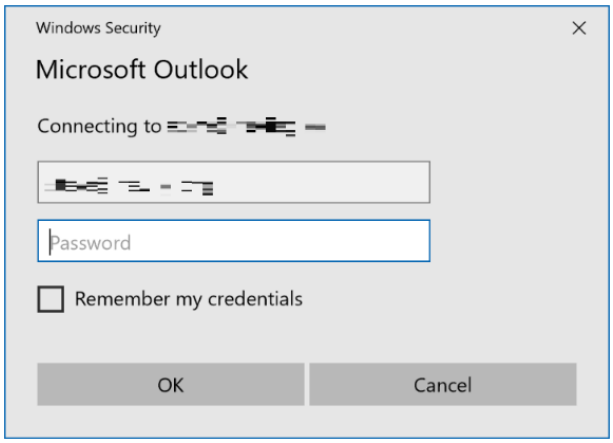
When you are first rolling DMARC out, it is best to start with the policy set to **p=none**, because this will allow you to start collecting data about messages that fail the DMARC, and take necessary actions to course-correct using SPF and DKIM *before* moving the DMARC policy up to a setting of **quarantine**, or even **reject** (the strongest setting).

The policy setting p=reject, for instance, tells recipient mail servers that they should reject (delete) all messages which fail DMARC. Much better to start out with a less restrictive policy, and monitor the results, so that you have a chance to adjust before ratcheting up.

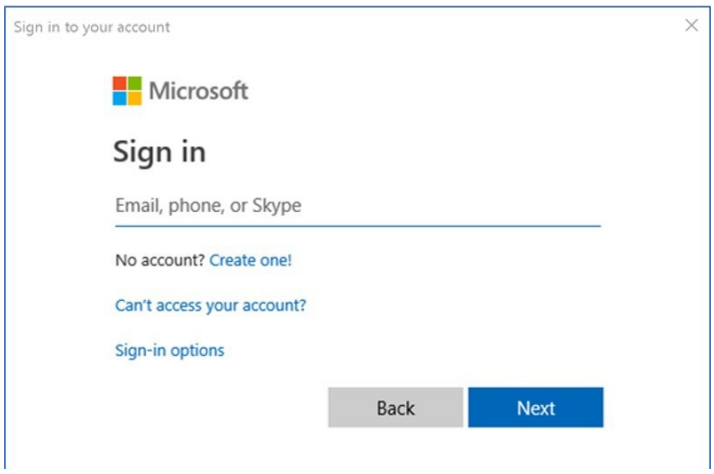
☐ Client authentication: moving from Basic to Modern auth

Secure Score impact:
- Enable policy to block legacy authentication (+20)

Modern authentication (or OAuth) is to be distinguished from Basic (or legacy) authentication. A Basic auth prompt looks like this from the client perspective:



While Modern auth prompts look more like this:



Switching to Modern auth (even without implementing MFA on top of that) is a major improvement in security. Modern authentication is not subject to the same types of attacks and exploits that are possible with Basic auth. For example, the credentials are not stored on the client device, and whenever something about the connection or state changes, the client is required to reauthenticate. Additionally, we can layer true MFA on top of modern auth to make client authentication even stronger.

Legacy clients such as Outlook 2010 are not compatible with modern auth. Even 2013 clients aren't compatible without making a modification to the registry. But my advice is to get off of Office 2013, and install the newer Office 365 bits instead. Soon 2013 clients will not be able to connect to Office 365 anyway.

☐ Enable Modern authentication

This may already be enabled for your tenant, but if not, there is no harm in running the command anyway. We can enable modern authentication for clients connecting to Exchange Online using a one-liner in PowerShell:

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```

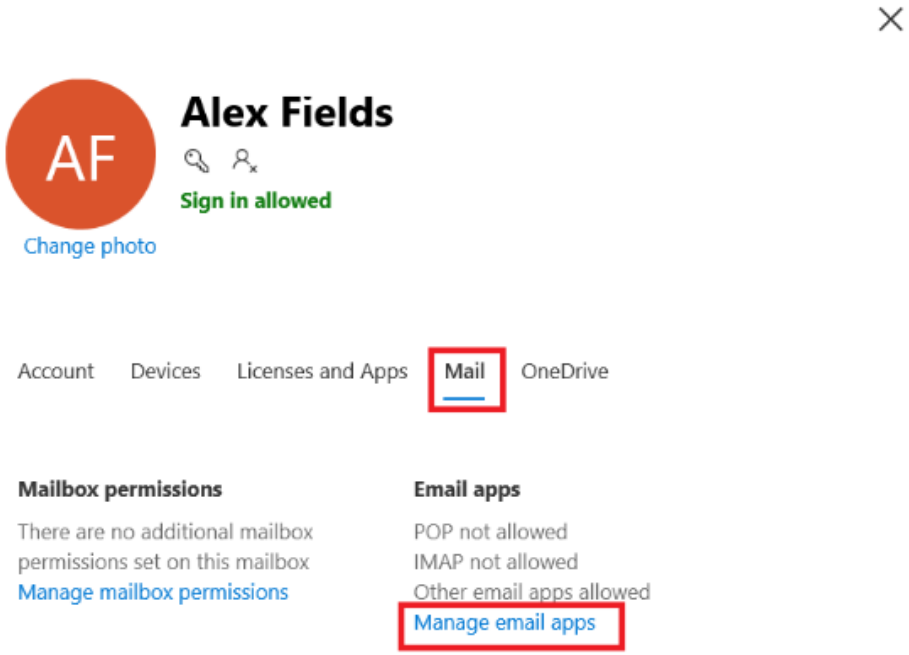
☐ Eliminate Legacy Protocols and Block Basic authentication

We have several ways of either limiting or completely eliminating the use of Basic auth and legacy protocols (e.g. IMAP and POP) which do not support Modern auth:

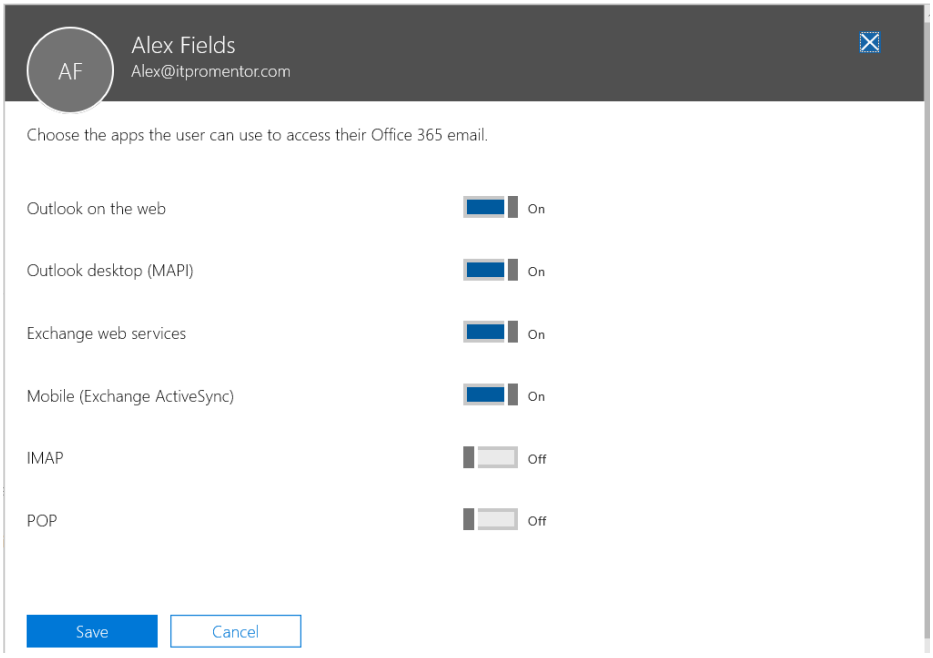
1. Disable legacy protocols such as POP, IMAP on mailboxes individually
2. Create an Authentication policy that blocks Basic authentication
3. Use a Conditional Access policy to prevent legacy clients from connecting

☐ **Option 1: Disable legacy protocols such as POP and IMAP**

This is an easy, low-risk place to start. You should try to block the use of legacy protocols (such as POP and IMAP) wherever possible. Attacks on these protocols are launched against your tenant daily. From the Microsoft 365 admin center, select a user account. Go to the "Mail" tab and select the option to **Manage email apps**.



From here it is very easy to turn off any legacy protocols that you know are not (or should not be) in use.



You can accomplish the task in bulk on all mailboxes at once as follows in PowerShell:

```
Get-Mailbox | Set-CASMailbox -PopEnabled $false -ImapEnabled $false
```

Additionally, you can use Set-CASMailboxPlan organization-wide so that newly created mailboxes will have these settings by default also.

```
Get-CASMailboxPlan | Set-CASMailboxPlan -ImapEnabled $false -PopEnabled $false
```

☐ **Option 2: Block Basic Authentication via an Authentication Policy**

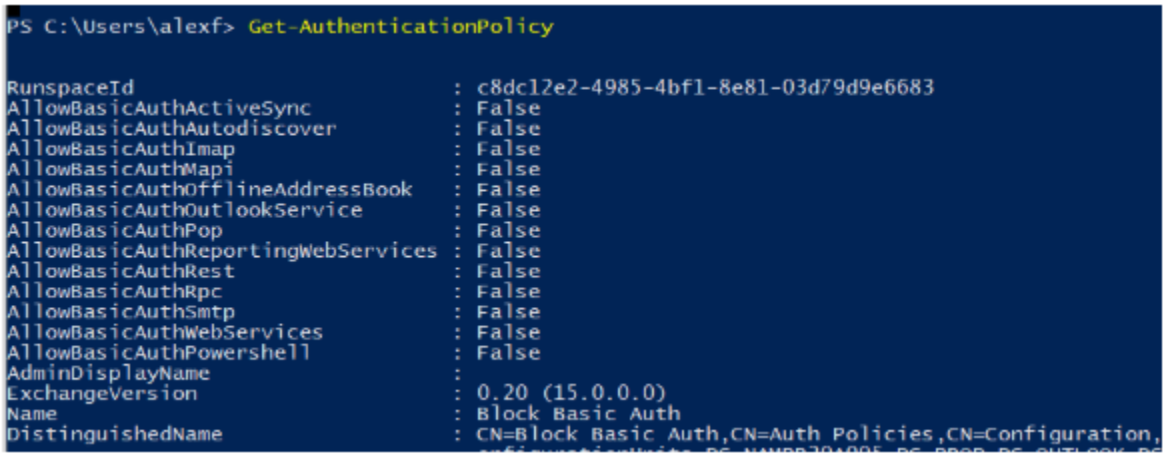
The first option only turns down the IMAP and POP services. Basic auth is still possible on any of the other services. SMTP, EWS, and more--PowerShell even. To completely eliminate basic authentication in Exchange Online, we simply have to create a new authentication policy with no additional parameters, and assign it as the default policy for the organization:

```
New-AuthenticationPolicy -Name "Block Basic Auth"
Set-OrganizationConfig -DefaultAuthenticationPolicy "Block Basic Auth"
```

NOTE: Some legacy applications or devices may be connecting to Exchange Online using basic authentication or legacy protocols. You should try to eliminate these exceptions from your environment; however, it is possible to create another authentication policy which would allow basic auth using specific protocols, and then assign the policy to users individually. Example:

```
New-AuthenticationPolicy "Allow Basic Auth Exceptions" -AllowBasicAuthImap -AllowBasicAuthWeb
Services
```

In this example, we can allow IMAP and EWS to use Basic auth, but leave it disabled for other services. You can simply Get-AuthenticationPolicy to see all of the individual services for which you can enable basic auth:



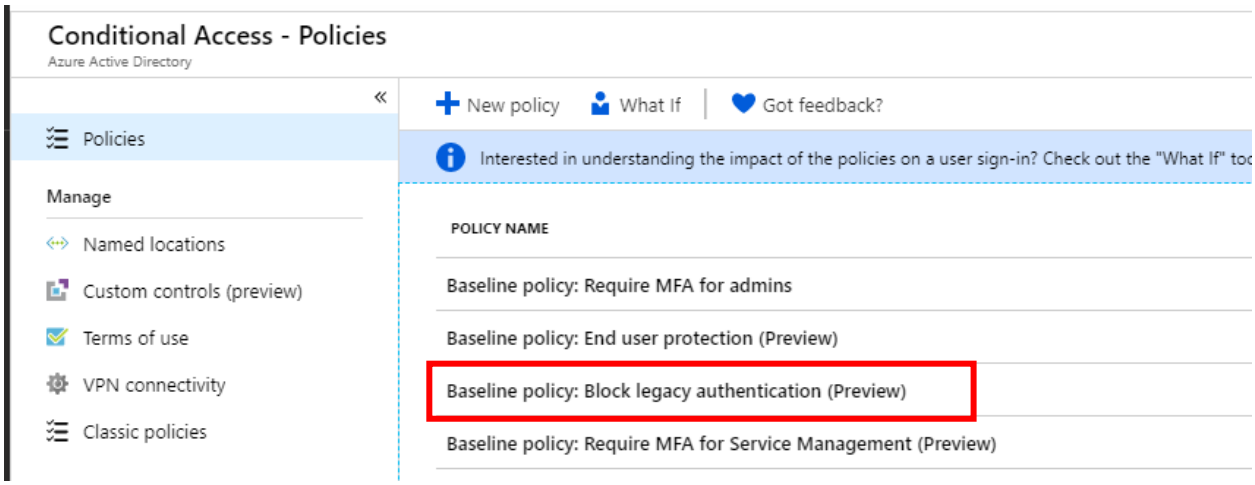
To apply the new “exception” policy to a specific user (such as a service account):

```
$ExceptionUser = “username@domain.com”
Set-User -Identity $ExceptionUser -AuthenticationPolicy "Allow Basic Auth Exceptions"
```

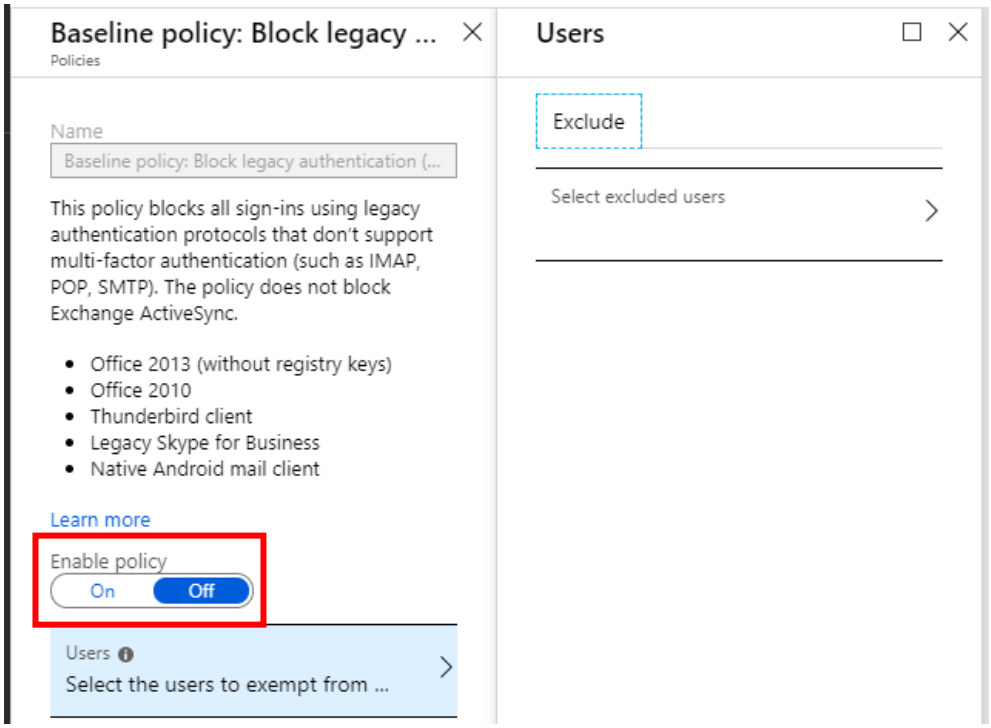
☐ **Option 3: Use Conditional Access to block legacy clients (preferred)**

Conditional access is the easiest way to block legacy authentication and protocols. This used to require Azure AD Premium, but does no longer. Now *Block legacy authentication* is included with all subscriptions as a “baseline” conditional access policy.

Navigate to Azure Active Directory and find Conditional access from the left menu. Select *Baseline policy: Block legacy authentication*.



Then you can simply **Enable** the policy, optionally selecting any users you would like to exclude from the policy (for instance, if you had a service account that relied on legacy authentication).



You can also combine this method with an Exchange Online authentication policy (after all, you might only need to open EWS or some other service for your exception, yet disable the rest).

☐ Enable Multifactor authentication (MFA)

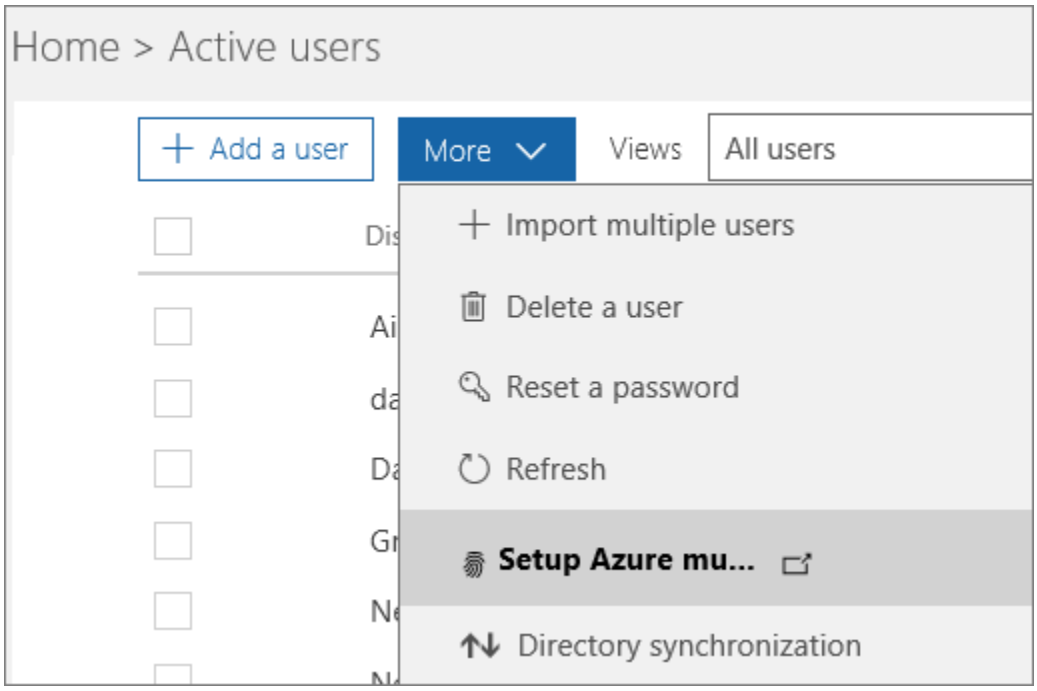
Secure Score impact:
- Require MFA for Azure AD privileged roles (+50)
- Register all users for multi-factor authentication (+20)
- Require MFA for all users (+30)

Some people think that multifactor or 2-step authentication is the silver bullet to all security ailments. Sorry, but I have bad news for you: it is not. Most MFA implementations can be bypassed, including Microsoft's. Nevertheless, it is a critical security control that should be implemented along with other controls (e.g. Conditional access). Never rely on just one strategy.

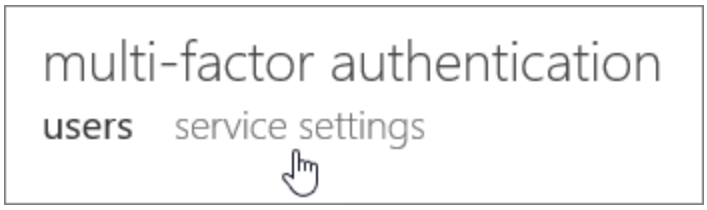
You can enable MFA on user accounts individually with any subscription. If you have the Azure AD Premium P1 subscription, you can instead enable Conditional access rules for MFA (meaning that you can choose to require an MFA challenge only under certain circumstances).

☐ Option 1. Setup MFA for users individually

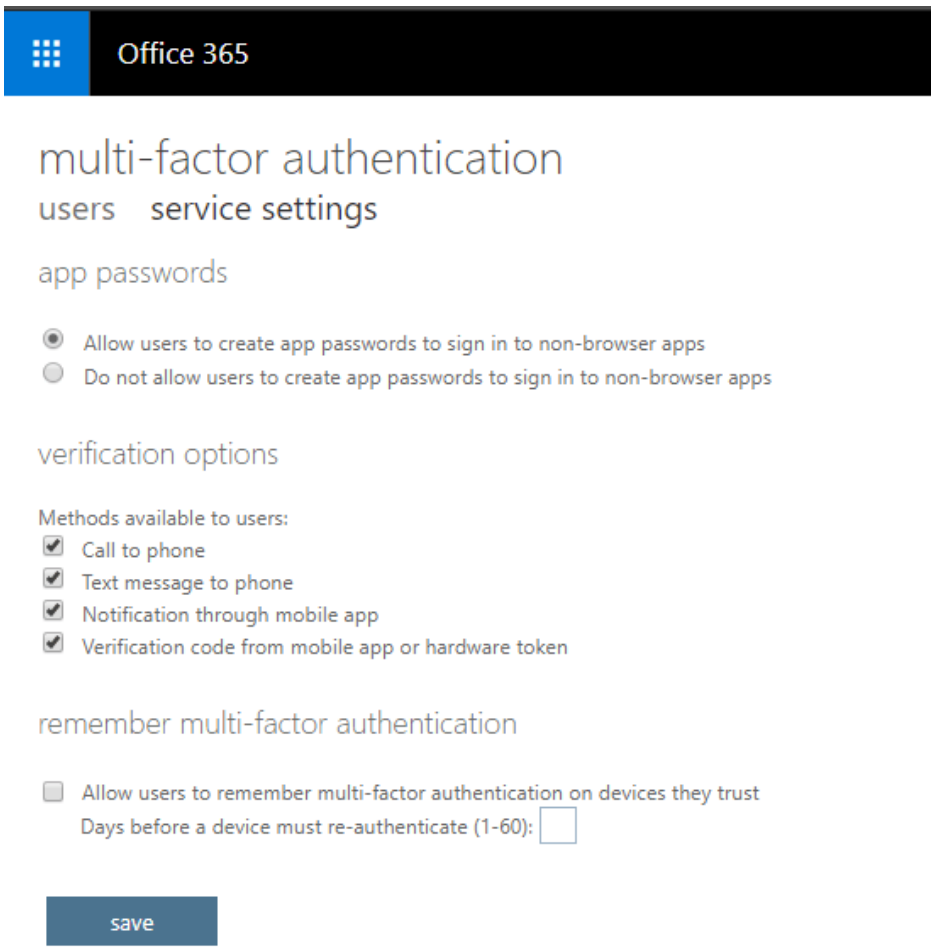
Go to the Office 365 Admin Center and navigate to **Users** > **Active users**. Find **More** > **Setup Azure multi-factor…**



You can see your users listed here, but before you enable MFA for anyone in particular, check out the **service settings** area.

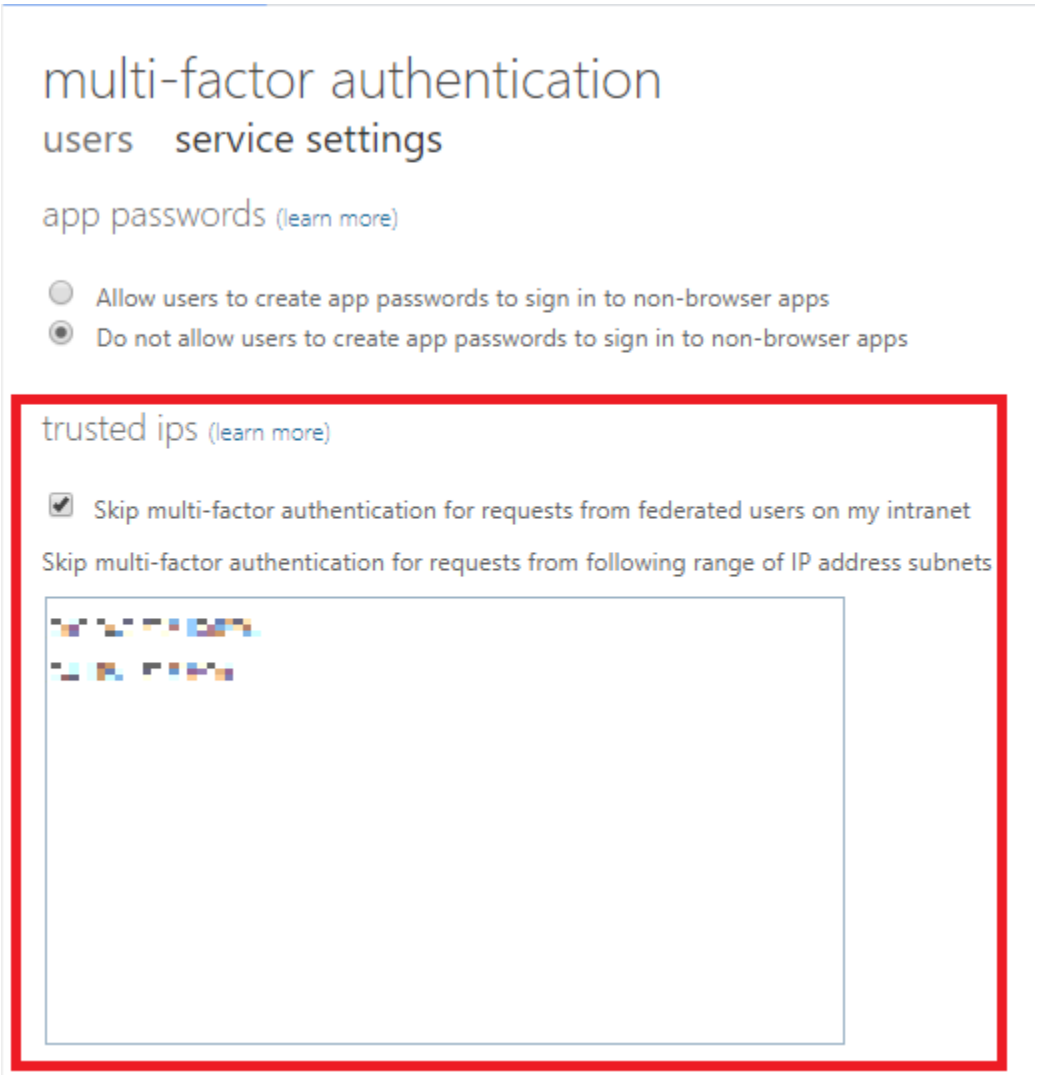


Here you can select various options surrounding the use of MFA. For example, allow certain types of MFA challenge such as phone calls, SMS, mobile app notifications, or hardware tokens. It is also where you allow or disallow users to generate app passwords (for applications that do not support a second factor prompt–e.g. older versions of Office apps, Apple Mail, etc.).

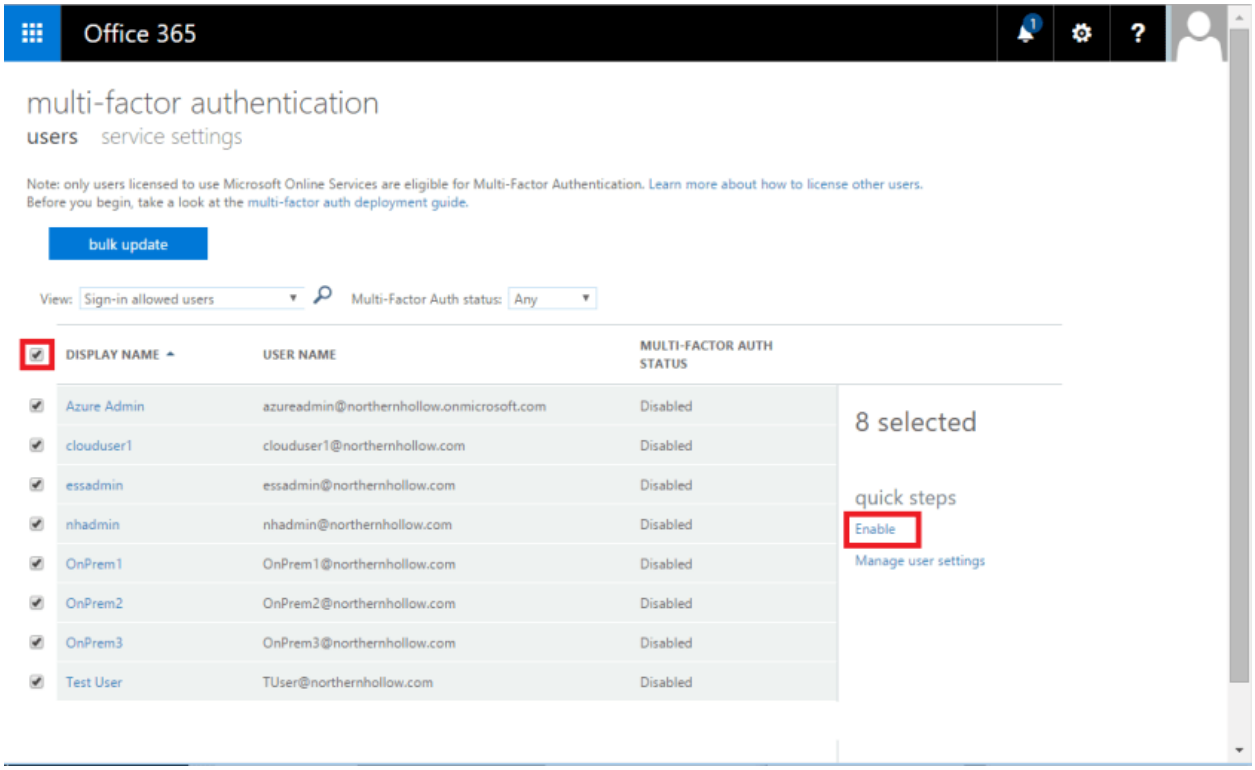


Note: I find the mobile app notification option is usually the best user experience.

When you have access to Azure AD Premium P1 and Conditional access, you will also see an option to exclude **trusted IPs** (e.g. corporate locations). Please note, this means the external IP addresses, not the internal IP subnets.



Back on the **users** tab, we can turn MFA on for users one by one, or several at a time. Simply select one, many (or all) of the users, and choose **Enable** on the right.



You also have the option to use the **bulk update** button at the top of this page, and provide a CSV file which is formatted as follows:

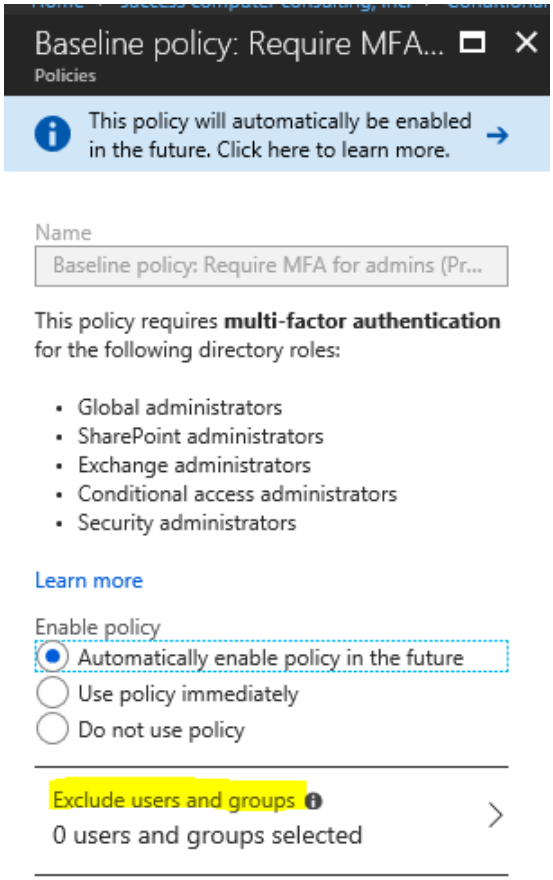
	A	B
1	Username	MFA Status
2	chris@contoso.com	Enabled
3	ben@contoso.com	Disabled
4	kyle@contoso.com	Disabled
5	kenny@contoso.com	Enabled
6	eric@contoso.com	Enabled

You may also notice that when you choose one or more of the users from this area, you have an option to **Manage user settings**. You get these choices:

- **Require selected users to provide contact methods again**
- **Delete all existing app passwords generated by the selected users**
- **Restore multi-factor authentication on all remembered devices**

☐ Option 2. Use Conditional Access to enforce MFA

From the **Azure Active Directory,** find the **Conditional Access** blade. You will notice a policy present in here called ***Baseline policy: Require MFA for admins***.

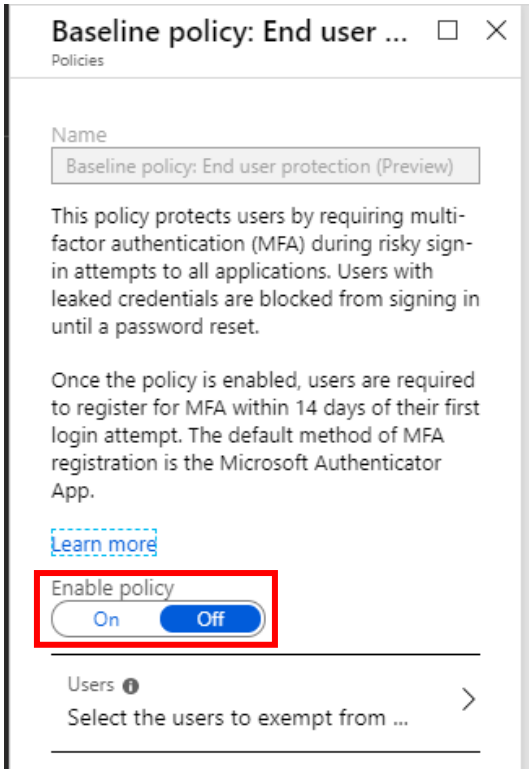


You should switch this policy on (**Use policy immediately**). However, it is recommended to exclude at least one emergency access or "break glass" account, but you need to treat that account *very differently* than normal accounts:

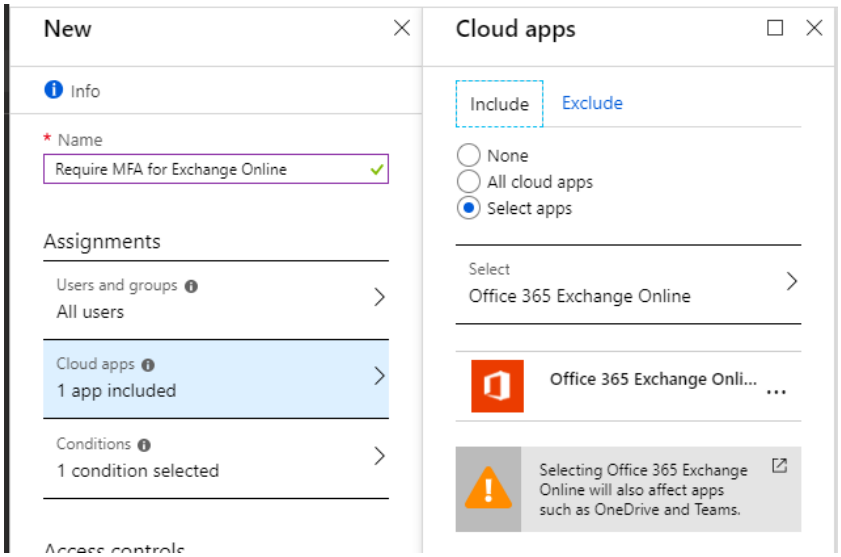
- they should not be used for anything other than administrative tasks
- use a cloud-only ID with logon suffix such as "@tenant.onmicrosoft.com" rather than your vanity domain name, or some AD-Synced account
- change the password regularly, and whenever administrative users who know this password leave or are terminated

Here are Microsoft's notes on emergency access accounts, for further reference. So that covers administrative users, which is your bare minimum.

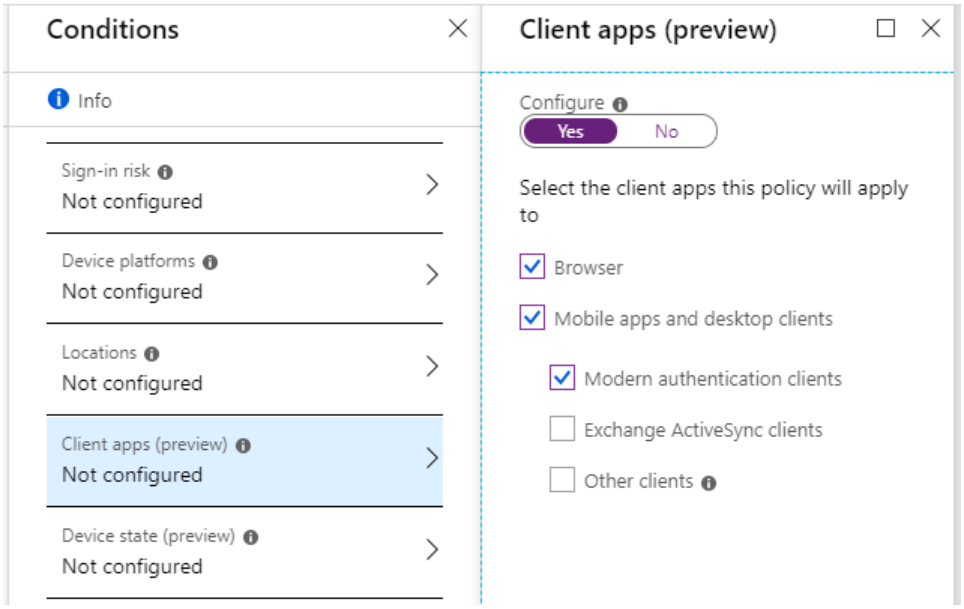
Another baseline policy will enable MFA for end users, but only under "risky" sign-in conditions. Select ***Baseline policy: End user protection***. You will notice that this policy also blocks sign-in and forces users with leaked credentials to perform a password reset (which again requires the second factor). Bonus!



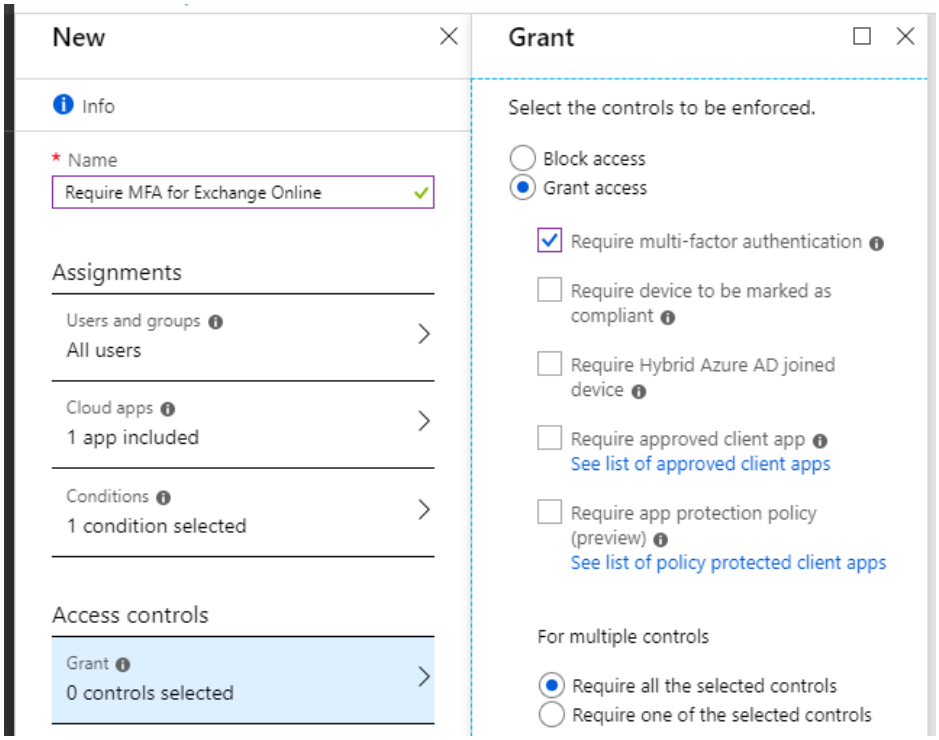
That may be good enough for some. It is recommended, however, to enforce MFA more strictly. Simply create a new policy and call it "Require MFA for Exchange Online." Pick **All users** and **Office 365 Exchange Online** as the cloud app that you are targeting.



Under **Conditions > Client apps**, select **Browser** as well as **Mobile apps and desktop clients > Modern authentication clients**. "Exchange ActiveSync" clients and "Other clients" do not support MFA.

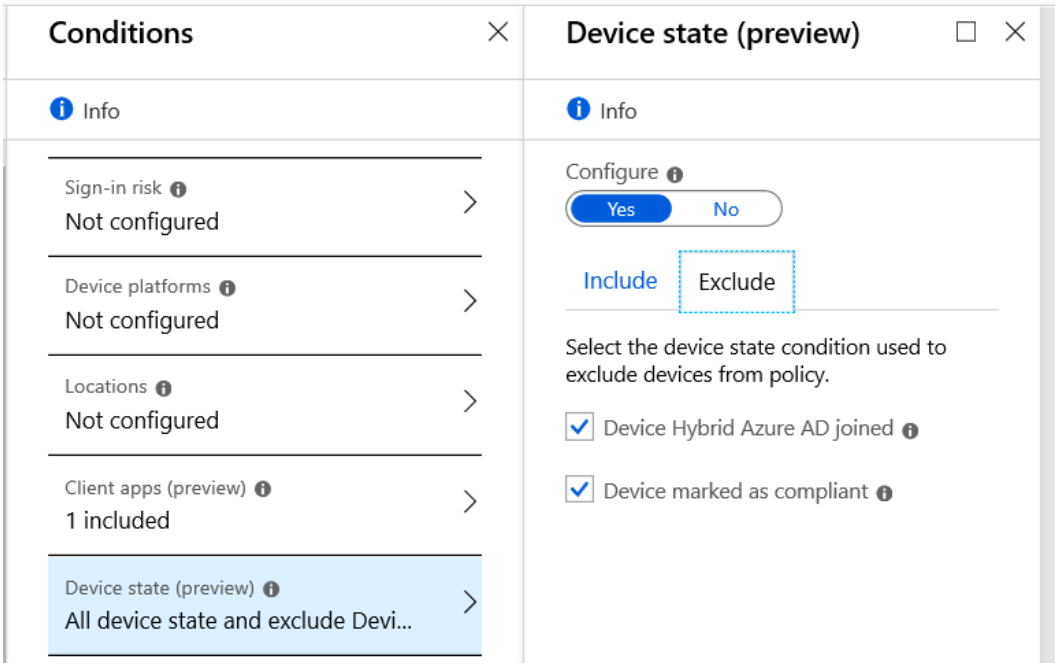


Last go to **Access Controls > Grant** and choose **Require Multi-factor authentication**.



Save your selection and **Enable** the policy.

Some additional notes about Conditional access: It is possible to exclude managed/enrolled devices by using the **Conditions > Device state** blade. On the **Exclude** tab, select both options to exclude managed devices.



This option can make life easier for users on corporate owned/issued devices (because the managed device itself is a "factor" being evaluated during authentication). It is also possible to use *Exclude* tabs in other places, e.g. users/groups, locations and so forth. Use these sparingly and try to keep your attack surface as small as possible.

☐ Instructions for end users

Communicate the MFA changes in advance to your end users. You can provide them with links to the Microsoft support literature on this, also:

- Setup 2-Step verification for Office 365

Referring to the official support articles might be the easiest (vs. creating your own documentation), since Microsoft changes things so often, anyway.

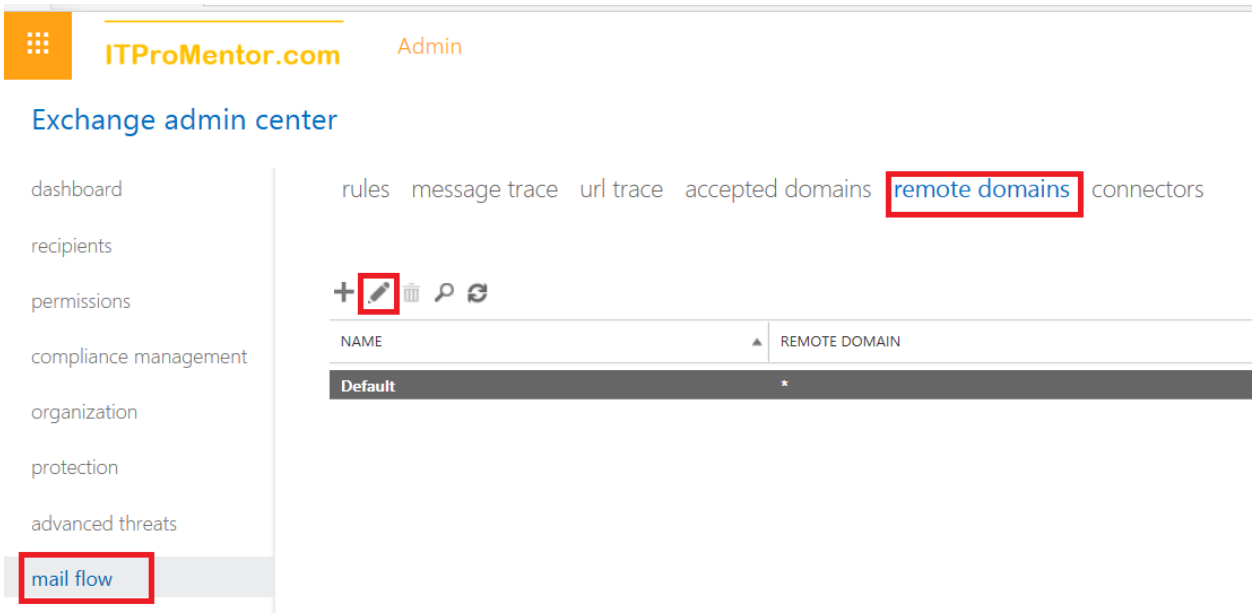
☐ Disable Mailbox forwarding to remote domains

Secure Score impact:
- Block client forwarding rules (+20)

When attackers get a hold of a mailbox, they will often exfiltrate data by setting up mailbox forwarding to an outside email address that they can then monitor without needing constant access to the source mailbox.

There are actually several ways to deal with this problem including RBAC (limiting permissions) and transport rules that will block / reject auto-forwarded messages, but I am going to recommend that you implement the easiest and most effective solution. Simply disable the auto-forwarding behavior globally—for all remote domains.

You can find this setting in the Exchange admin center also under **mail flow > remote domains**. Edit the Default remote domain object (*).



Clear the selection for **Allow automatic forwarding**.

In PowerShell, the command is:

```
Set-RemoteDomain Default -AutoForwardEnabled $false
```

To enable exceptions, you would create a new remote domain (to a specific place like a partner organization) and then enable the option instead of disabling it.

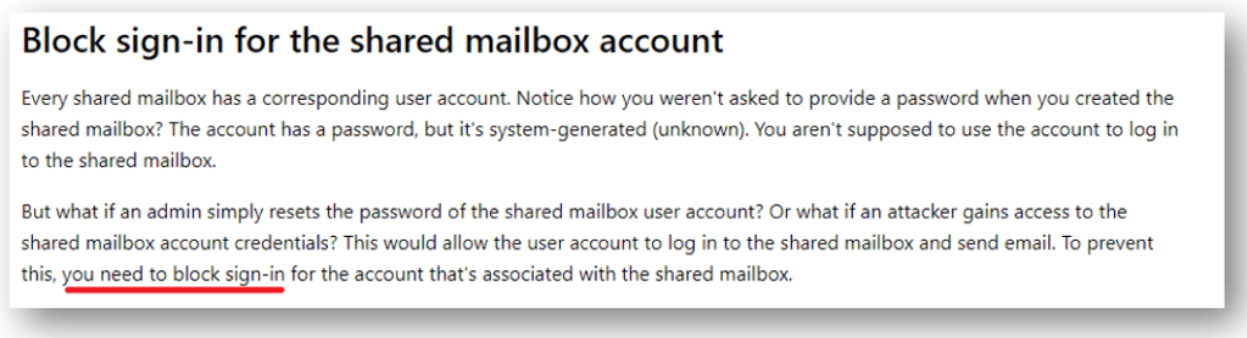
If you want to see whether any existing users will be impacted by this change, you can export to CSV the people who have either created inbox rules or configured a mailbox forwarder.

```
## This script collects and exports existing mailbox forwarding info;

CSV files are deposited into C:\temp\

## Find the default accepted domain name and store in a variable:

$DefaultDomainName = Get-AcceptedDomain | Where-Object Default -EQ True

## Export forwarders to CSV:

Get-Mailbox -ResultSize Unlimited -Filter {(RecipientTypeDetails -ne "DiscoveryMailbox") -and ((For
wardingSmtpAddress -ne $null) -or (ForwardingAddress -ne $null))} | Select Identity,ForwardingSmt
pAddress,ForwardingAddress | Export-Csv c:\temp\$DefaultDomainName-MailboxForwarding.csv -
append

foreach ($a in (Get-Mailbox -ResultSize Unlimited |select PrimarySMTPAddress)) {Get-InboxRule -M
ailbox $a.PrimarySMTPAddress | ?{($_.ForwardTo -ne $null) -or ($_.ForwardAsAttachmentTo -ne $n
ull) -or ($_.DeleteMessage -eq $true) -or ($_.RedirectTo -ne $null)} |select Name,Identity,ForwardT
o,ForwardAsAttachmentTo, RedirectTo, DeleteMessage | Export-Csv c:\temp\$DefaultDomainNam
e-InboxRules.csv -append }

## NOTE: After running this script, check the CSV files under C:\temp for a list of mail users who ma
y be affected by disabling the ability to auto-forward messages to external domains
```

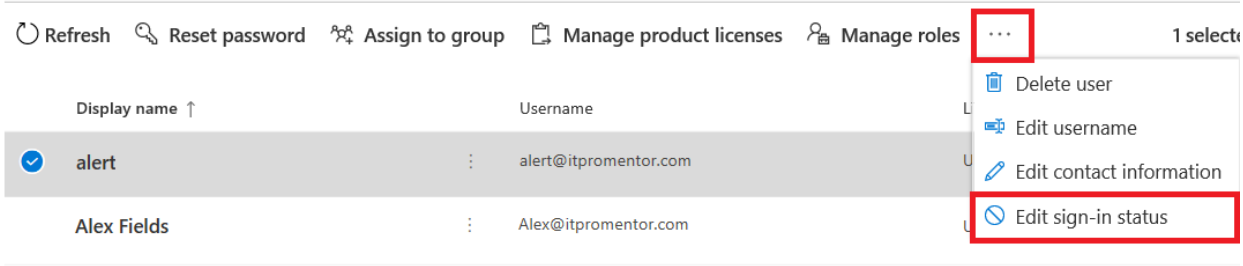
☐ Block sign-in for all shared mailboxes

Secure Score impact:
- None

Shared mailboxes (including Resource mailboxes) do not require interactive login. Rather, users who are delegated permission can access and interact with the contents of the shared mailbox. When organizations do dumb things like allow multiple users to sign into shared mailboxes on mobile devices, they are not working within the conceptual framework of a shared mailbox. So effectively, those which are enabled for interactive sign-in become real user mailboxes and need to be treated as any other user account at that point.



Otherwise, you should be blocking sign-in on these accounts. Note that accounts which are synced from on-premises Active Directory would need to be disabled on-premises. In the 365 admin center, select one or multiple accounts and **Edit the sign-in status** from the **ellipses**.



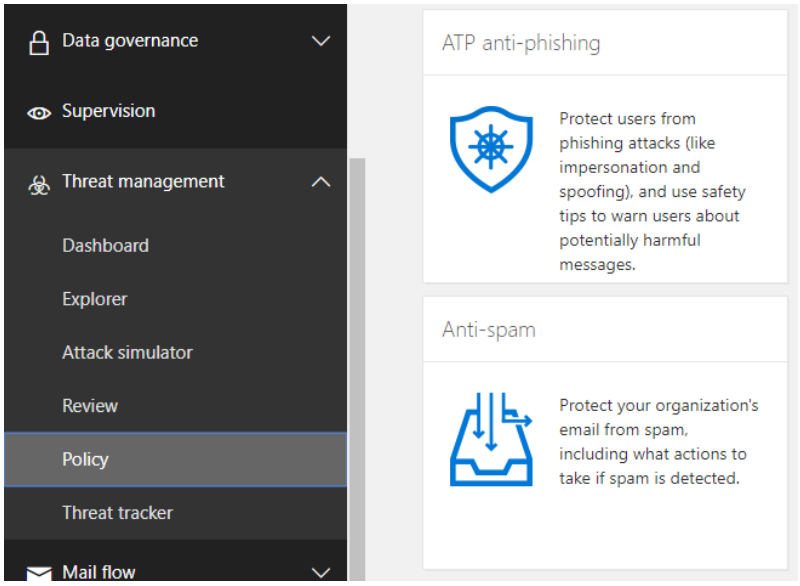
This action would be equivalent to the following in PowerShell (Connect-MsolService):

```
Set-MsolUser -UserPrincipalName username@company.com -BlockCredential $true
```

☐ Tune up your Exchange Online Protection policies

Secure Score impact:
- Set outbound spam notifications (+15)

The default antispam and antimalware policies… leave something to be desired, shall we say. Basically, nothing is turned on by default. Sad. But we're going to fix that now. In the Security & Compliance center, navigate to **Threat Management > Policy**.



If you prefer to use the graphical interface, then here is where you would find various UI-driven policy builders, for both Exchange Online protection (anti-spam, anti-malware) as well as ATP (anti-phishing, safe links and safe attachments).

To configure new custom baseline policies, we can do this in PowerShell. Connected to Exchange Online via the PowerShell module, use the script blocks below. (I will also depict some of the same settings as seen via the UI, but the script blocks will take you from zero to configured much more quickly.)

In this first script block, you need to specify some variables that are particular to your environment, such as the domain name(s) you need to include in protection, as well as a mailbox that can receive alerts about suspicious emails and attachments.

```
## Specify your recipient domain(s) in the variable:
$RecipientDomains = "tenantname.onmicrosoft.com", "companydomain.com"
## Specify your alert mailbox:
$AlertAddress= "securityalerts@companydomain.com"
```

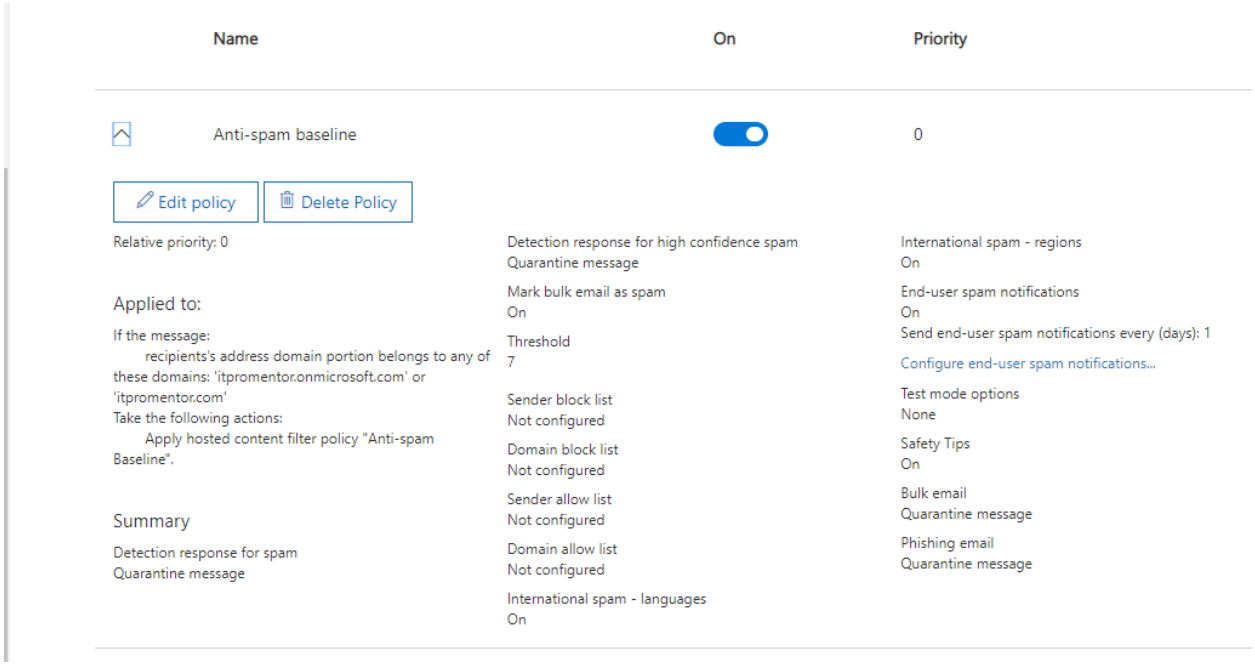
☐ Configure the spam filter policy

To configure the (inbound) spam filter policy, run the following:

```
$antispamparam = @{
```

```
   "name" = "Anti-spam Baseline";
   'bulkspamaction' =  'quarantine';
   'bulkthreshold' =  '7';
   'highconfidencespamaction' =  'quarantine';
   'inlinesafetytipsenabled' = $true;
   'markasspambulkmail' = 'on';
   'increasescorewithimagelinks' = 'off'
   'increasescorewithnumericips' = 'on'
   'increasescorewithredirecttootherport' = 'on'
   'increasescorewithbizorinfourls' = 'on';
   'markasspamemptymessages' ='on';
   'markasspamjavascriptinhtml' = 'on';
   'markasspamframesinhtml' = 'on';
   'markasspamobjecttagsinhtml' = 'on';
   'markasspamembedtagsinhtml' ='on';
   'markasspamformtagsinhtml' = 'on';
   'markasspamwebbugsinhtml' = 'off';
   'markasspamsensitivewordlist' = 'on';
   'markasspamspfrecordhardfail' = 'on';
   'markasspamfromaddressauthfail' = 'on';
   'markasspamndrbackscatter' = 'off';
   'phishspamaction' = 'quarantine';
   'spamaction' = 'quarantine';
   'zapenabled' = $true;
   'EnableEndUserSpamNotifications' = $true;
   'EndUserSpamNotificationFrequency' = 1;
   'QuarantineRetentionPeriod' = 15
}
New-HostedContentFilterPolicy @antispamparam

$antispamruleparam = @{
   'name' = 'Anti-spam baseline';
   'hostedcontentfilterpolicy' = 'Anti-spam baseline';
   'recipientdomainis' = $RecipientDomains;
   'Enabled' = $true
}
New-HostedContentFilterRule @antispamruleparam
```

As seen via the admin center, the same policy can be reviewed.



Note that our default configuration uses the option to **Quarantine** spam. You can also choose **MoveToJmf**, if you prefer that the users review spam messages via their "Junk Mail Folder" in Outlook. However, **Quarantine** is considered safer, because potentially malicious emails are not so easy to access—so there is less chance of a user finding something bad within the Junk folder and clicking on it, thinking it is legitimate.

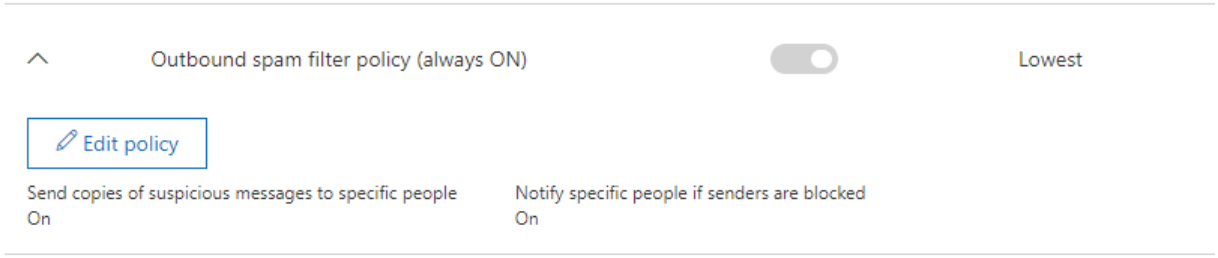
Users can sign into https://protection.office.com to review their own quarantine at any time. With the settings specified here, they will also receive a daily "digest" of messages that went to quarantine during the day. They can review and release these messages as needed.

☐ Configure the outbound spam policy

To configure the outbound spam policy, run the following:

```
$outboundparam = @{
   "identity" = 'Default';
   'bccsuspiciousoutboundadditionalrecipients' =  $AlertAddress;
   'bccsuspiciousoutboundmail' = $true;
   'notifyoutboundspam' = $true;
   'NotifyOutboundSpamRecipients' = $AlertAddress
}
Set-HostedOutboundSpamFilterPolicy @outboundparam
```

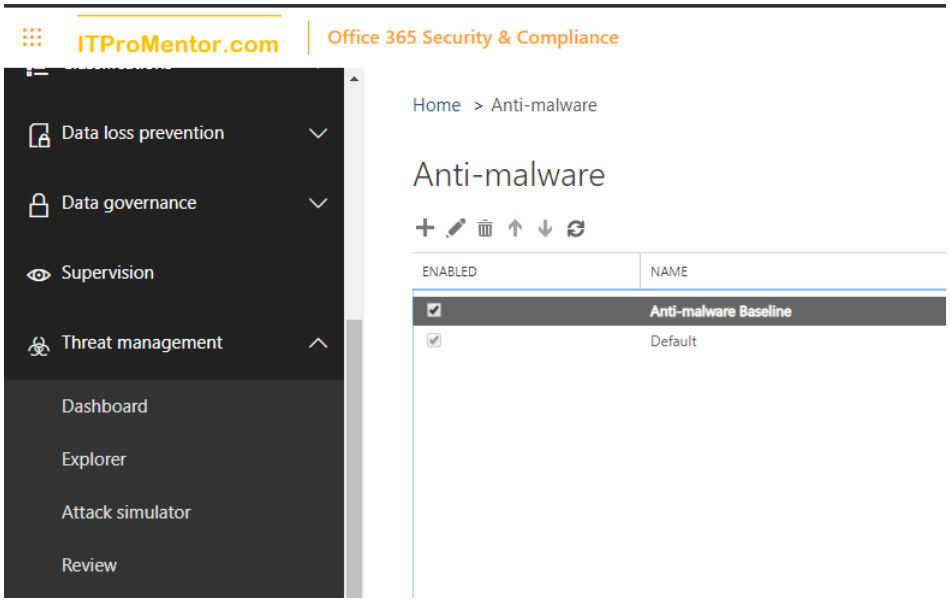
As seen from the UI, just scroll down further past the custom policy to find the **Outbound spam filter policy**. This has been configured to alert the specified user when outbound mail is suspected as spam.



☐ Configure the malware filter policy

```
$malwareparam = @{
   "Name" = "Anti-malware Baseline";
   'Action' =  'deletemessage';
   'Enablefilefilter' =  $true;
   'EnableInternalSenderAdminNotifications' = $true;
   'InternalSenderAdminAddress' =  $AlertAddress;
   'Enableinternalsendernotifications' =  $true;
   'ZapEnabled' = $true
}
New-MalwareFilterPolicy @malwareparam


$malwareruleparam = @{
   'name' = 'Anti-malware Baseline';
   'malwarefilterpolicy' = 'Anti-malware Baseline';
   'recipientdomainis' = $RecipientDomains;
   'Priority' = 0;
   'Enabled' = $true
}

New-MalwareFilterRule @malwareruleparam
```

As seen from the UI, select the Anti-malware Baseline policy to review its settings.



☐ Turn on Office 365 Advanced Threat Protection

Secure Score impact:
- Set up Office 365 ATP Safe Attachment policies (+15)
- Set up Office 365 ATP Safe Links to verify URLs (+15)

Office 365 Advanced Threat Protection (ATP) plan 1 is recommended for ALL mailbox users in Office 365. It includes the following policies which are configurable from Security & Compliance Center > **Threat Management > Policy**:

Safe Links – Hyperlinks which exist in email messages or other content in Office 365 are re-written into a new URL which includes a Microsoft "wrapper." The Microsoft URL acts like a proxy, launching the links—and the links that are found within those links, and the links within those links—before sending your own web browser on to the "real" destination. This allows Microsoft to test out in advance if a website has "gone dark" or contains potentially bad content, before you get there.

WARNING: it is important to realize how this timing works—the scans are taking place literally at the time you click the link, not when the link was created or sent.

Safe Attachments – Safe attachments will essentially launch any downloadable attachment and execute it in a virtual machine (what they call 'detonating'), before allowing it to go on to the end-user. This sandbox environment is looking for behaviors that are unusual or abnormal, and which could represent malware. This is beyond virus scanning–it is looking for zero-day threats–stuff without signatures.

WARNING: enabling this feature will cause noticeable delays in delivery of certain content/attachments. In some cases, I have seen some email messages delayed by up to 10 minutes.

Anti-phishing – ATP anti-phishing policies allow you to put in place some anti-impersonation protections against specific mailboxes and domains. You can enable policy tips that would, for example, raise a user's attention to the fact that a domain name contains unusual characters (e.g. a zero instead of the letter "O"), which is often exploited in certain attacks/spoof attempts.

Furthermore, you can apply "Mailbox intelligence" which applies machine learning to the message exchange patterns between your users and their usual contacts. This helps Microsoft identify when a known contact sends a suspicious message, which may actually be an impersonator standing in the shoes of that contact.

☐ Set Default ATP policy & Configure Safe Links

Before you run the PowerShell scripts to configure ATP features, be sure to define these variables in advance:

```
## $AlertAddress = Who will receive notifications/redirected emails?

$AlertAddress = "securityalerts@companydomain.com"

## $RecipientDomains = Fill in the domain names that will be protected by domain impersonation:

## e.g. $RecipientDomains = "tenantname.onmicrosoft.com", "domain1.com", "domain2.com", "do
main3.com"

$RecipientDomains = "tenantname.onmicrosoft.com", "companyname.com"

## $TargetedUsersToProtect = Fill in the users who will be protected by user impersonation:

## e.g. $TargetedUsersToProtect = "Display Name 1;user1@domain.com", "Display Name 2;user2@
domain.com", "Display Name 3;user3@domain.com"

$TargetedUsersToProtect = "Alex Fields;alex@comanyname.com","Natalie Smith;natalie@company
name.com", "Jim Bryan;jim@companyname.com"
```

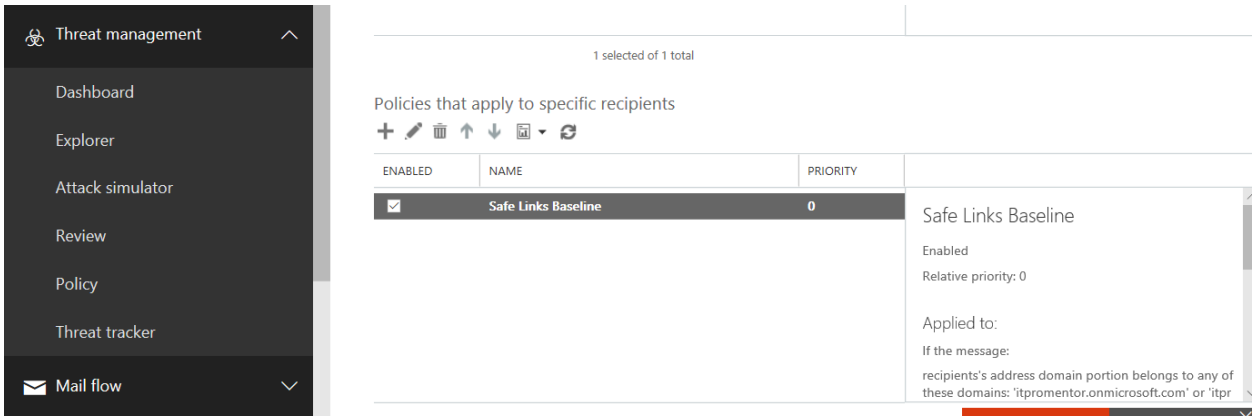
Next, configure the default ATP policy, which will enable Safe Links for client apps, and turn on Safe Attachment scanning for SharePoint and OneDrive.

```
Set-AtpPolicyForO365 -EnableSafeLinksForClients $true -EnableATPForSPOTeamsODB $true -AllowC
lickThrough $false -TrackClicks $true
```

Then, to configure the Safe Links policy and rule which will apply to all users:

```
$SafeLinksPolicyParam=@{
  'Name' = "Safe Links Baseline Policy";
  'AdminDisplayName' = "Safe Links Baseline Policy";
  'DoNotAllowClickThrough' =  $true;
  'DoNotTrackUserClicks' = $false;
  'EnableForInternalSender' = $true;
  'ScanUrls' = $true;
  'TrackClicks' = $true;
  'IsEnabled' = $true
}

New-SafeLinksPolicy @SafeLinksPolicyParam

## Create the Safe Links Rule
$SafeLinksRuleParam = @{
   'Name' = "Safe Links Baseline";
            'SafeLinksPolicy' = "Safe Links Baseline Policy";
            'RecipientDomainIs' = $RecipientDomains;
            'Enabled' = $true;
            'Priority' = 0
}

New-SafeLinksRule @SafeLinksRuleParam
```

Review the same from **Threat Management > Policy > Safe Links**.

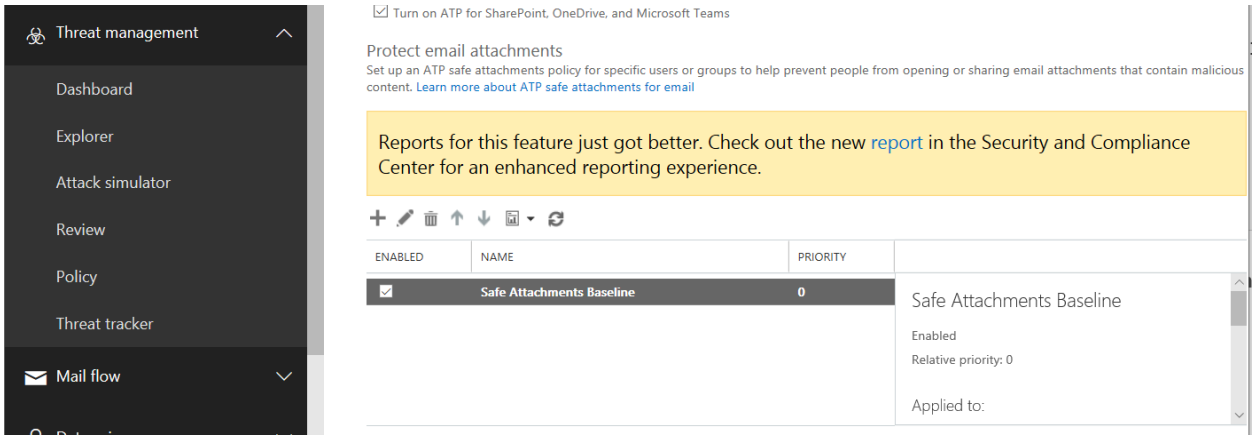


☐ Configure Safe Attachments

Now to setup Safe Attachments policy and rule:

```
## Create the SafeAttachments policy
## Action options = Block | Replace | Allow | DynamicDelivery

$SafeAttachmentPolicyParam=@{
  'Name' = "Safe Attachments Baseline Policy";
  'AdminDisplayName' = "Safe Attachments Baseline Policy";
  'Action' =  "Block";
  'ActionOnError' = $true;
  'Enable' = $true;
  'Redirect' = $false;
}

New-SafeAttachmentPolicy @SafeAttachmentPolicyParam

## Create the SafeAttachments rule
$SafeAttachRuleParam=@{
   'Name' = "Safe Attachments Baseline";
            'SafeAttachmentPolicy' = "Safe Attachments Baseline Policy";
            'RecipientDomainIs' = $RecipientDomains;
            'Enabled' = $true;
            'Priority' = 0
}

New-SafeAttachmentRule @SafeAttachRuleParam
```

Review the same from **Threat Management > Policy > Safe Attachments.**



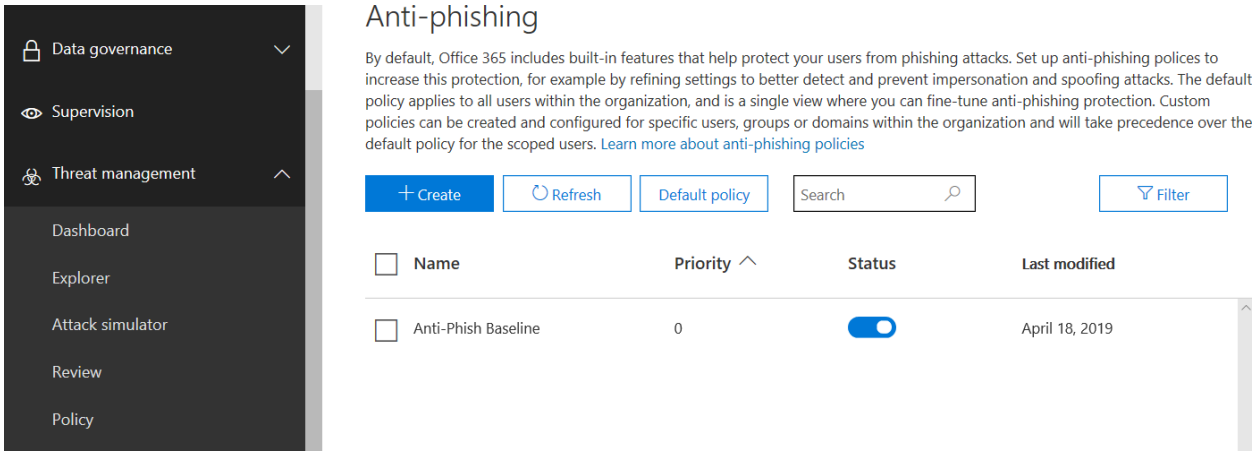
☐ Configure Anti-Phish policy

And last, configure the Anti-Phish policy and rule as follows:

```
## Create the Anti-Phish policy

$PhishPolicyParam=@{
  'Name' = "Anti-Phish Baseline Policy";
  'AdminDisplayName' = "Anti-Phish Baseline Policy";
  'AuthenticationFailAction' =  'Quarantine';
  'EnableAntispoofEnforcement' = $true;
  'EnableAuthenticationSafetyTip' = $true;
  'EnableAuthenticationSoftPassSafetyTip' = $true;
  'Enabled' = $true;
  'EnableMailboxIntelligence' = $true;
  'EnableOrganizationDomainsProtection' = $true;
  'EnableSimilarDomainsSafetyTips' = $true;
  'EnableSimilarUsersSafetyTips' = $true;
  'EnableTargetedDomainsProtection' = $false;
  'EnableTargetedUserProtection' = $true;
  'TargetedUsersToProtect' = $TargetedUsersToProtect;
  'EnableUnusualCharactersSafetyTips' = $true;
  'PhishThresholdLevel' = 1;
  'TargetedDomainProtectionAction' =  'Quarantine';
  'TargetedUserProtectionAction' =  'Quarantine';
  'TreatSoftPassAsAuthenticated' = $true
}

New-AntiPhishPolicy @PhishPolicyParam

## Create the Anti-Phish rule
```

```
$PhishRuleParam = @{
   'Name' = "Anti-Phish Baseline";
            'AntiPhishPolicy' = "Anti-Phish Baseline Policy";
            'RecipientDomainis' = $RecipientDomains;
            'Enabled' = $true;
            'Priority' = 0
}

New-AntiPhishRule @PhishRuleParam
```

Review from **Threat management > Policy > Anti-phishing**.



☐ Protect mailboxes with a Retention policy or Litigation hold

Secure Score impact:
- None

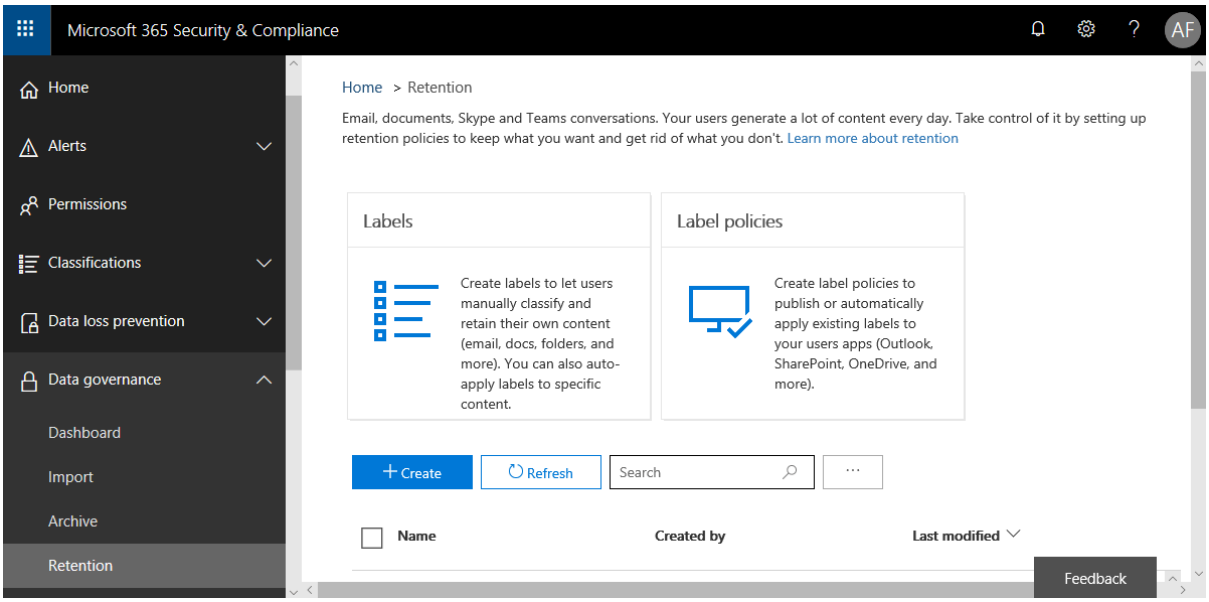
You will need an Enterprise plan such as E3 or E5, or any Microsoft 365 plan, to gain access to features like litigation hold and retention policies. But they are critical (so you should really consider one of these plans). When you enable either litigation hold or a retention policy, it means that email data will be preserved in the background, even if a user or attacker deletes items from a mailbox (and they often do in an attempt to cover their tracks).

Therefore, retention policies or litigation hold can be used to *protect* mailbox data against accidental or nefarious deletion activities. Even deleting entire user accounts will leave the mailbox itself preserved, in an offline state, so that you could recover it later as needed. Use PowerShell to see the “SoftDeletedMailbox” list.

```
PS C:\WINDOWS\system32> Get-Mailbox -SoftDeletedMailbox | Select-Object Name,ExchangeGuid

Name                  ExchangeGuid
----                  ------------
[redacted]            35caa4ac-2d05-46de-9c77-aeaf2b35a649
[redacted]            f90e806e-ac8b-4dd3-a9b7-081a1a351f86
[redacted]            71336b87-8385-42c0-acc0-af92a2539b09
[redacted]            6bb15404-3f1e-4d32-9ea0-f368bd550020
[redacted]            64d5e3dd-9cf1-4884-a10f-12f076e5f97f
[redacted]            97d257c3-9011-422b-8aeb-6956aaeb002c
```

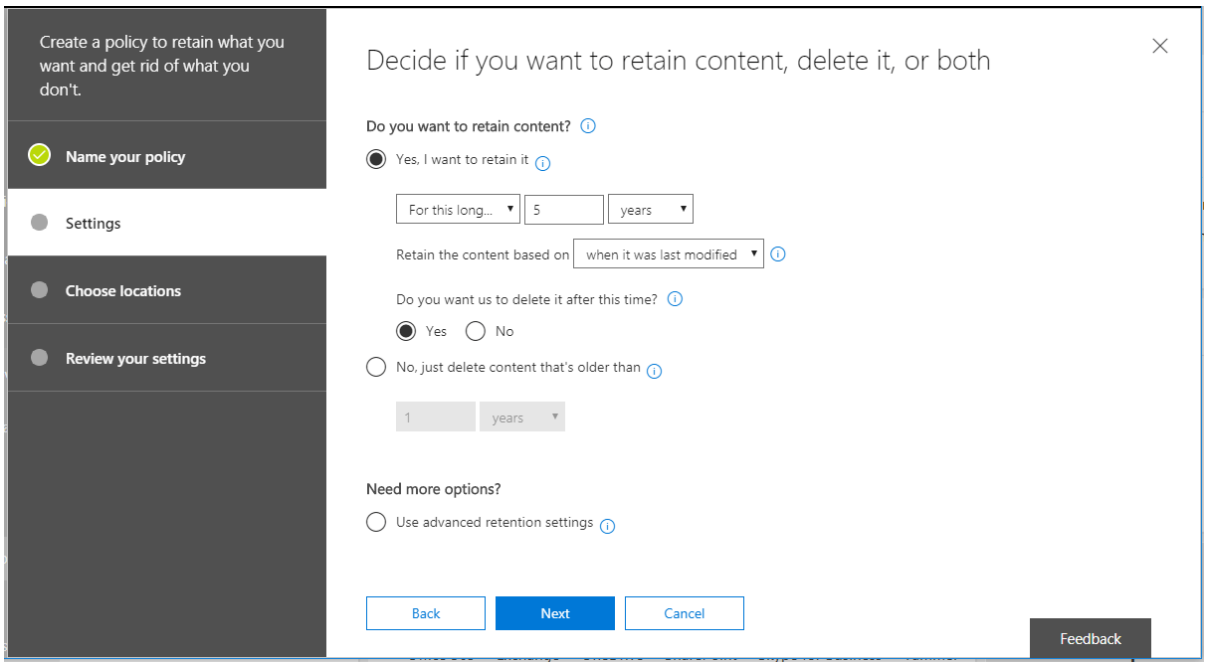
☐ Option #1: Create a Retention Policy

This is the preferred option since you can specify precisely how long to preserve data (consult with your attorney if you need guidance on just how long is necessary). From Security & Compliance center under **Data governance**, pick **Retention**. Simply choose **Create**. You will start by giving it a name and proceeding.

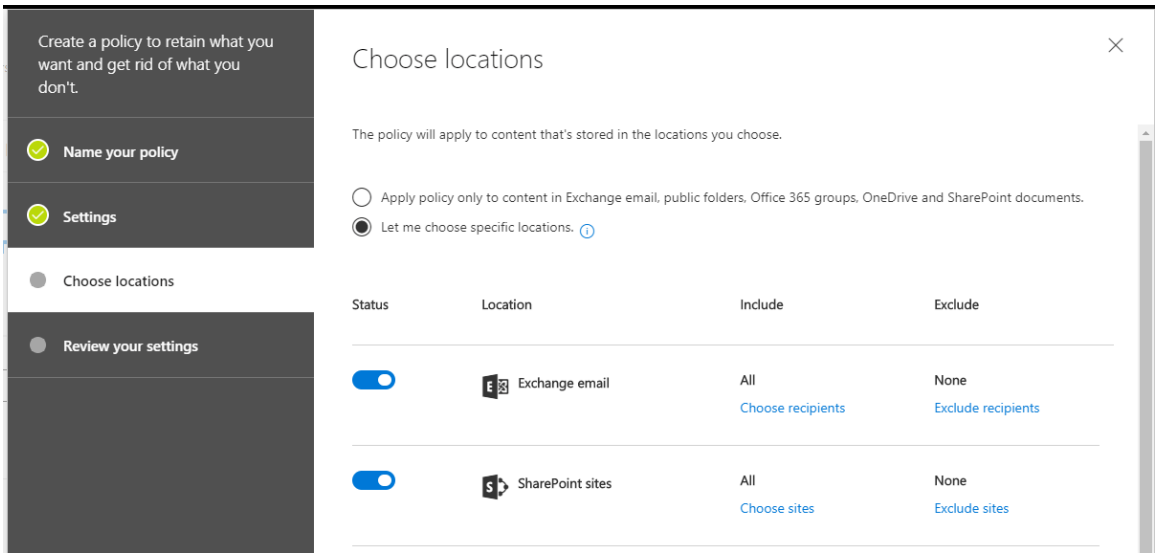


Now, you can begin to build your new policy. Notice, for example, that while you can set up to *retain*, *retain and delete*, or to just *delete* content older than a certain time frame. Be sure you understand your own organization's requirements before implementing your options.

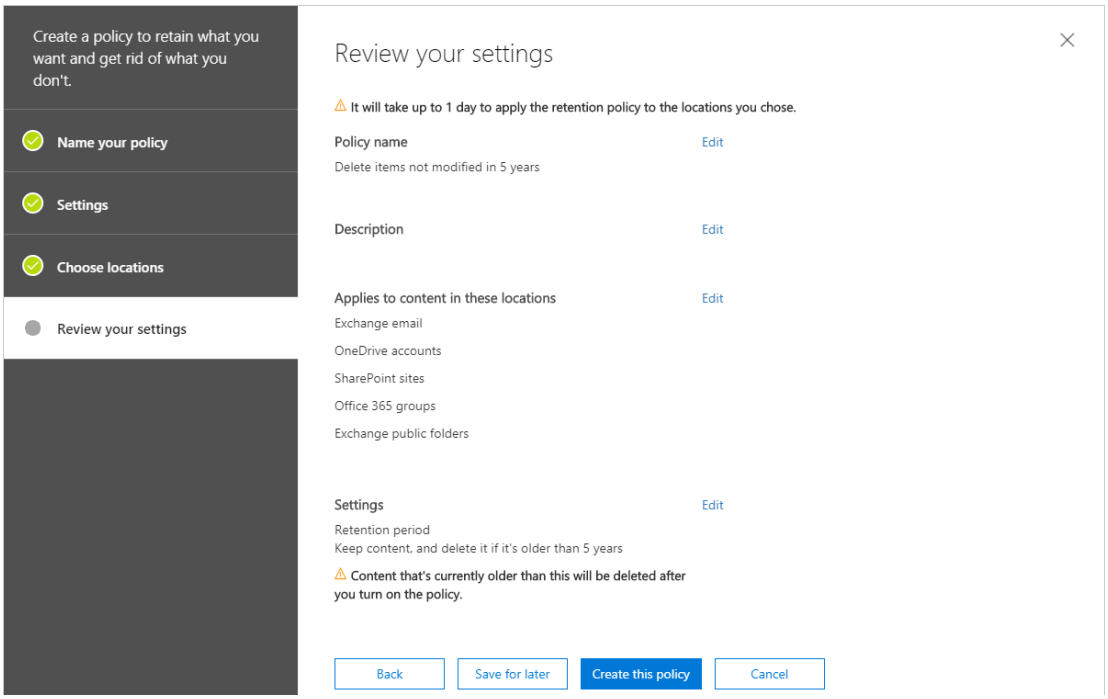
By way of example only, we will build an example policy that retains content for five years from the date it was last modified, then deletes it thereafter. Keep in mind that your own circumstances could require a completely different policy.



Next you can choose specific locations to which this policy applies—notice that it can be configured against just *one* or across *many* of the services within Office 365. Select at least **Exchange email**.



Finally, review the policy settings one more time before you **Create this policy**.



I like this option because you don't have to enable it for every individual mailbox, you can simply apply a blanket policy to all Exchange email data, just like that.

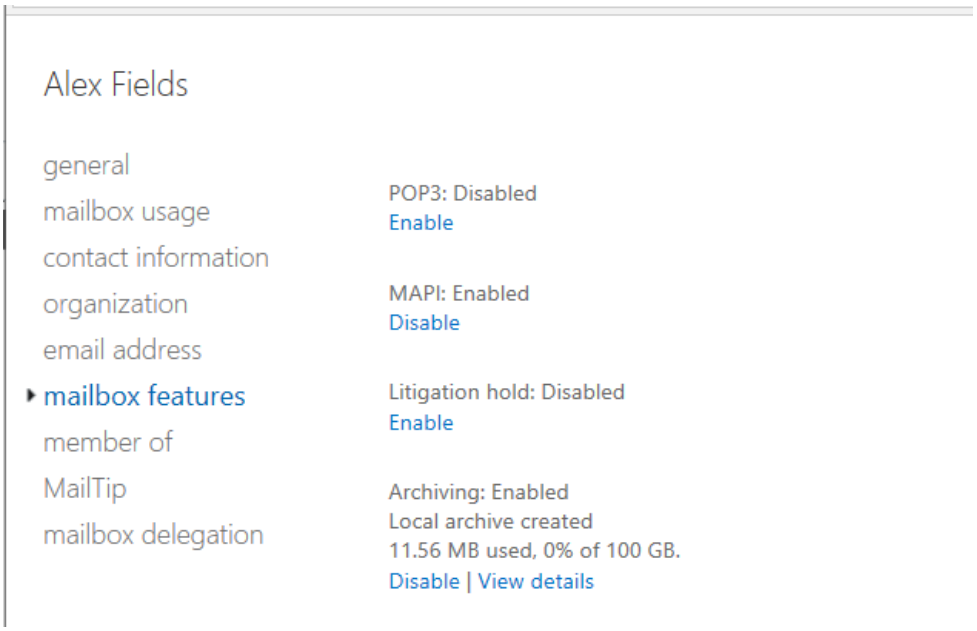
☐ Option #2: Enable Litigation hold

Another option that you have with these plans to enable litigation hold. Also known as legal hold, this feature will preserve mailbox data *indefinitely* (or until you remove the hold). Be sure to incorporate enabling this feature into your mailbox provisioning process if you choose to go this route.

In PowerShell we can accomplish the task quickly for all mailboxes as follows:

```
Get-Mailbox | Set-Mailbox -LitigationHoldEnabled $true
```

In the **Exchange admin center**, select any recipient mailbox to see the same option under **mailbox features**:



☐ Configure Mobile device policies

Secure Score impact:
- Activate mobile device management services (Not Scored)
- Varies depending on method selected (Office 365 vs. Intune)

We will cover briefly the various methods for enforcing policies against mobile devices accessing Office 365.

1. **Method #1: Exchange ActiveSync** - Exchange Online allows you to enforce controls against mobile devices using built-in Exchange ActiveSync policies (a.k.a. Mobile Device Mailbox policies).
2. **Method #2: Mobile Device Management in Office 365 (MDM) -** Technically there is a "free" version of MDM built-in to most Office 365 plans. However, there isn't much more to them than what you can already achieve with Exchange ActiveSync.
3. **Method #3: Device Management using Intune (MDM)** – Intune offers a full featured MDM solution. Note that Intune also manages Windows and MacOS.
4. **Method #4: Application Management using Intune (MAM)** – An alternative to MDM is MAM, where you assert controls against the applications rather than the device. This is available with an Intune subscription.

☐ Method #1: Exchange ActiveSync

Secure Score impact:
- None (yet you can get most of the same benefits as MDM solutions)

The real benefit of using this method to enforce mobile device policies is that you can do it natively in Exchange Online without any additional licensing. The limitations of this solution are that the policies do not support Conditional access, and only apply to mobile devices, whereas Intune supports Conditional access, and you can use it to manage all platforms, including iOS, Android, Windows and Mac.

From PowerShell, run the following script to setup a basic mobile device mailbox policy:

```
## Creates a baseline mobile device mailbox policy

$MobileDeviceParams= @{
  'Name' = "Baseline Mobile Device Policy";
  'PasswordEnabled' = $true;
  'AllowSimplePassword' =  $false;
  'PasswordRecoveryEnabled' = $true;
  'MinPasswordLength' = "4";
  'MaxPasswordFailedAttempts' = "15";
  'AllowExternalDeviceManagement' = $true;
  'AllowNonProvisionableDevices' = $false;
  'RequireDeviceEncryption' = $true;
  'MaxInactivityTimeLock' = "00:05:00";
  'IsDefault' = $true
}

New-MobileDeviceMailboxPolicy @MobileDeviceParams
```

☐ Method #2: Mobile Device Management in Office 365 (MDM)

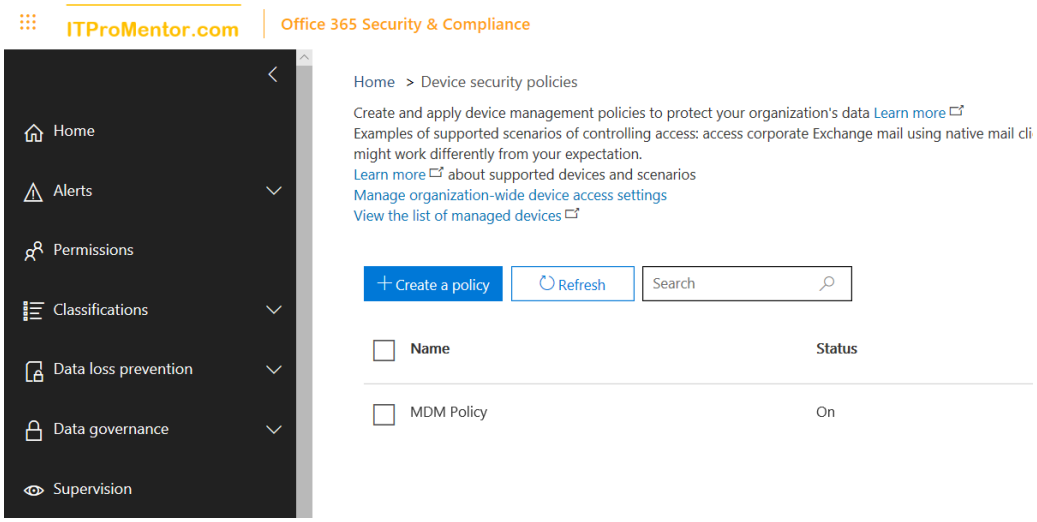
Secure Score impact:
- Activate mobile device management services (+20)
- Several smaller actions scored between 1-5 points each, e.g. Require mobile devices to use a password, Require mobile devices to use encryption, etc. (~25 points)

Office 365 has built-in Mobile Device Management using a "lite" implementation of Intune (but you cannot get to an "Intune portal view" of these configurations. They are only accessible in the 365 admin center.

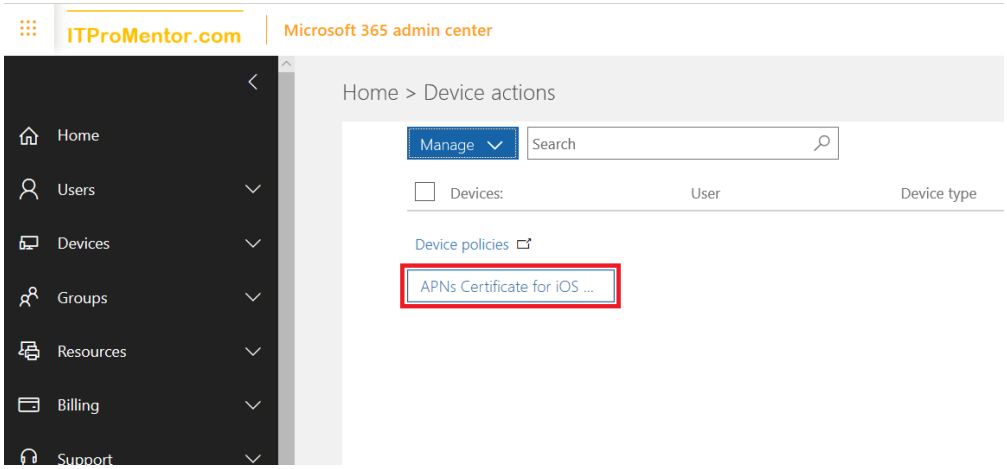
The benefit to this method is that it is free with most Office 365 bundles, and it gives you slightly more control than Exchange Active Sync policies since you can require a managed email profile (read: Conditional access) and selective wipe (wipe only the corporate data). The drawbacks are that it only supports a basic policy set (not as robust as Intune) and only on mobile devices (iOS and Android).

Note: I always recommend Intune over this method for full MDM. I would recommend EAS over this method for a "free" mobile device policy option. Nevertheless, we'll cover it quickly.

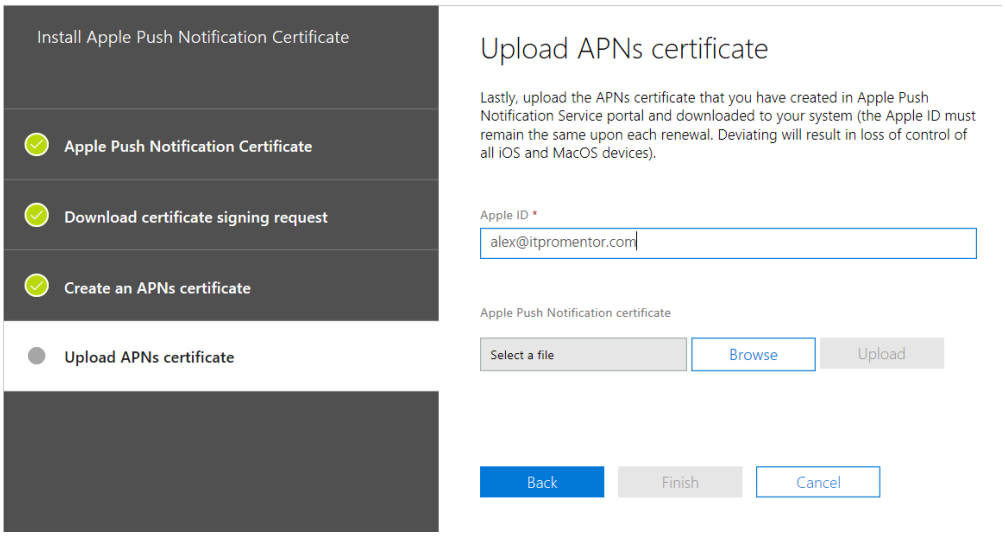
Access Device security policies from the Security Center or Security & Compliance center.



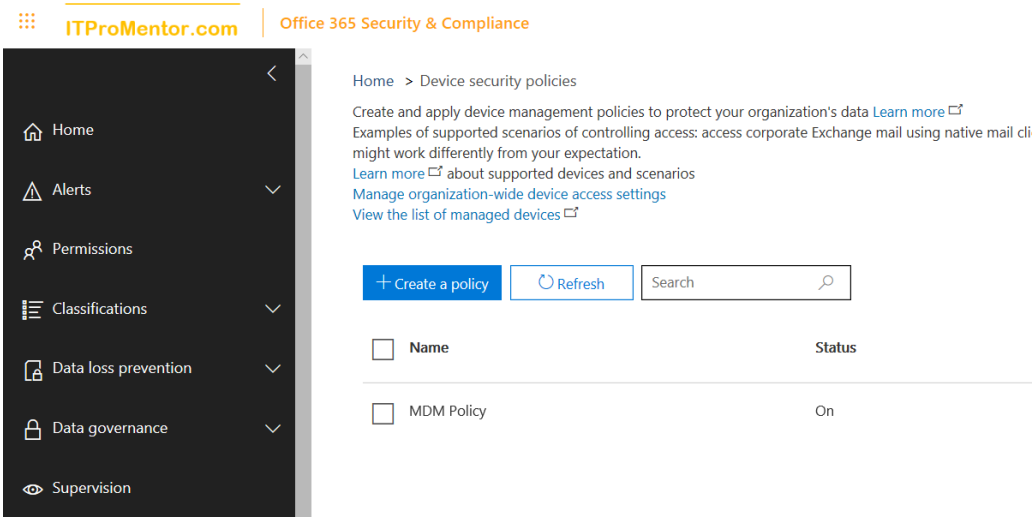
Use the link to ***View the list of managed devices***. This takes you to the Device actions page in the Microsoft 365 admin center. On this page you should first of all setup your **APNS Certificate for iOS…**



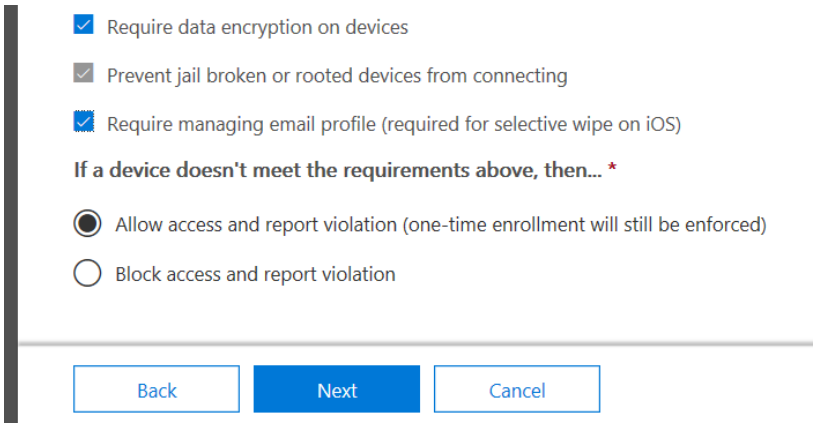
Just step through the wizard to download your certificate request, go upload it at apple.com, and then download the resulting certificate from Apple and upload it back to Office 365.



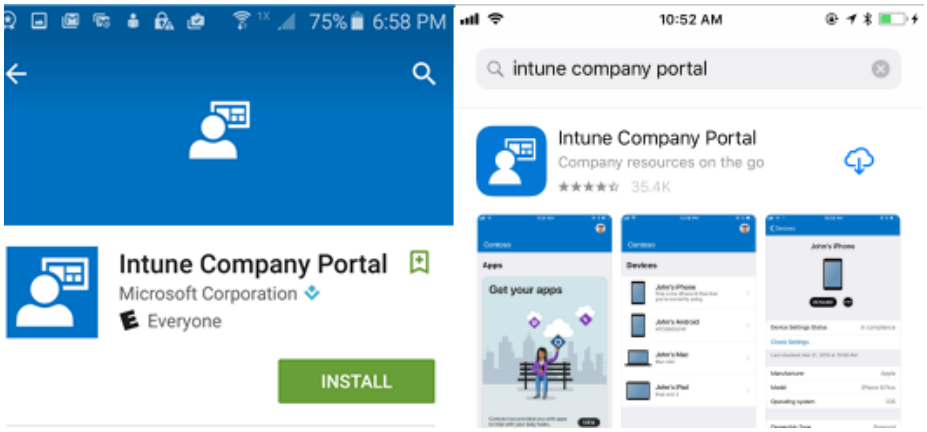
Once you are done return to the device policies page and click **Create a policy**.



Just follow along in the wizard to create your policy, be sure to select the option for a managed email profile if you want the “selective” wipe feature (wipe only corporate data).



Once your policy is deployed to a group of users, they will need to download the **Company portal app** in order to enroll their devices and become managed.



Warning: there are a lot of screens involved in getting through the enrollment process. I won't go through them all, just know that it can be a while.

☐ Method #3: Device Management using Intune (MDM)

Secure Score impact:
- Enable Microsoft Intune Mobile Device Management (+20)
- Compliance policies (+10 per device platform)
- Configuration profiles (+10 per device platform)

Using Intune, you can pick how you want to secure mobile devices—manage them either at the device level, or at the application level. This section describes managing *devices*. Typical for corporate owned devices.

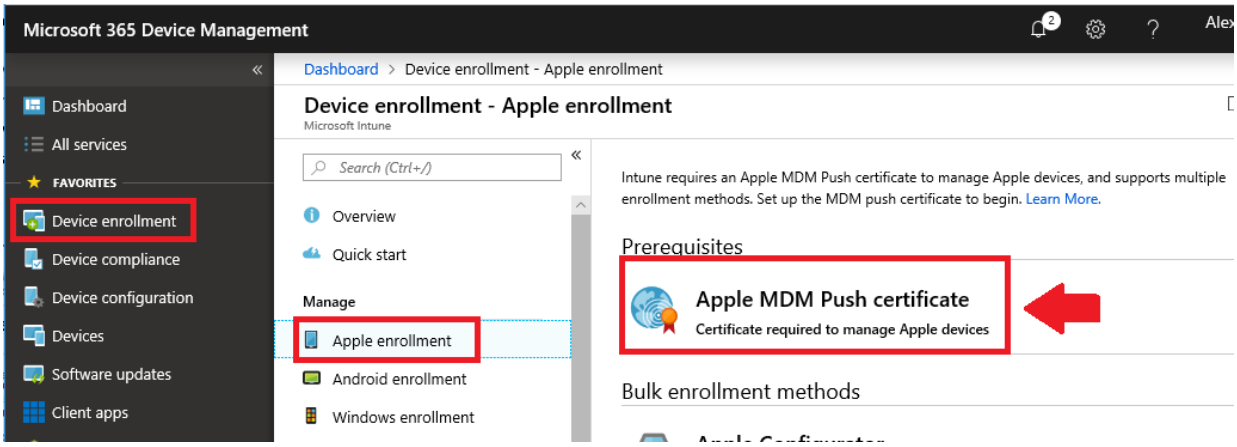
Although Intune is an add-on to standard Office 365 plans, it is included with Enterprise Mobility + Security, as well as all Microsoft 365 bundles. The benefit to this product is the vast menu of configuration options available to you, as well as the ability to visualize and manage complaint and non-compliant devices easily in the portal.

To configure MDM, you must complete these five steps:

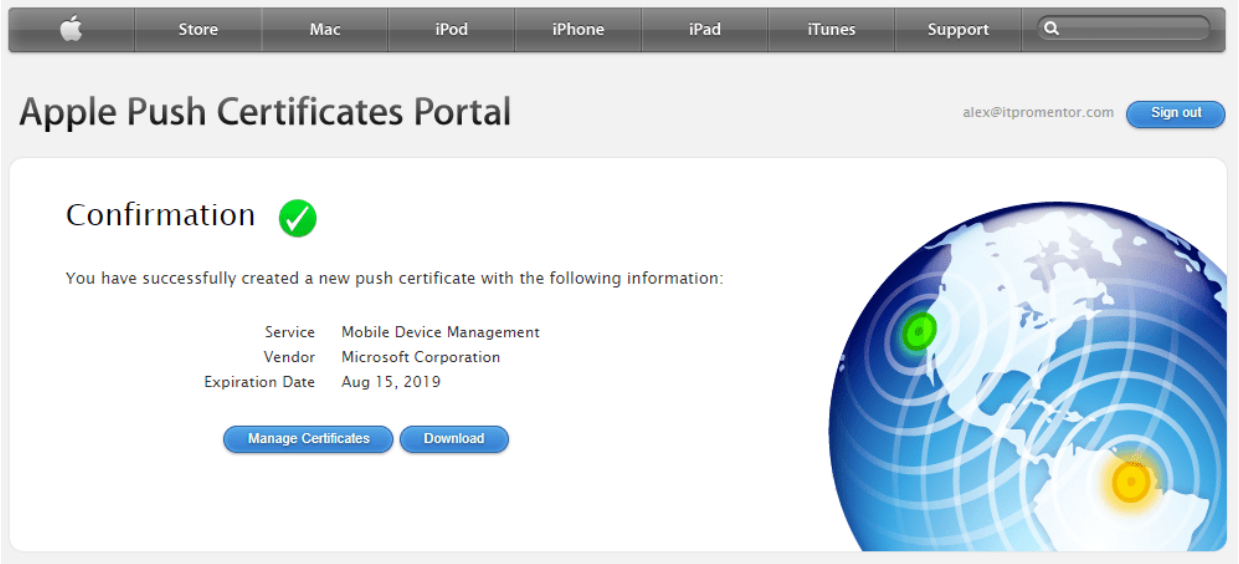
1. Configure iOS enrollment certificate
2. Create Device compliance policies
3. Create Device configuration profiles
4. Create Conditional Access policies
5. Enroll devices

1. Configure iOS enrollment certificate

From the Device management portal, go to **Device enrollment > Apple enrollment > Apple MDM Push certificate**.



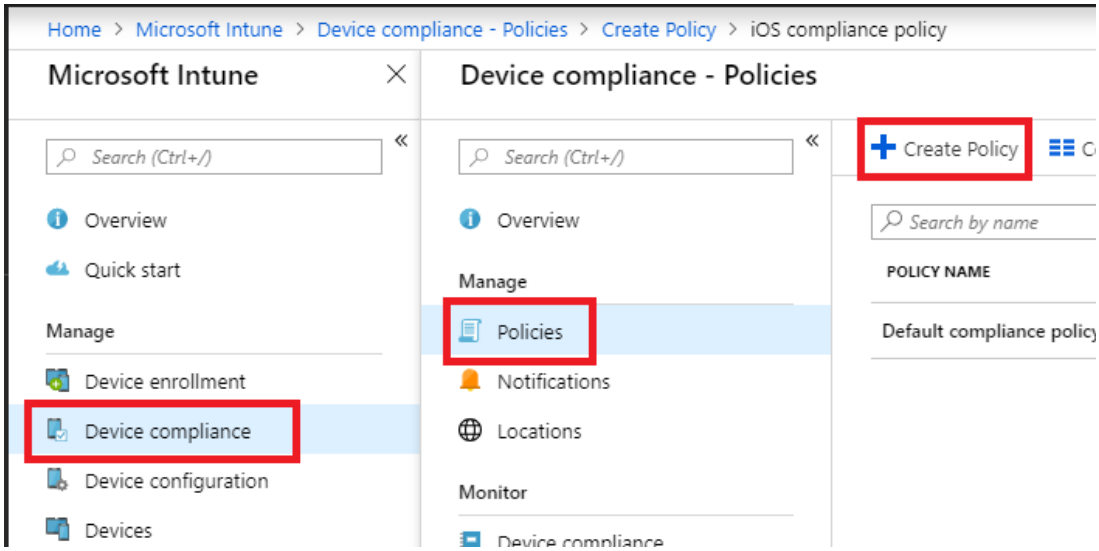
Simply follow the process laid out on this page—basically you just need to download the CSR (Certificate Signing Request) from Microsoft, then hop over to the Apple portal, logging in with an Apple ID that is registered to an admin account at your organization. If you need to register a corporate email account with Apple and create a new ID, see this article from Apple.



Upload the CSR to Apple, and then download the certificate that Apple provides you with. You will return to the Microsoft 365 Device management portal and upload the certificate here.

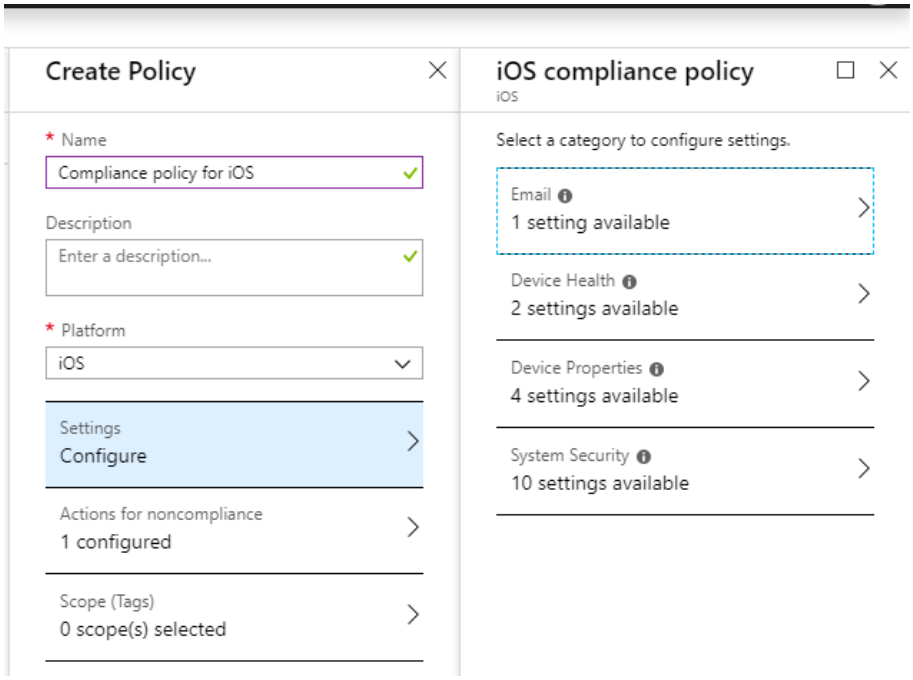
2. Create Compliance policies

You should configure at least one compliance policy for each platform. Go to **Device compliance > Policies > Create Policy**.

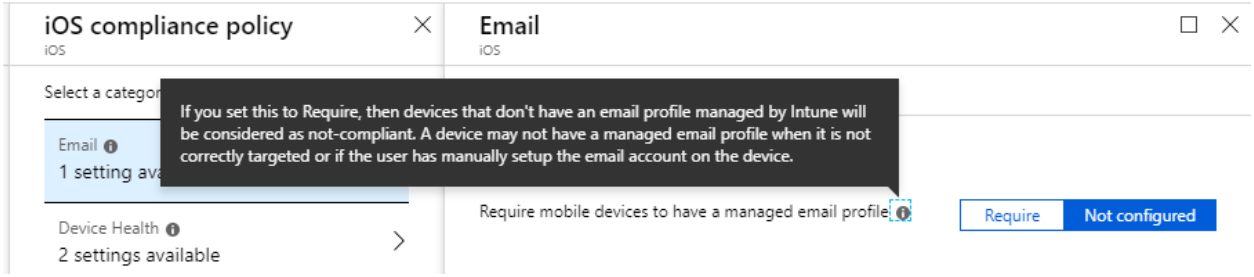


You can only select a single platform for any given policy. You will notice that Windows, iOS, Android, and even macOS have support in Microsoft Intune/Device management. You would want to create policies for each type of device that you expect to have in the organization.

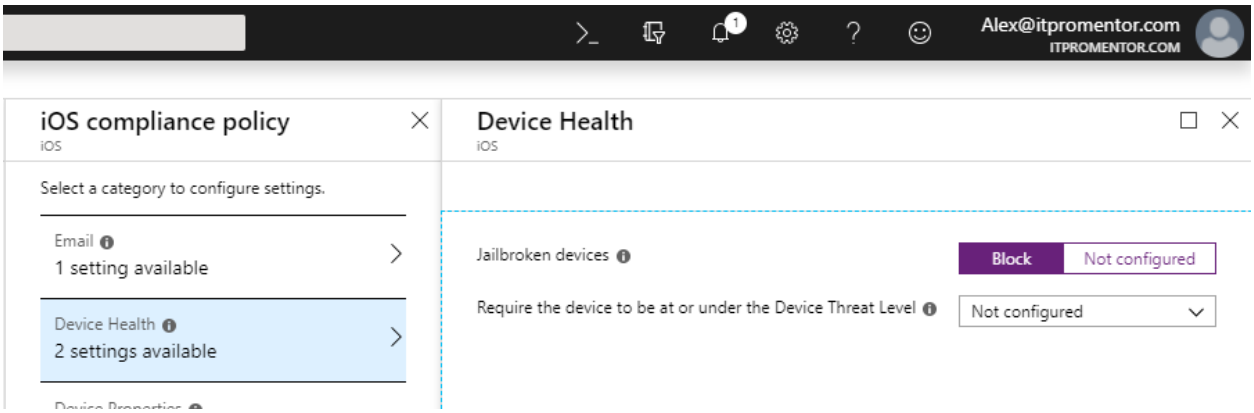
In this example I have selected iOS, but they are all very similar in how they work.



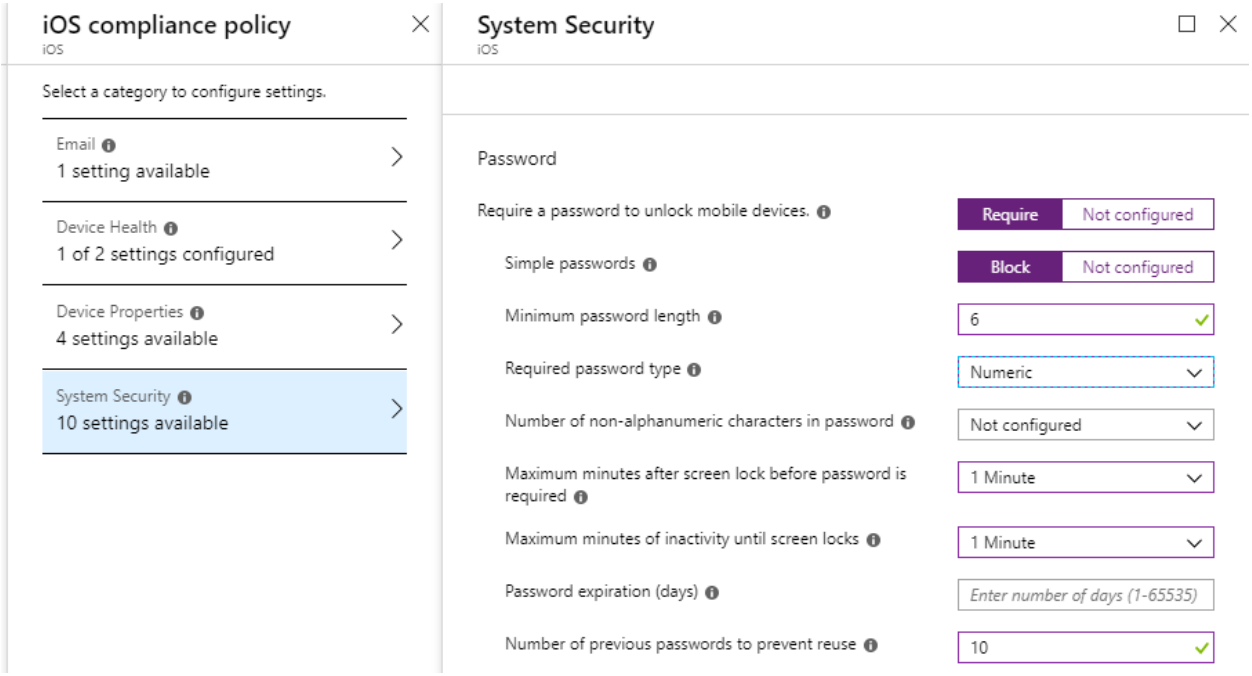
Check out **Settings > Email**. From here, you can tell Intune to require a managed email profile. Note: this means the native mail app on the device. In this example, we will **Require** the managed email profile.



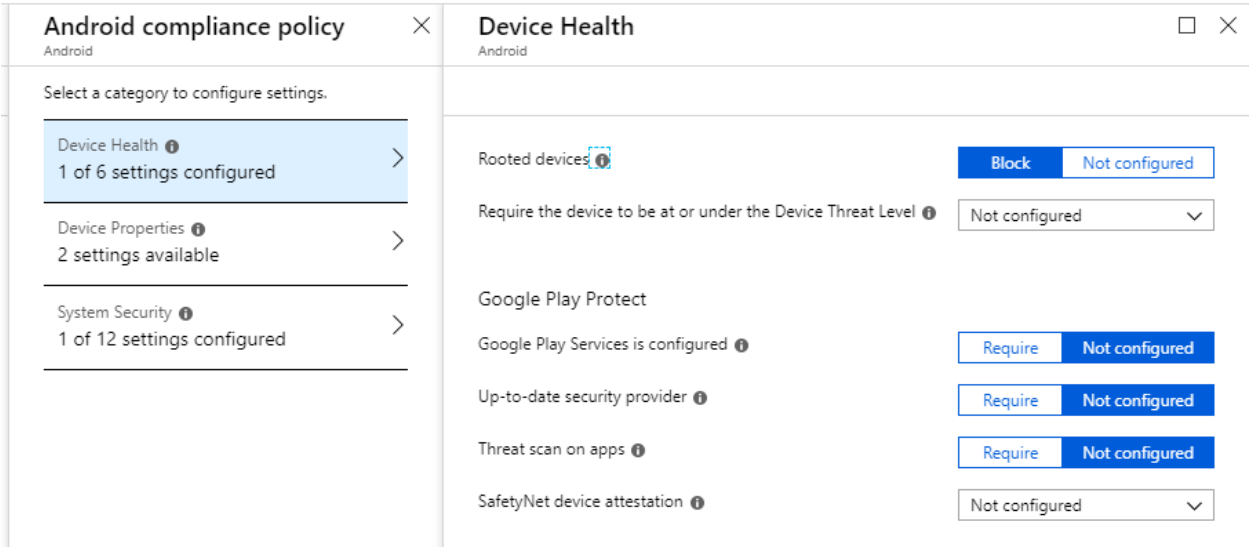
Under **Device Health**, we can choose **Block** for *Jailbroken devices*.



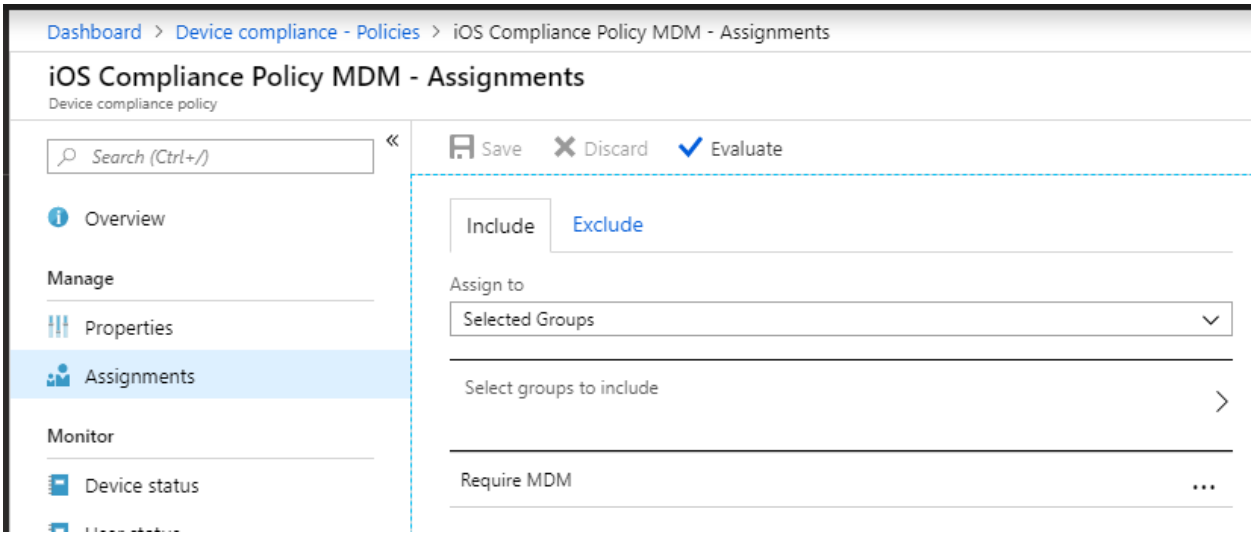
System Security is where you can set a passcode requirement and associated parameters.



Android policies (or any other platform) basically work the same way as what we're depicting here with an iOS-targeted policy. But, you will find differences in the settings available because different platforms will provide different options. For instance, you may see references to Google Play and other Android-specific settings.

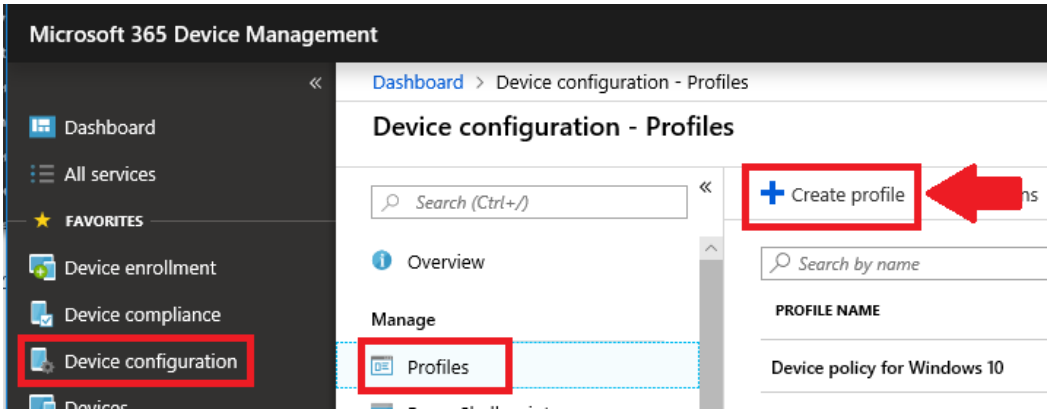


Once you have your policies all configured, you will need to scope them to specific groups. This is done under **Assignments**. Don't skip this step or your users will not fall under the requirements of the policy! After you have assigned it either to *All users* or *Selected groups*, such as *MDM Users*, **Save** the selection.



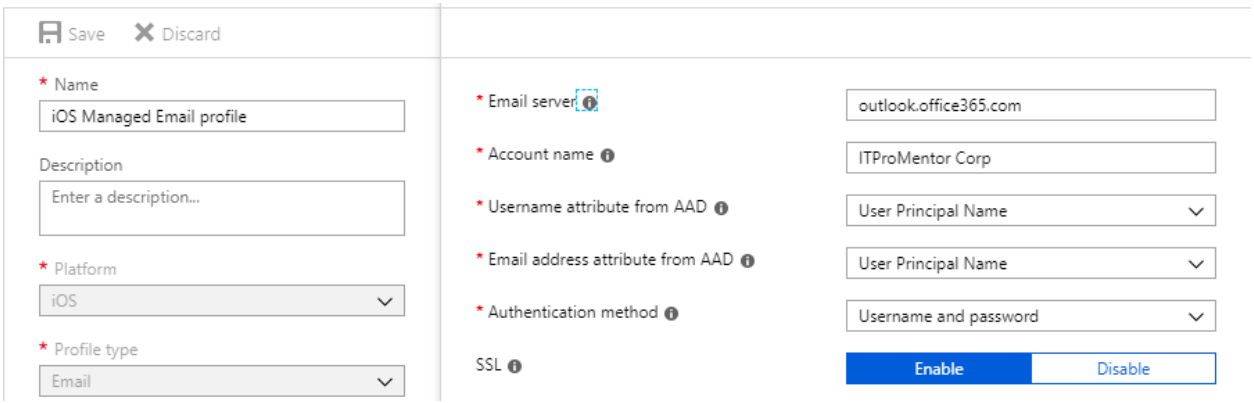
3. Create Device configuration profiles

Device configuration profiles allow you to manipulate specific settings on devices. You can enforce device restriction policies, or push Wi-Fi or Email profiles to the device.

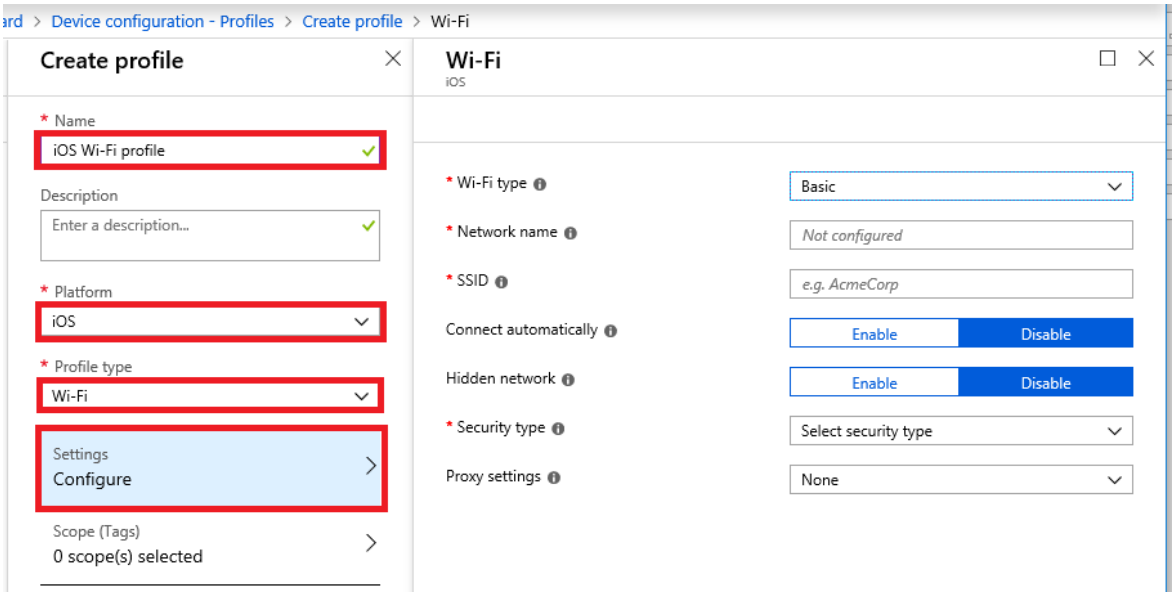


To continue with our example, to create a new device configuration profile, navigate within the device management portal to: **Device configuration > Profiles > Create profile**. Give it a descriptive **Name** such as *iOS Managed Email profile*.

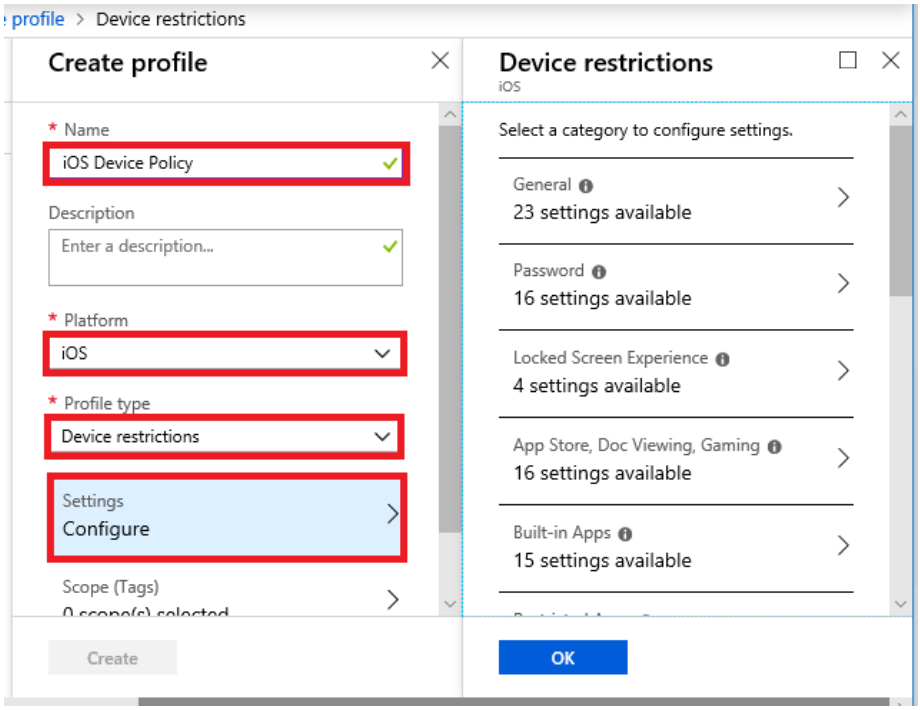
Choose ***iOS*** as the **Platform** and ***Email*** as the **Profile Type**. For mailboxes hosted in Office 365, the **Email server** name is ***outlook.office365.com***. You can use the ***User Principal Name*** for both **Username** and **Email address**. Specify ***Username and password*** as the **Authentication method**.



Optionally, it is possible to create an additional iOS policy that pushes a Wi-Fi profile to the device, if you have a corporate Wi-Fi that you wanted to pre-configure for auto-connection, for example.

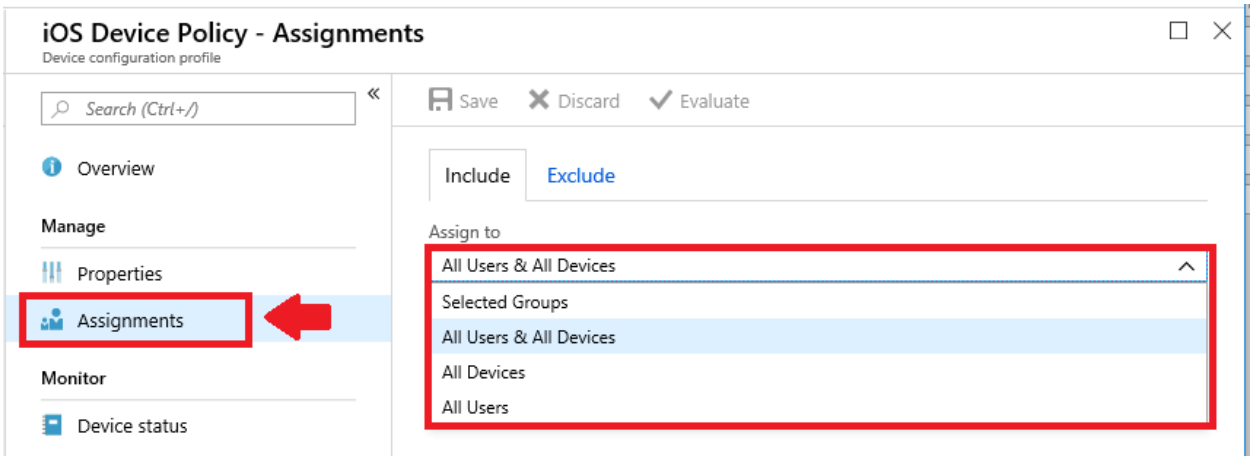


Optionally, you can also create another policy selecting ***Device restrictions*** as the **Profile type**. This allows you to control a great many other settings.



Again, the specific options will look different depending on the platform you select.

Once you have made all your selections for any given policy, under **Assignments**, you can assign the policy to either **Selected Groups** or alternately, **All Users and/or All Devices**.



This makes it possible to configure multiple policies, scoped to different groups, or even have more than one policy scoped to the same groups.

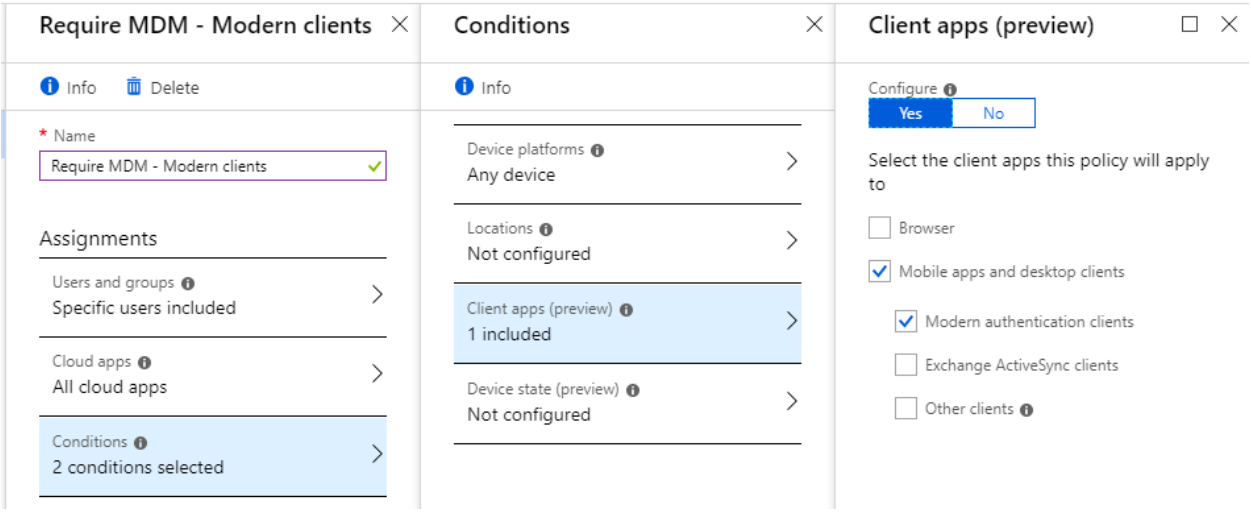
4. Create Conditional access policies

Conditional access enforces the requirements that you set within your compliance policies. In other words, devices which do not meet compliance, do not get access. This makes it a pretty powerful control. Create a new Conditional Access policy from the **Device management portal > Conditional access**. Name the policy something descriptive such as *Require MDM – Modern clients*.

Under **Assignments**, select the **Users and groups** to whom the policy will be applied.

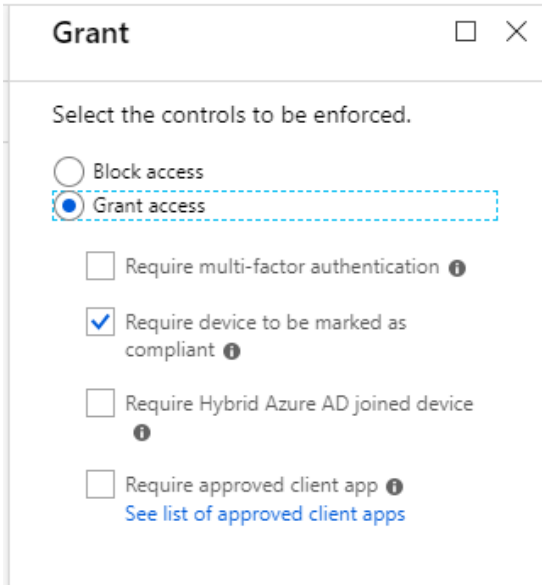
For **Cloud apps**, you can certainly choose **All cloud apps** to protect apps across the board, including Exchange Online, SharePoint/OneDrive, Teams, etc., or, select specific cloud apps such as Exchange Online, if, for instance, you only want to require MDM for access to email.

Under **Conditions > Device platforms**, select ***iOS*** and ***Android***. Optionally, you can choose ***All devices*** if you intend to require enrollment of all Windows and Mac clients, also.

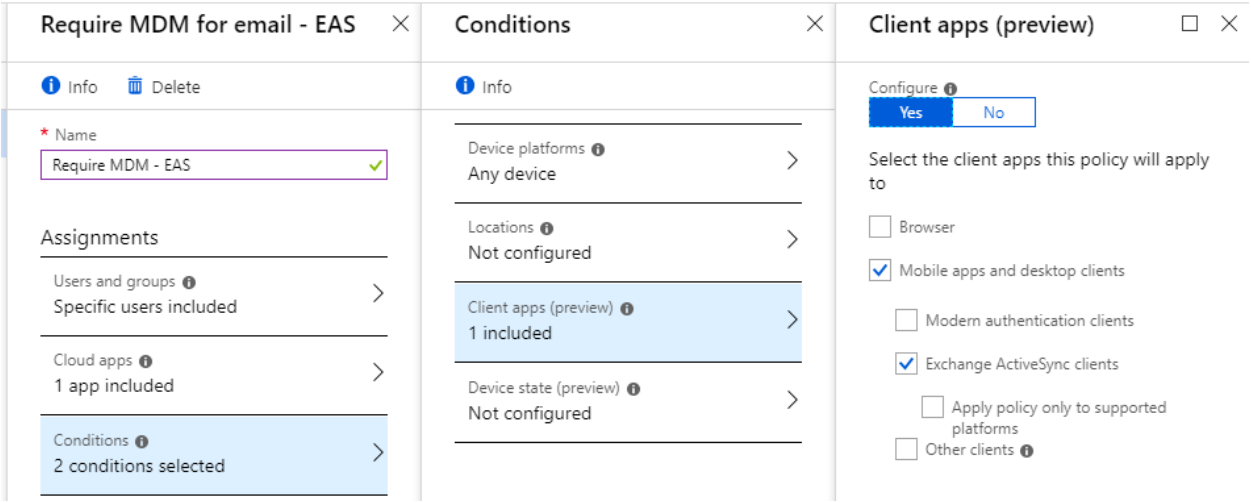


Finally, under **Client apps** select only **Mobile apps and desktop clients > Modern authentication clients**.

Saving all those selections, scroll down to the **Access controls** blade and pick **Grant access** with the option: ***Require device to marked as compliant***.



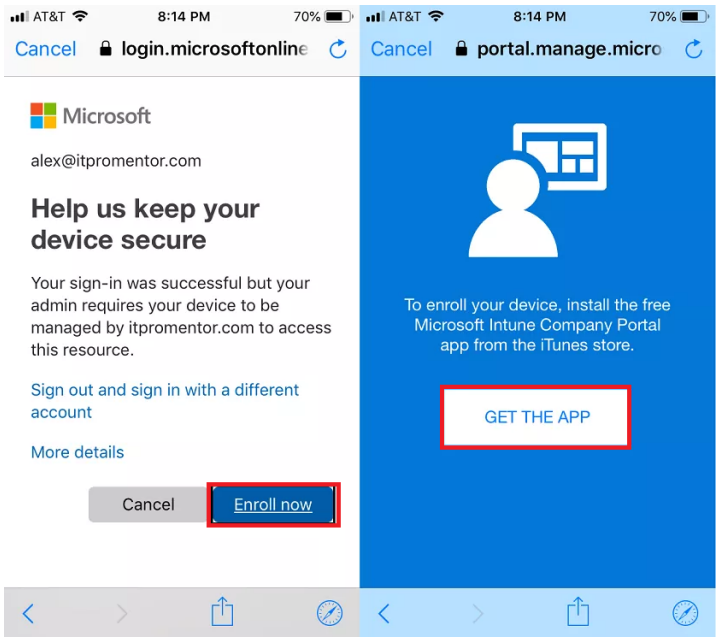
Save all your selections and **Enable** the policy. Now you need to create the same policy again, but for EAS clients. The only difference with targeting EAS clients, is that you cannot choose any other conditions besides the **Client apps** condition, and you may specify no other cloud applications besides **Office 365 Exchange Online** (so **All cloud apps** doesn't mean anything to EAS).



Just target **Mobile apps and desktop clients > Exchange ActiveSync clients**. Require the same access control as before to enforce compliance with Intune, then save and **Enable** the policy.

5. Enroll devices

With a proper Conditional Access policy, users will receive a prompt as they attempt to add an email profile to the device, which will in turn direct them to download the **Intune Company Portal** app from the app store, to complete the enrollment.



Note: If multi-factor is enabled, then the end-user will also need to have the Microsoft authenticator app handy.

Of course, you can also just obtain the **Intune Company Portal app** via the app store and enroll from there, without attempting to add an email profile first. A fair warning: there are a good number of screens that the user must step through to enroll the device, always selecting options in the affirmative such as *Continue*, *Trust*, *Enroll*, *Accept*, *Install*, etc.

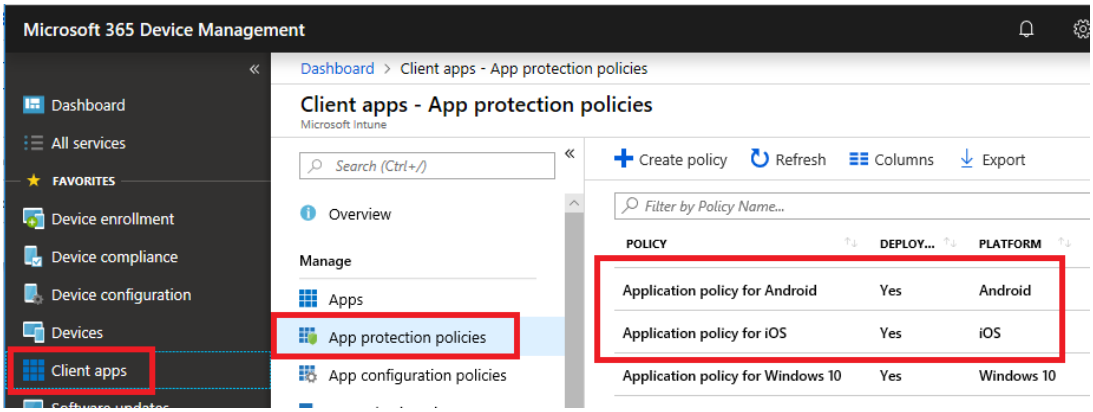
☐ Method #4: Mobile Application Management (MAM)

Secure Score impact:
- App protection/WIP policies (+10 per device platform)

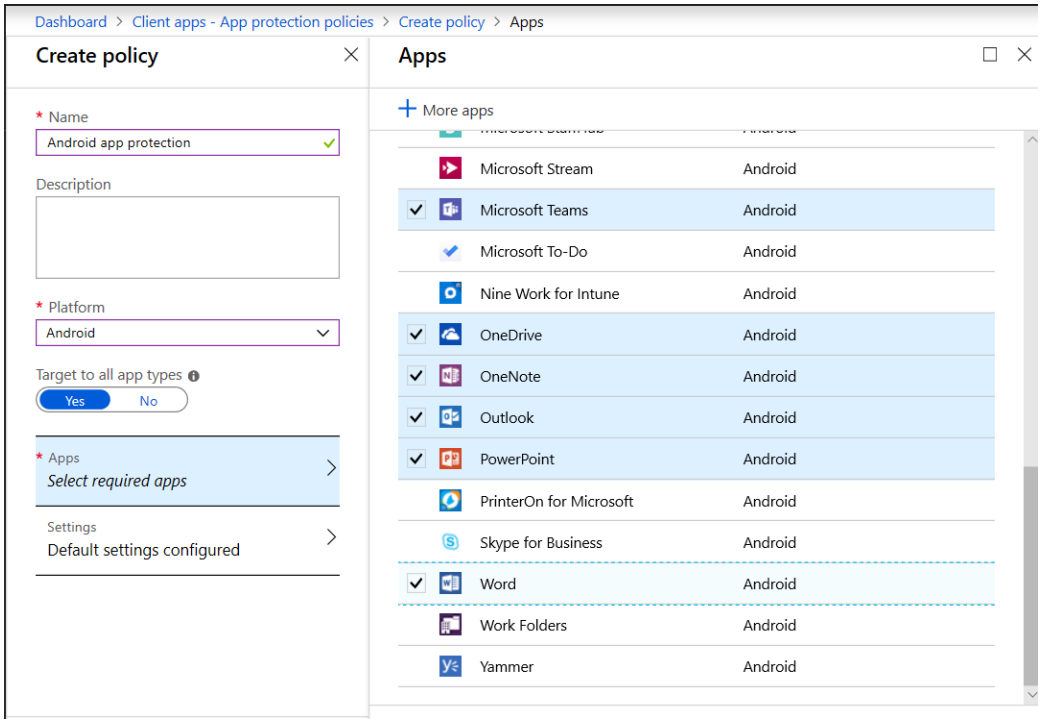
If you choose to use MAM rather than MDM, you are choosing to use the Outlook app for Android and iOS, rather than the built-in email clients for these platforms. The benefit of MAM is that you do not have to enroll devices and it is therefore a good "bring your own device" (BYOD) management solution. Here is a chart comparing MDM and MAM:

Mobility Concerns	MDM solution (corporate-owned)	MAM solution (user-owned)
Unauthorized data access	Require device enrollment	Require protected app
Compromised account	Require device PIN	Require app PIN
Compromised device	Encrypt device data	Encrypt app data
Jail broken device	Require compliant device	Check for jailbreak on app launch
Lost or stolen device	Wipe device data	Wipe app data
Termination of employment	Wipe account data	Wipe app data
Prevent data leakage	Manage device apps	Restrict copy/paste/save

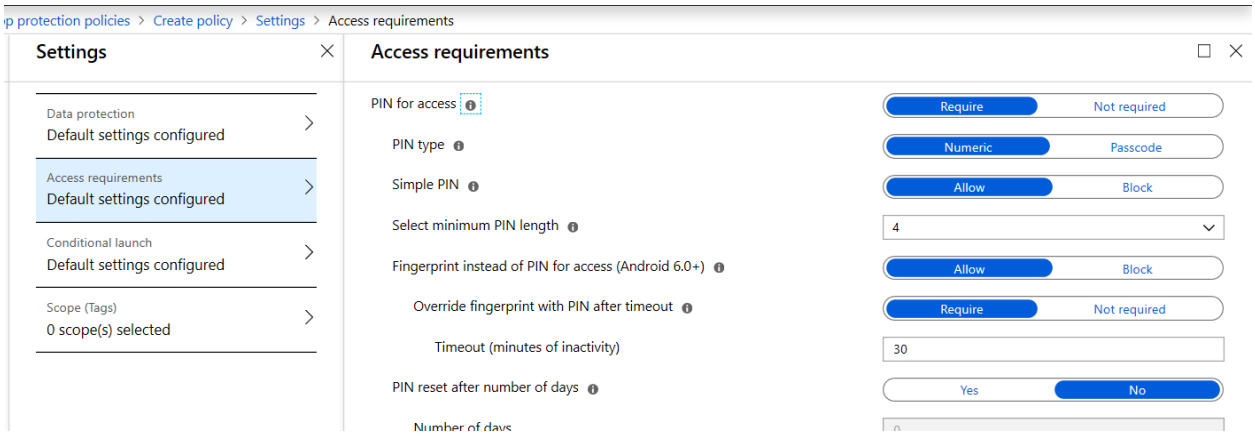
Find MAM policies in the Device management portal, at https://devicemanagement.microsoft.com **> Client apps > App protection policies**.



Choose **Create policy** if one does not yet exist. Give it a descriptive name such as **Android app protection**, selecting **Android** as the **Platform**, and selecting the apps to which you want the protections to apply (**Outlook** at the very least, and optionally others e.g. OneDrive, OneNote, Teams, etc.).



In a typical baseline policy, you may simply accept the defaults under **Settings**. But look through the options and make any adjustments as you see fit.



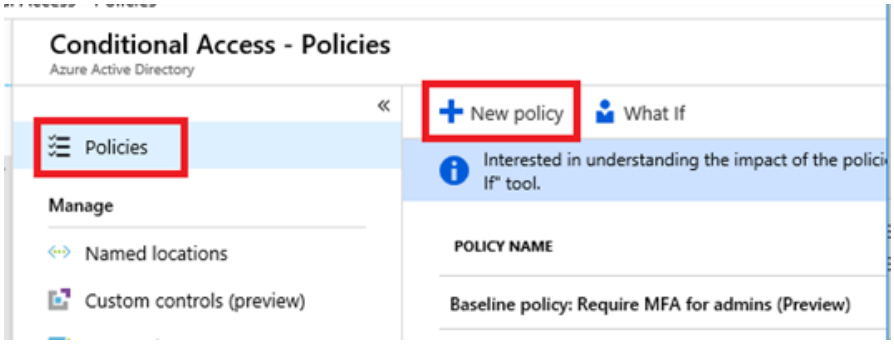
After you save your selections and **Create** the policy, be sure to go back into the policy and select **Assignments** (so that the policy is applied to **All Users** or another subset of users).

When done, choose **Save**. Now repeat the process for enabling iOS app protection.

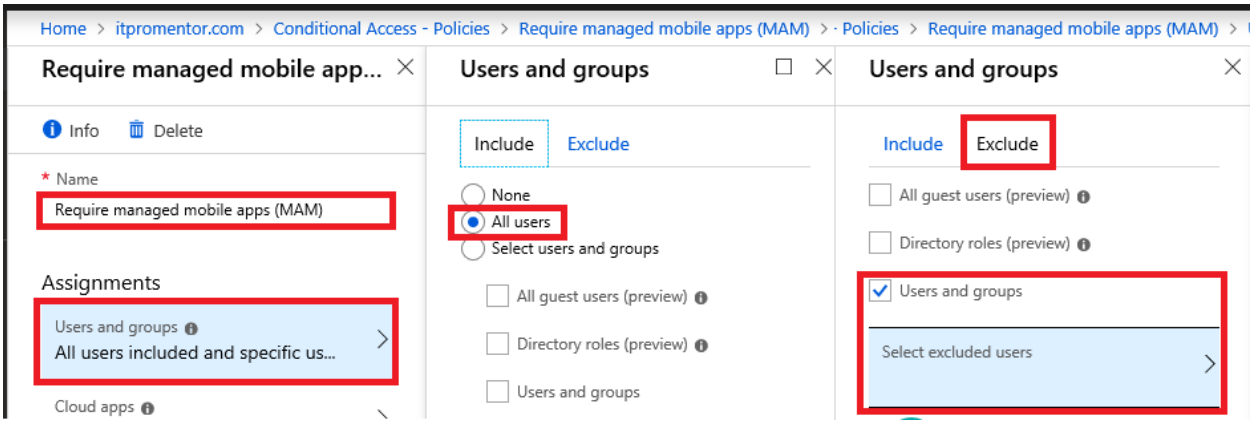
Next configure two Conditional access policies: one that targets modern authentication clients, and one that targets Exchange ActiveSync clients.

> ***Warning***: *If the user has an existing native mail profile, then enabling this policy means they will get a password prompt—it just stops working. However, if you attempt to add the account as a new profile to the native app, it will display a message to the end-user after sign-in, explaining that the app is unsupported. Therefore, instruct users to move to the Outlook app in advance, if possible, and warn them they should expect to lose access to email on the old app.*

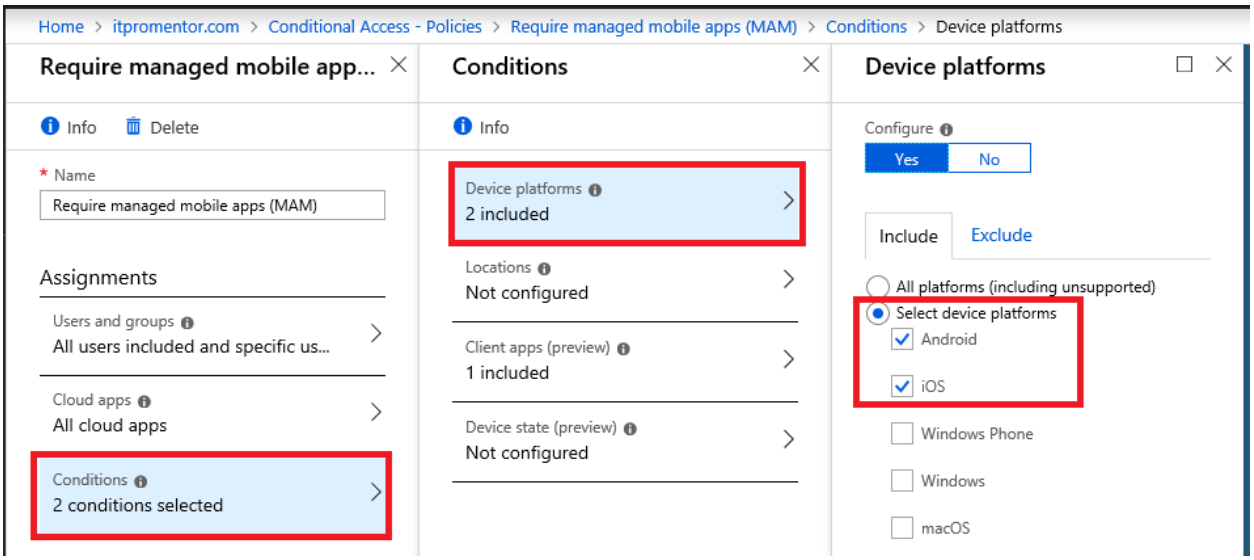
Select **Policies > + New policy**.



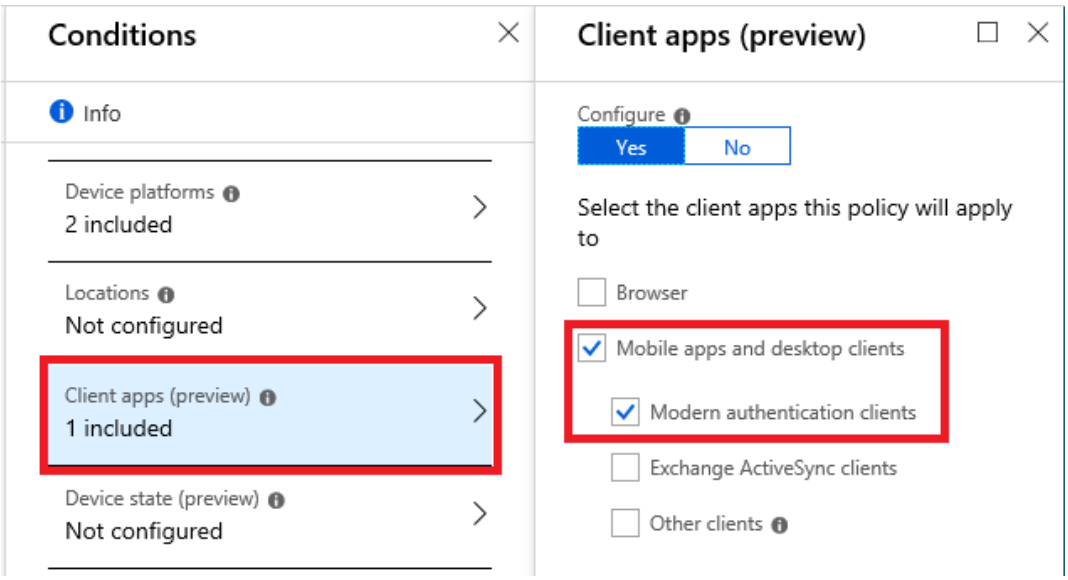
I will name my policy "**Require managed mobile apps (MAM)**" and pick my assignments. I want this policy to apply to **All users**. Otherwise, you can also constrain the assignment to a security group such as *BYOD Users*, populated with individuals who will bring their own mobile devices.



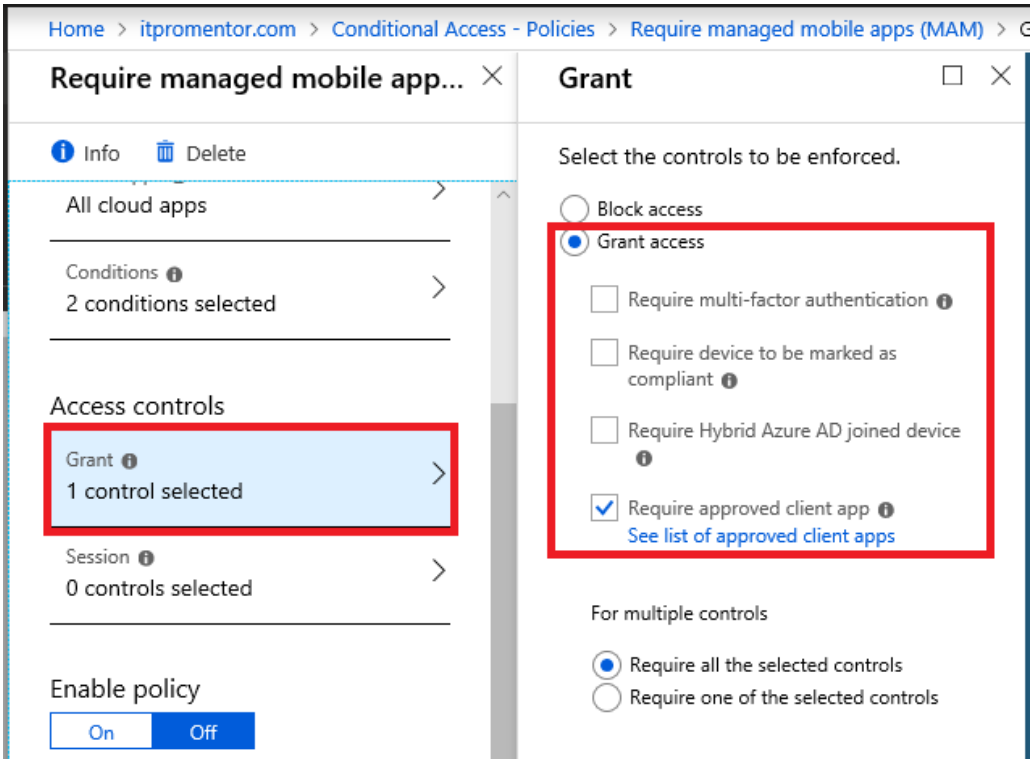
Under **Cloud apps**, choose **Office 365 Exchange Online**. For **Conditions**, under **Device platforms**, select only **Android** and **iOS** (these are the only platforms that support the access control "*Require approved client app*").



The only other condition you need to specify is **Client apps**; select **Mobile apps and desktop clients** and the option for **Modern authentication clients** only.



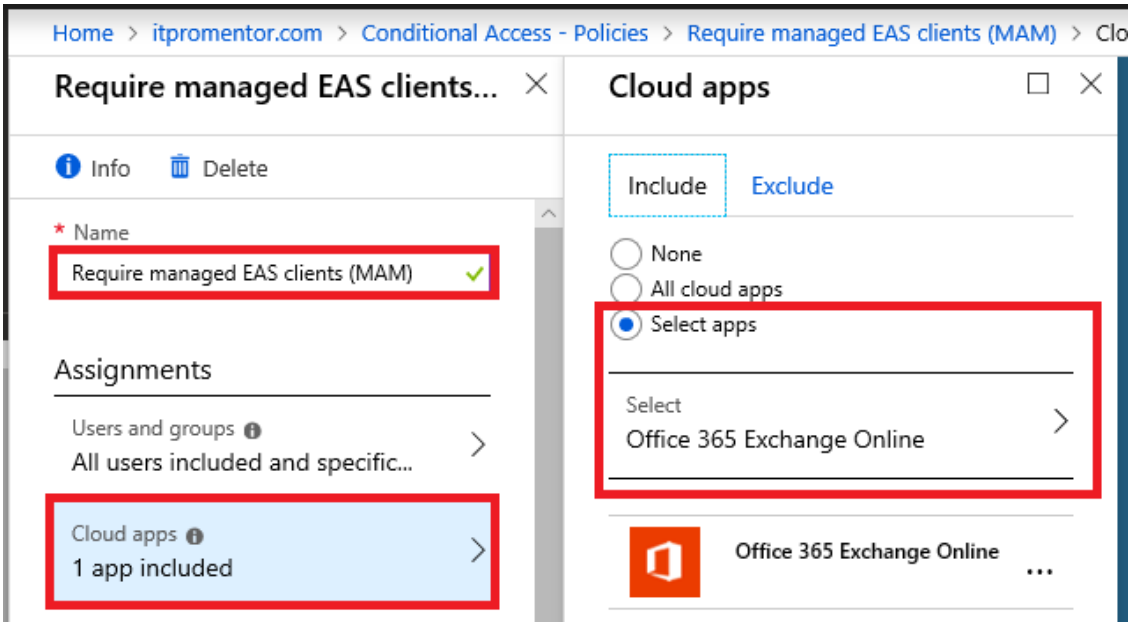
Now, under **Access Controls**, pick **Grant** and make the selections pictured—**Require approved client app** and **Require all of the selected controls**.



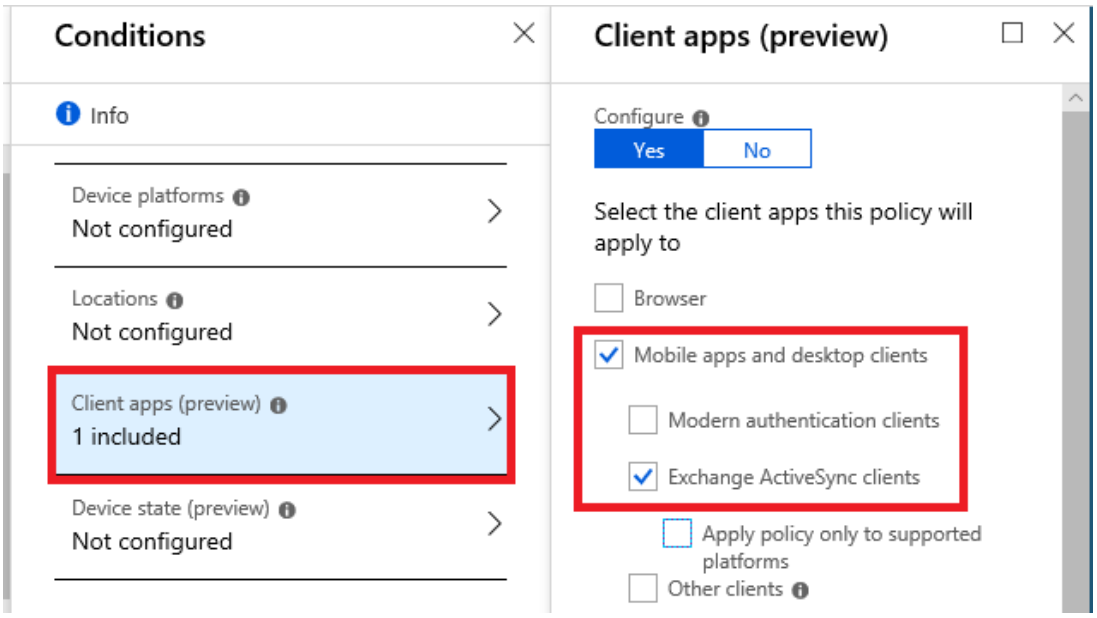
Microsoft does not support mixing Exchange ActiveSync (EAS) client targeting with any other conditions or client types. Therefore, we need a second policy to protect EAS clients, or those which do not support modern authentication.

Create a new policy. Name it something descriptive like *Require managed EAS clients (MAM)*. I will again assign the policy to **All users**, excluding an emergency admin account. Or, again, an alternative group such as *BYOD Users*.

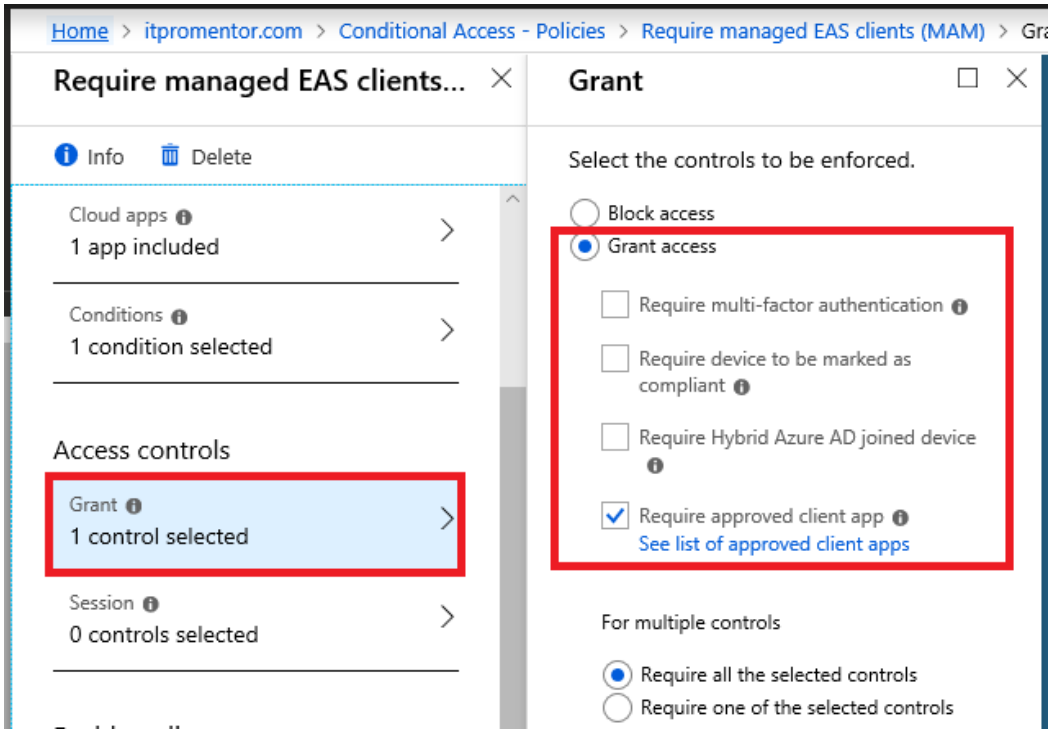
Under **Cloud apps**, select only **Office 365 Exchange Online**.



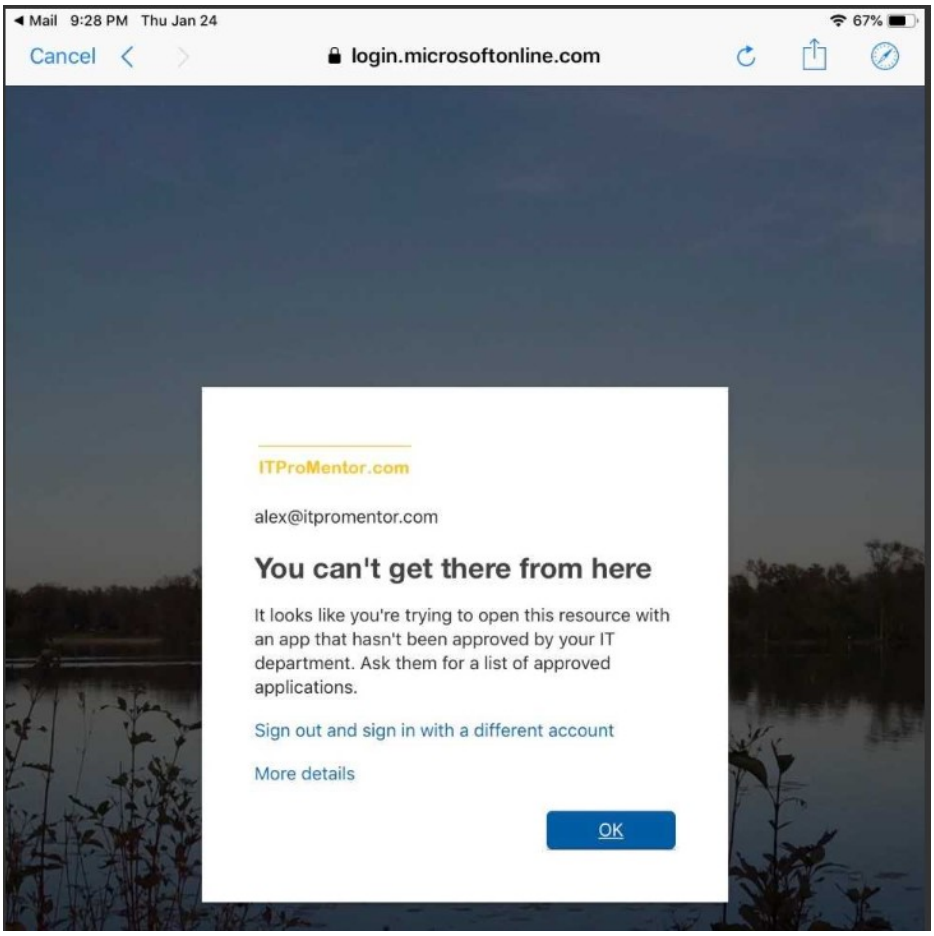
Microsoft does not support mixing EAS-targeted policies with any other conditions, or any other client types. Therefore, under **Conditions**, you will need to make the selections as pictured, for **Client apps** only, **Mobile apps and desktop clients > Exchange ActiveSync clients**.



Finally, based on the **Access controls**, go ahead and **Grant access** with **Require approved client app** as pictured.



After you save your selections and enable these policies your configuration is complete. The experience for end-users is this: adding an email profile to the native mail app on a mobile device will result in the access being blocked, with a message about using a supported app, instead.



☐ Block downloads from Outlook Web on unmanaged devices

Secure Score impact:
- None

If you have configured Device Management not only for mobile devices but also PC's and Macs (this is strongly recommended), then another good Conditional access policy to include may be *Block downloads from Outlook on the Web* (for unmanaged devices).

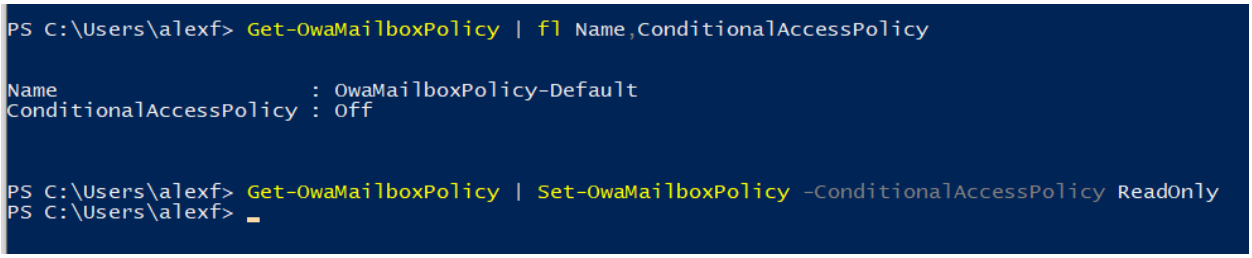
The reason we want to implement this policy is because we have no leverage over unmanaged devices—nor can we wipe them if they are lost or stolen. However, we may still want users to be able to access their resources via the web (e.g. OWA), even from a home PC or Mac.

SharePoint has similar functionality that can be enabled, but here we will target Exchange Online only (e.g. attachments in Outlook). Just know that this same protection can apply to OneDrive and SharePoint data locations also.

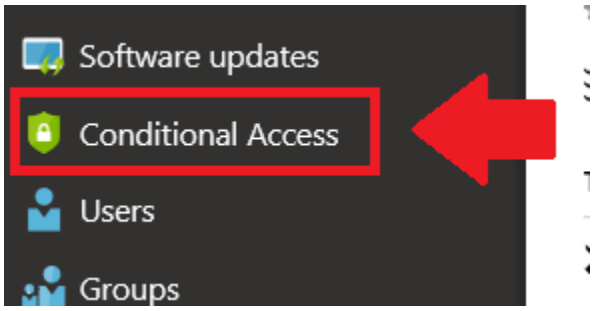
To implement the control requires a change in both the Exchange Online service, as well as a corresponding Conditional access policy.

First enable “ReadOnly” mode for Outlook on the Web:

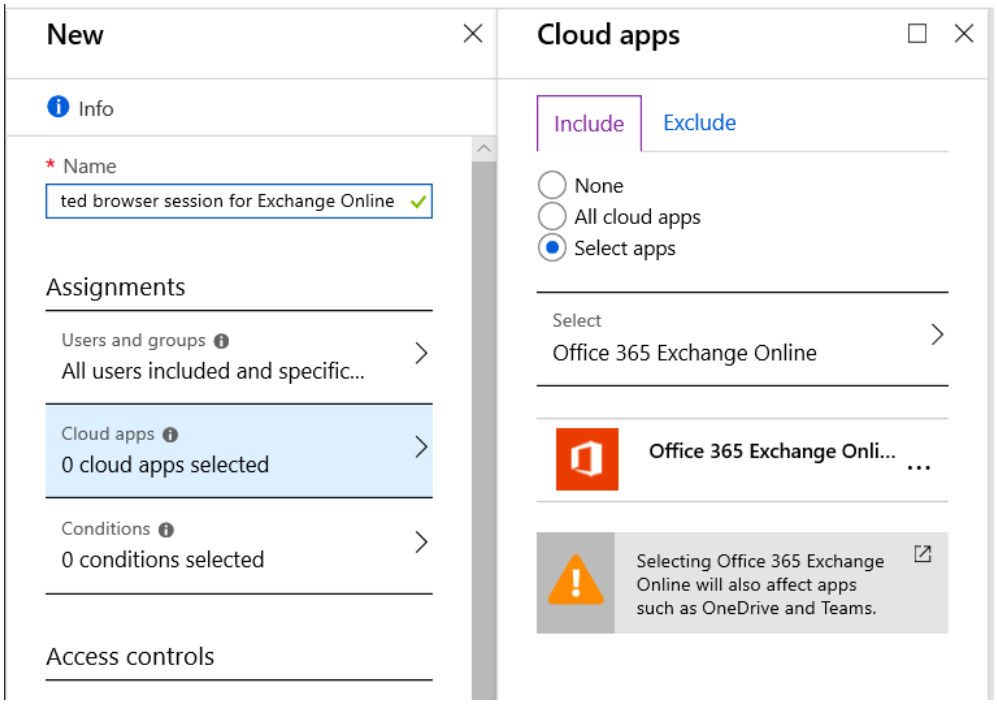
```
Get-OwaMailboxPolicy | Set-OwaMailboxPolicy -ConditionalAccessPolicy ReadOnly
```



Second, create a Conditional Access policy. From either the Device management or Azure AD Admin portals, find **Conditional Access** on the left menu.

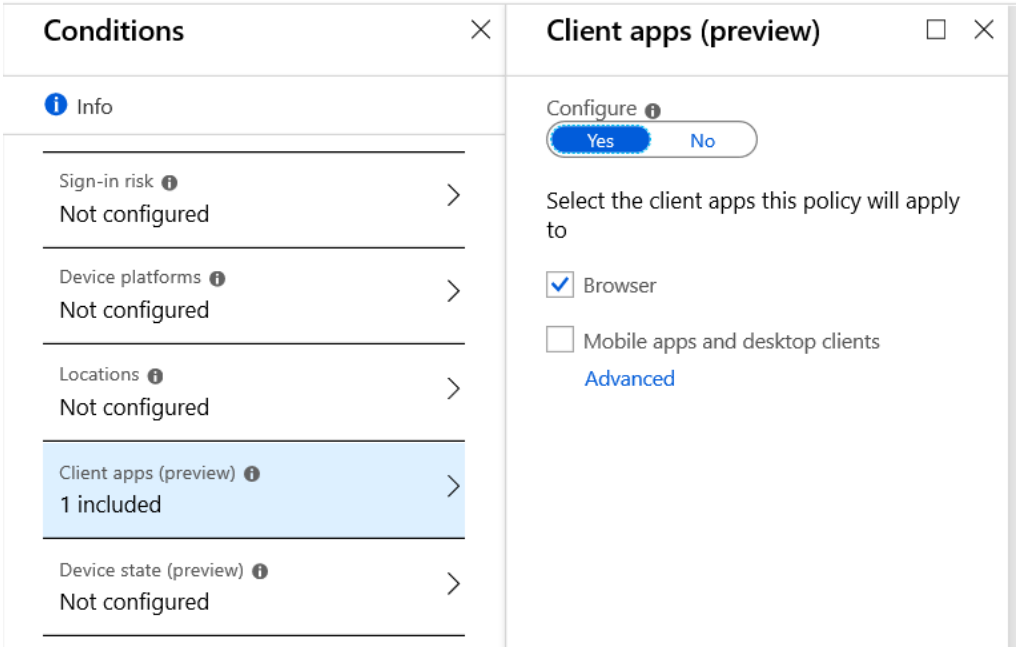


Next, create a **New Policy**, and give it a descriptive name such as “Limit browser sessions for Exchange Online” or whatever you like.

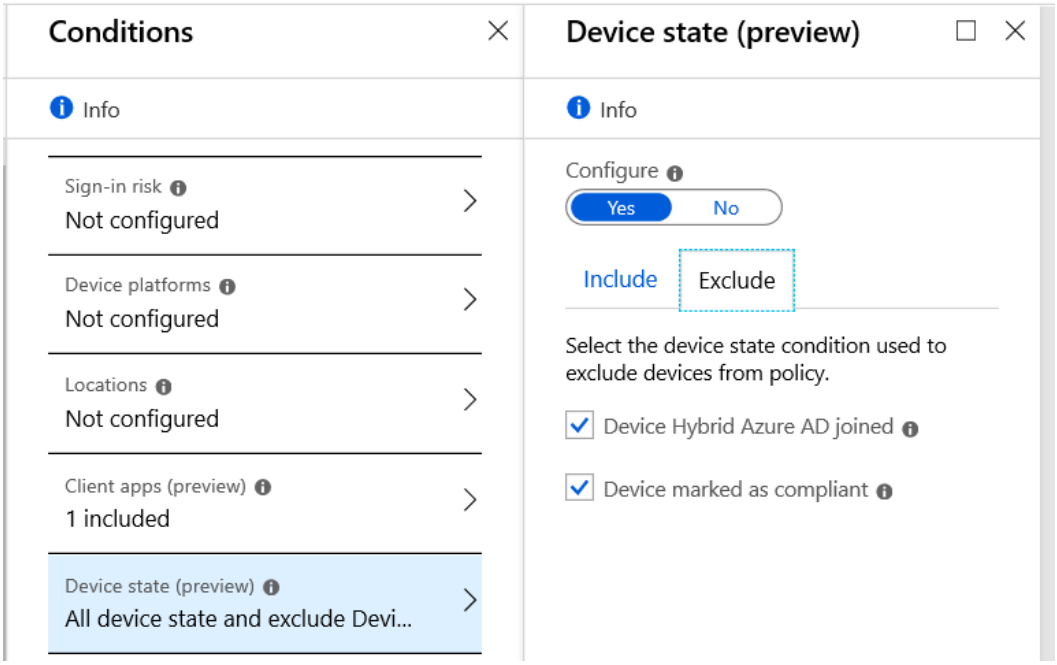


You can apply the policy to **All users** and choose your Cloud app: **Office 365 Exchange Online**.

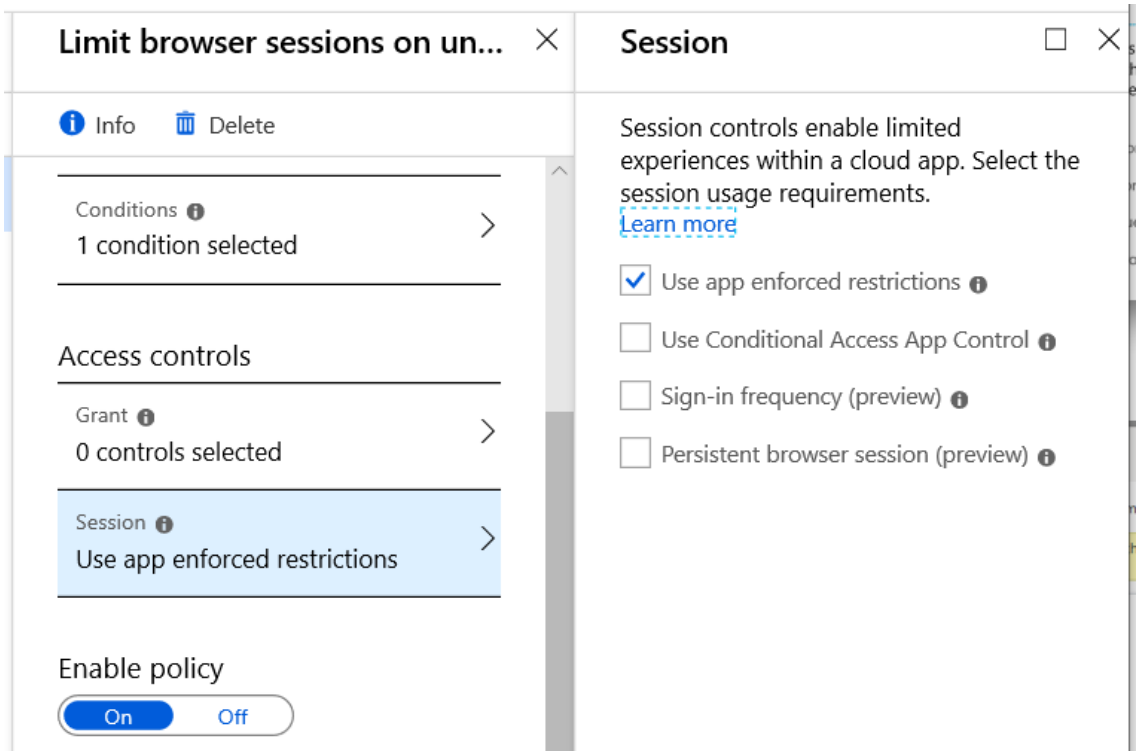
Note: This access control also can be applied to Office 365 SharePoint Online, however you can have the SharePoint admin center automatically create the necessary rules for you. See this article for more details.



Continuing on with the policy, for client apps, you must only select **Browser** (it is the only client app to which this access control applies anyway). You can also exclude managed devices under **Device state > Exclude** tab.



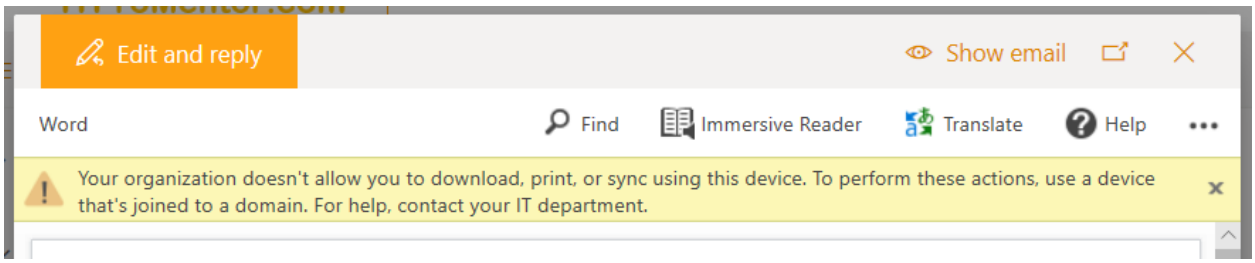
Then under the **Access controls > Session** blade, you must choose **Use app enforced Restrictions**.



Save your selections and **Enable** the policy (set it to **On**).

The result of this policy can be tested. From an unmanaged computer, open Outlook Web Access in Office 365, choose an email with an attachment, and see the banner at the top which reads:

> *Your organization doesn't allow you to download, print or sync using this device. To perform these actions, use a device that's joined to a domain. For help, contact your IT department.*



☐ Start using Office 365 Message Encryption features

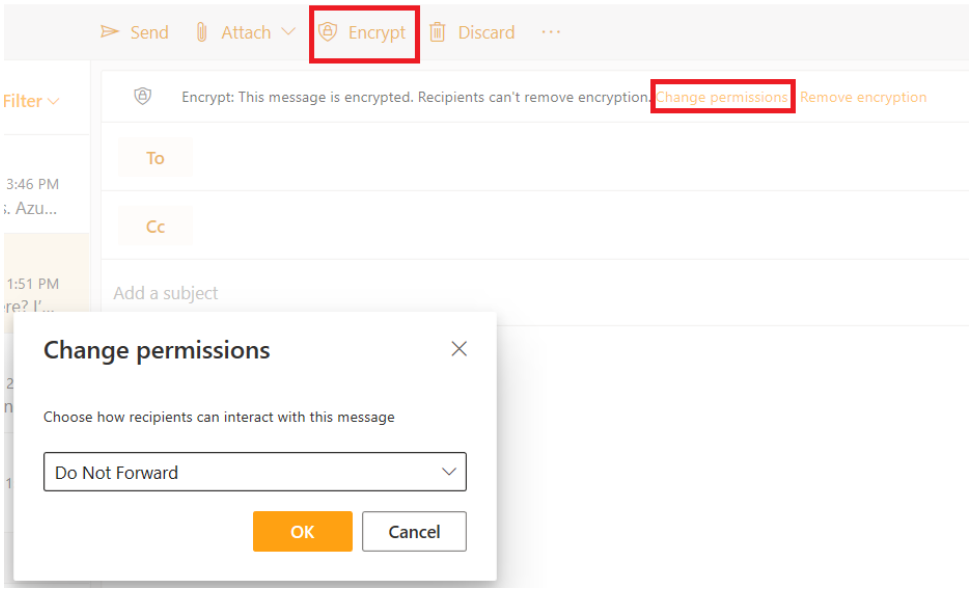
Secure Score impact:
- Activate Information Rights Management (IRM) services (+10)
- Apply IRM protections to email (+5)

Email encryption is available as part of Office 365 plans that include Azure Information Protection P1 (Office 365 E3 or E5, Microsoft 365 Business, or any Enterprise Mobility + Security bundle). Most of these features are now enabled for new tenants out of the box. Message encryption enables users to protect email messages and draw boundaries around certain communications (e.g. I want to share this with you, but I don't want you to share it with someone else).

To enable the option to display an "Encrypt" button in Outlook Web Access –by default, this value is set to $false, and we just need to flip it to $true:

```
Set-IRMConfiguration -SimplifiedClientAccessEnabled $true
```

Once a user clicks on **Encrypt**, the default template that is applied is *Encrypt* (also known as *Encrypt Only*). To change this to another template, such as *Do Not Forward*, click **Change Permissions**.

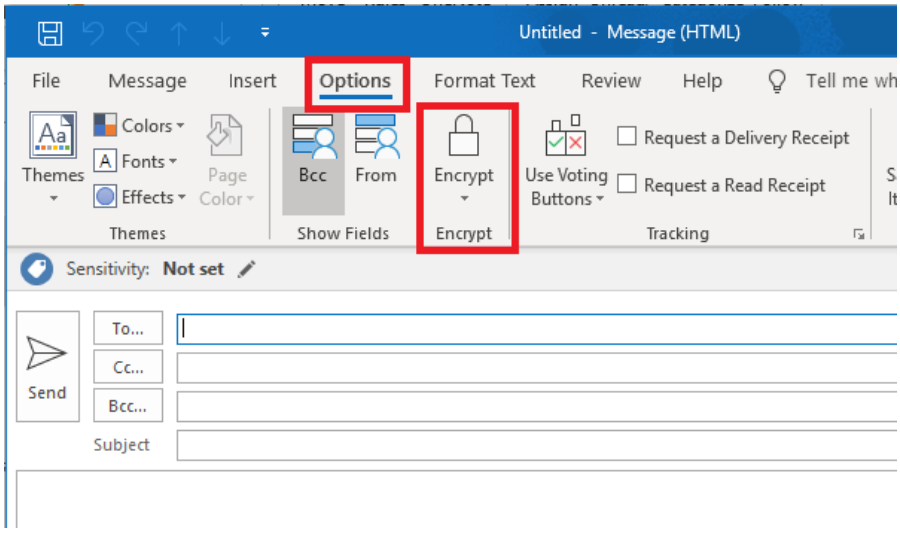


We find four default permissions templates available for sending email messages. They are:

- **Encrypt** – Use this template *only* to encrypt; no other special restrictions will be applied. This is the most popular template for sending encrypted email messages. External recipients are allowed with this template.

- **Do Not Forward** – Recipients of a message marked with *Do Not Forward* permissions will not be able to share, print or copy the message or document. External recipients are allowed with this template.
- **Confidential\All Employees** – Recipients of a message marked with *Confidential\All Employees* permissions can reply to and forward the content within the organization only. It is not possible to share with external users.
- **Highly Confidential\All Employees** – Similar to the above, *Highly Confidential* messages can only be shared within an organization, however, the content is accessible only to the specific individuals with whom the content has been shared. Forwarding to other users either internally or externally is not possible.

Users can access these same templates from the Outlook client. **New message > Options tab > Encrypt**.



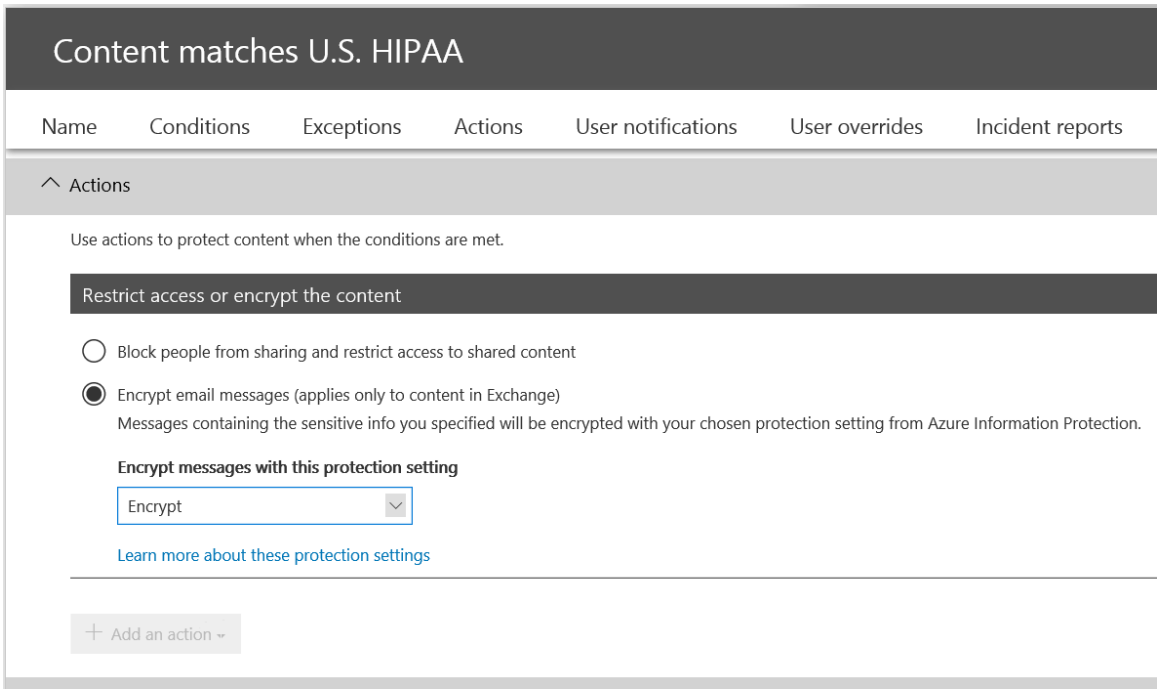
☐ Configure DLP Policy (if applicable)

Secure Score impact:
- Apply data loss prevention policies (+20)

Data Loss Prevention (DLP) can detect when "sensitive information types" are being shared and automatically apply actions based on a policy (e.g. GDPR, credit card data, US HIPAA data, etc.). Capabilities that we have when sensitive information is detected are as follows:

- **Encrypt** – automatically encrypt the content
- **Block** – do not allow the content to be shared or sent externally
    - Optionally allow override of the policy with business justification
- **Notify** – Notify users and/or admins when something is being shared externally, using Policy Tips (informational banners that appear within the application) and email notifications
- **File an incident report** – email an incident report to another mailbox when sensitive content is shared externally

You can choose any of these options individually (e.g. only file an incident report), or combine them—for instance, encrypt *and* file an incident report. Here is one example (auto-encrypt HIPAA data):



Create these policies under **Data Loss Prevention > Policy** in the Security and Compliance center.

Read more about Data Loss Prevention on Microsoft docs, and see additional examples:

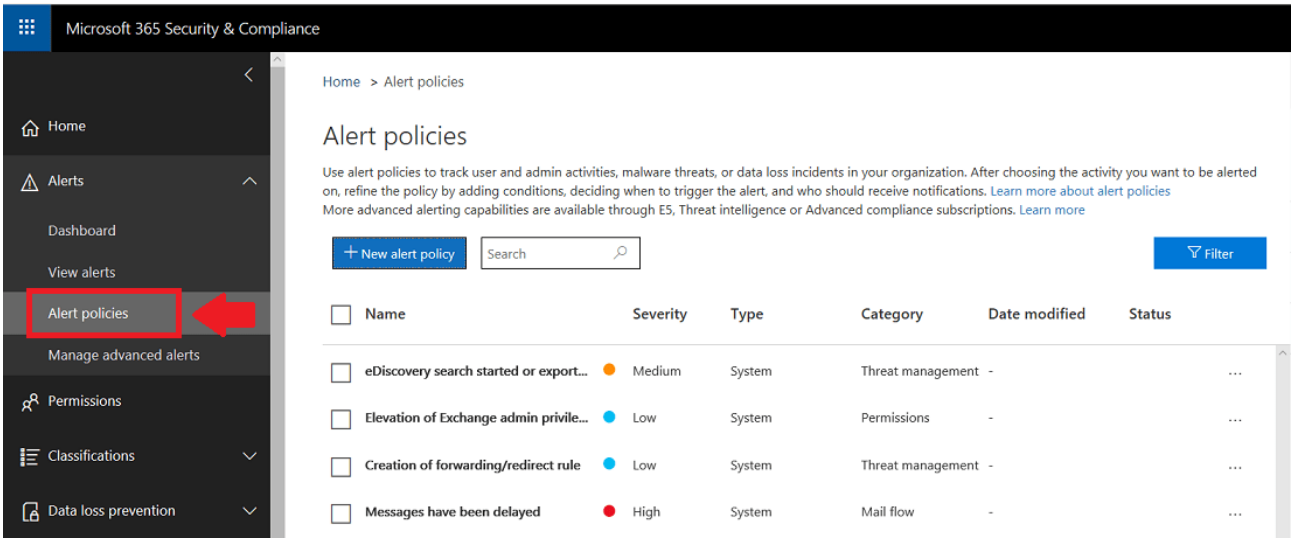
- HIPAA incident reports
- GLBA auto-encryption rule

☐ Enable the default Alert policies

Secure Score impact:
- None

Alert Policies is something that should be on your radar. These will generate email notifications (alerts) when certain events happen in Office 365.

Choose **Alerts > Alert policies**.

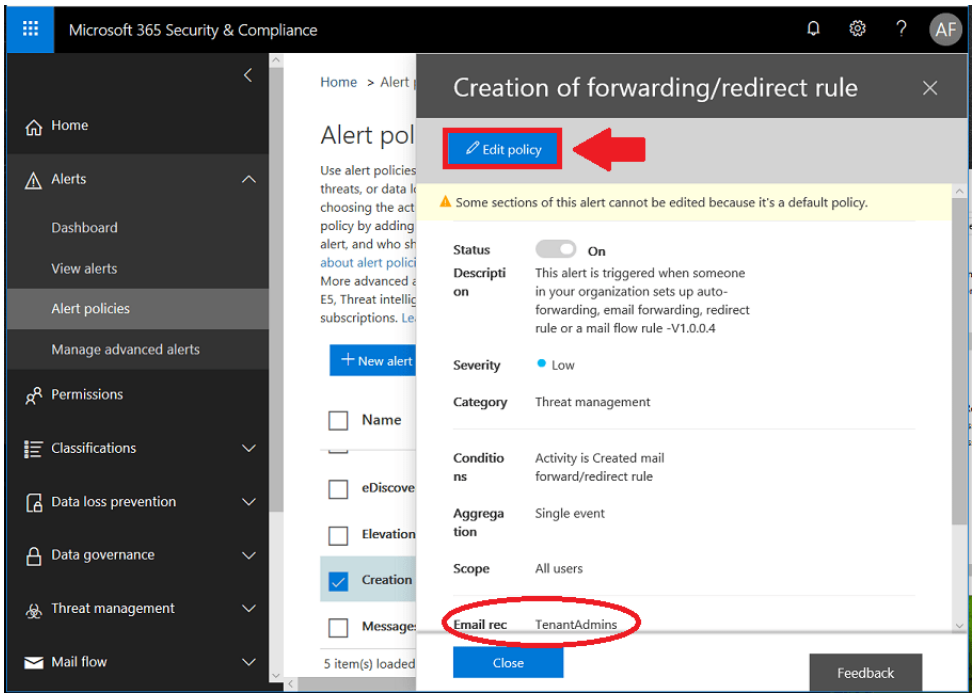


From here, you should see at least a few basic policies which are created by default:

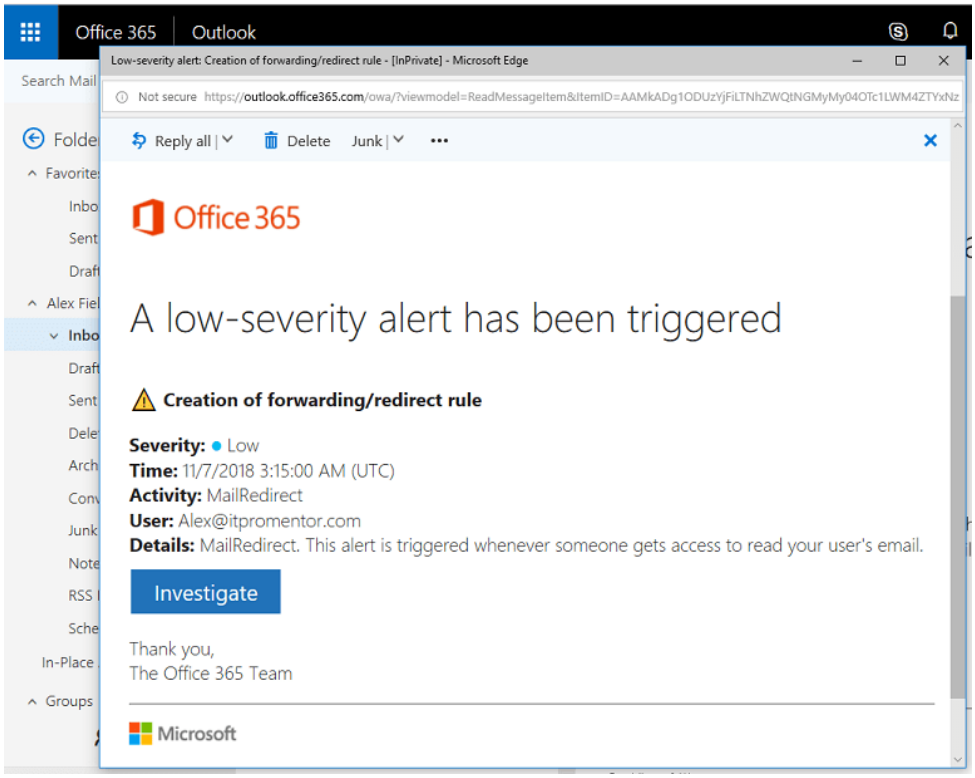
- eDiscovery search started or exported
- Elevation of Exchange admin privilege
- Creation of forwarding/redirect rule
- Messages have been delayed

I especially like *elevation of privilege* and creation of *forwarding/redirect rules* (this is one of the first things attackers will attempt if they gain control of a mailbox account). If you have Office 365 ATP Plan 2 or Office 365 E5, then this screen will include many more alerts. Refer here for more detail on the default policies included with each subscription.

If you don't monitor the inboxes for your tenant admins day to day, then you should probably edit these default policies now, and change the recipients to people who will actually see the alerts and act on them.



When an event occurs, you can expect an email notification like the one pictured below.

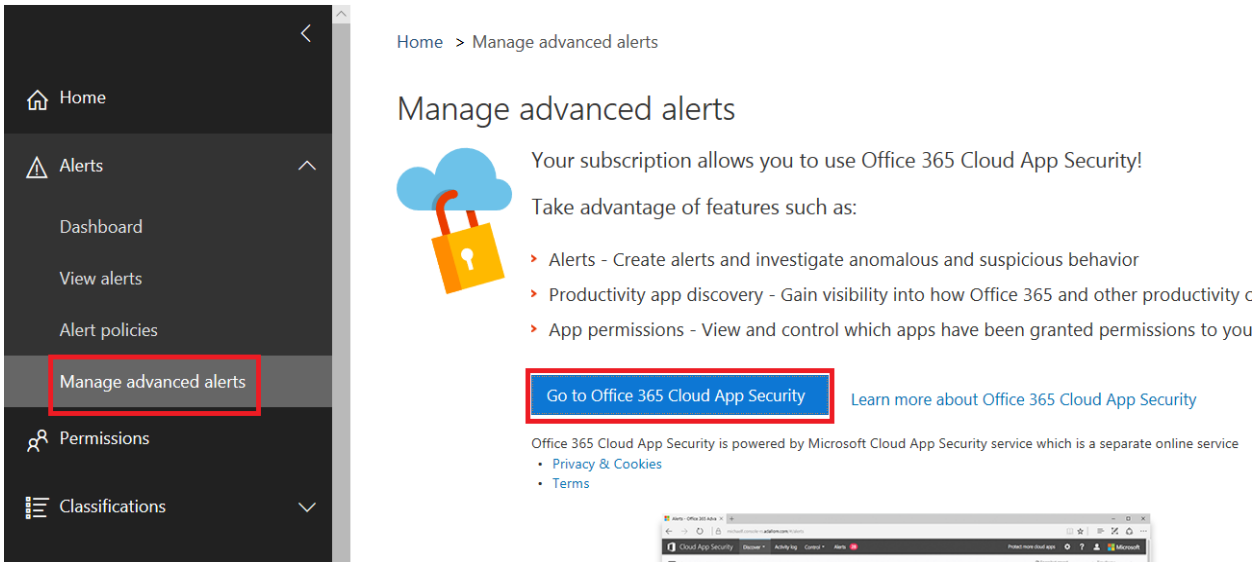


☐ Enable Advanced alert policies within Cloud App Security

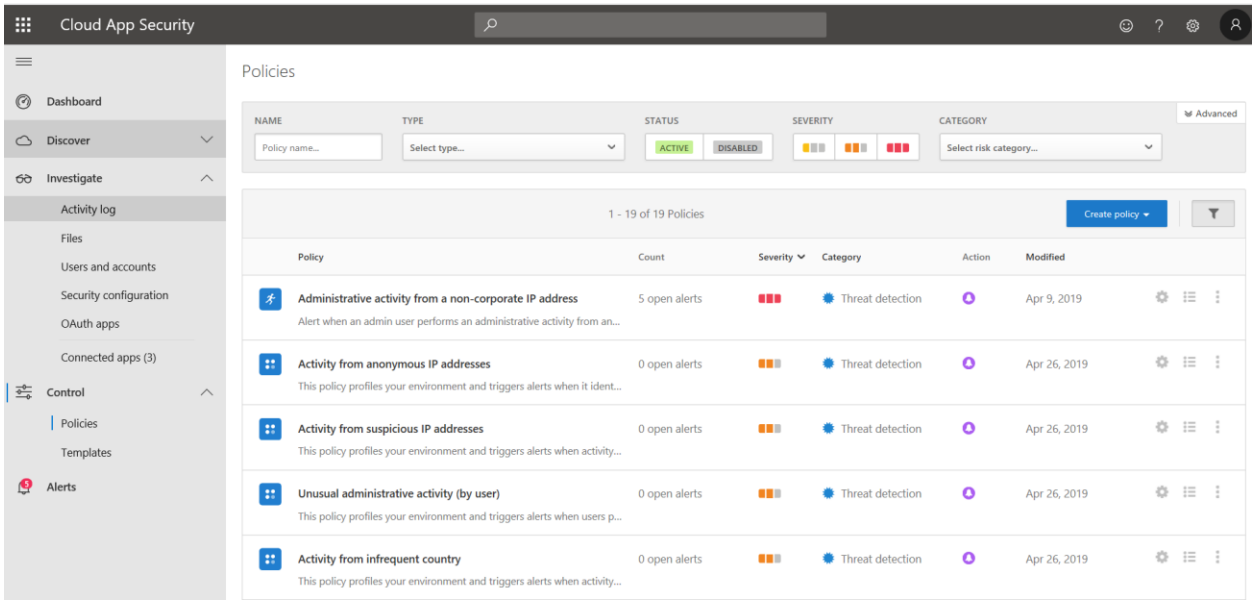
Secure Score impact:
- Turn on Cloud App Security console (+20)
- Use Cloud App Security to detect insider threat, compromised accounts and brute force attempts (+15)

Advanced alert policies require a subscription to Office 365 Cloud App Security (included with E5 plans) or Microsoft Cloud App Security (part of EM+S E5 or sold separately as an add-on). These go way beyond the standard alert policies, to provide intelligent analysis such as **Suspicious admin activity**, **Impossible travel** and others that look for "unusual behaviors."

You can get to Cloud App Security from Security & Compliance **> Alerts > Managed advanced alerts**. Choose **Go to Office 365 Cloud App Security**.



In the **Control > Policies** section, we have a giant list of pre-configured advanced "intelligent" alerts. Again, go through and edit these so that the alerts send email notification to the "right" places/people who are monitoring the system.



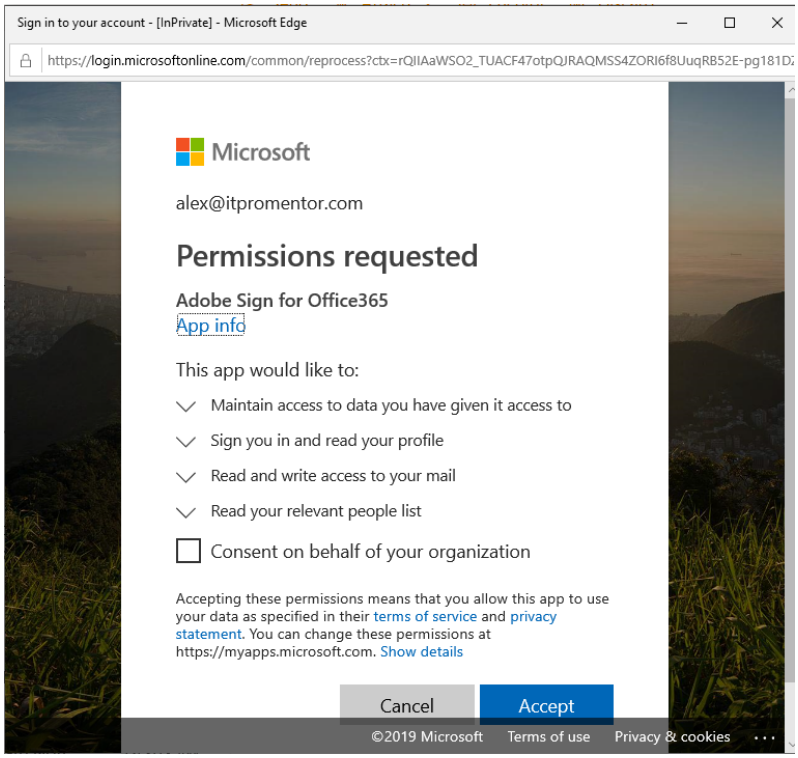
The secret power of MCAS is that you can use it to discover and then protect additional applications, beyond just Exchange email and Office 365. But even getting notification for events such as login from suspicious IP's, infrequent country, unusual administrative activity, etc. is pretty huge for protecting Exchange Online on its own. This is probably my favorite piece of the EM+S E5 bundle (and it is available separately at a relatively low cost, standalone).

One last note about MCAS: As of the time of this writing, I am not aware of any PowerShell access to this separate cloud service (you cannot manipulate objects and adjust settings using the shell, like you can via the rest of the Security & Compliance Center).

☐ OAuth App Notifications and Review

Secure Score impact:
- Set automated notifications of new and trending cloud applications… (+15)
- Review permissions and block risky OAuth applications… (+15)
- Set automated notifications for new OAuth applications… (+20)

Microsoft Cloud App Security can also be configured to alert you when new OAuth apps are authorized to access Office 365 data. For instance, third-party add-ins for Outlook may ask the user to essentially permit them to access data on their behalf. Below is an example when activating an Outlook add-in called Adobe Sign (for electronic signatures):



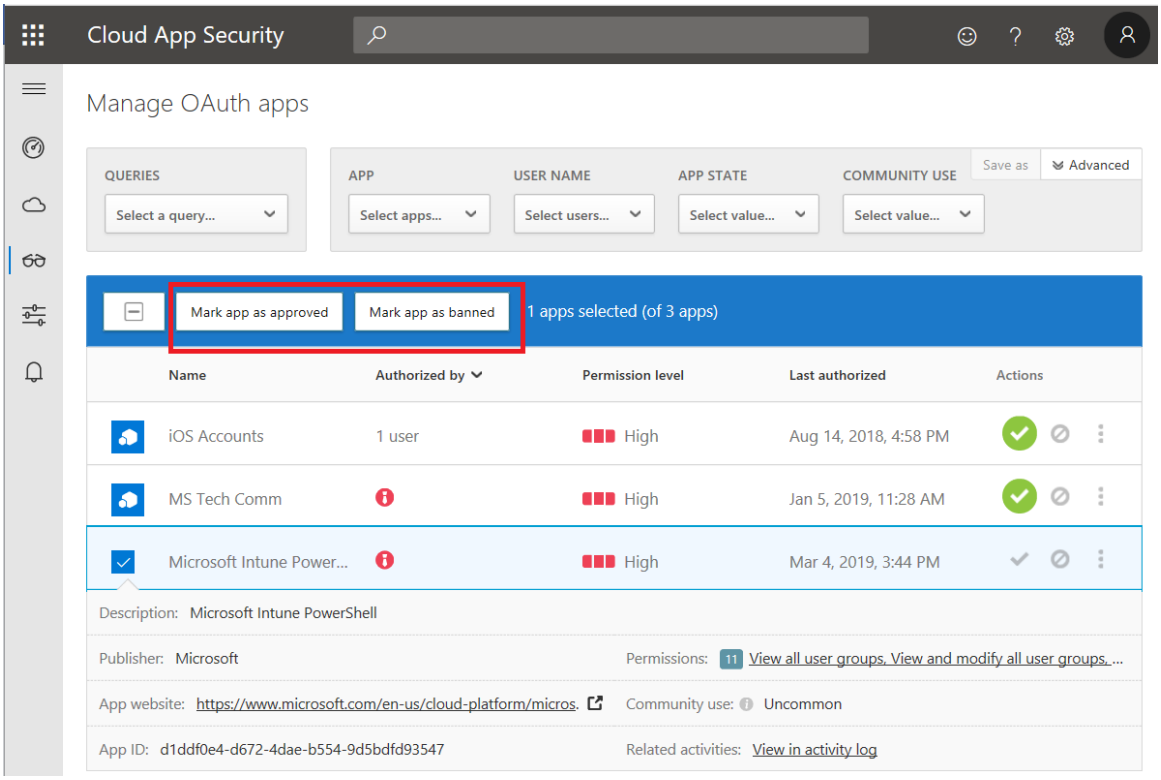
The reason this is risky is because phishing emails may contain links that trigger this type of workflow and ask the user to grant permission to their Office 365 mailbox data. That means the attackers would not even require a username and password to get in at all (because they would have an OAuth token granted to them by the already authenticated user). This is not just theoretical. It happens in real life.

Now it is also possible to prevent users from being able to consent to these items in the first place. That can be accomplished with PowerShell (first run Connect-MsolService):

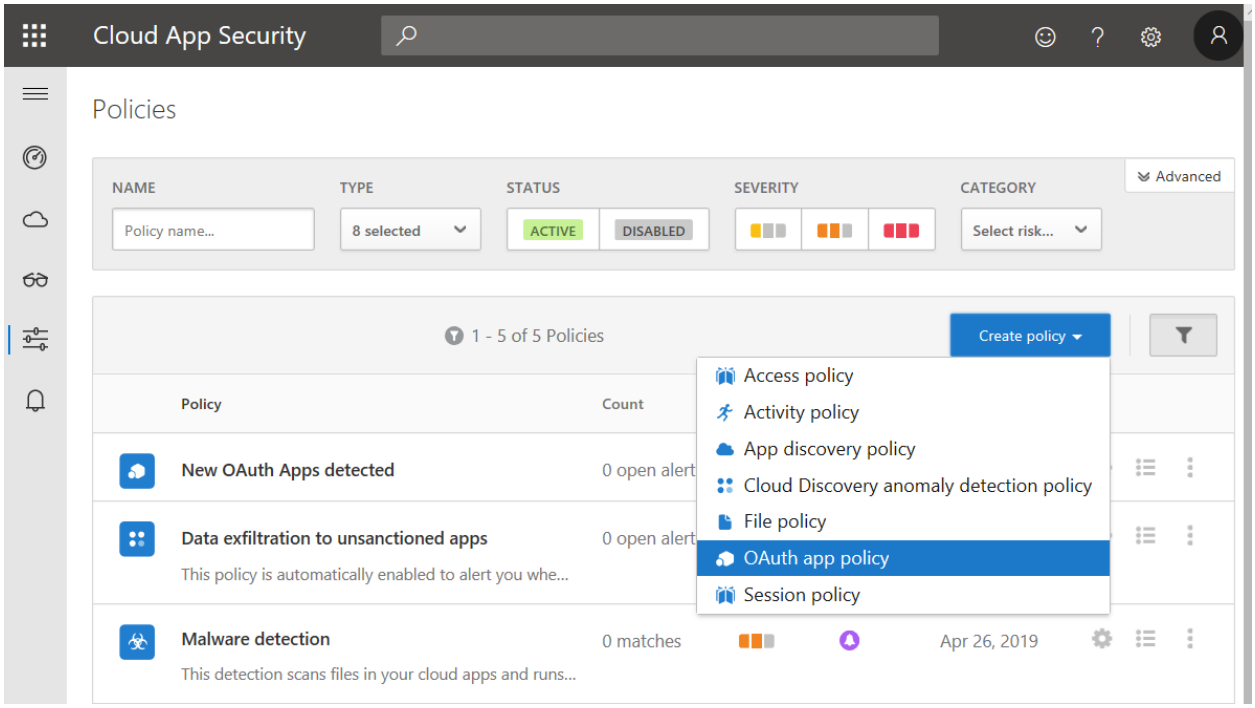
```
Set-MsolCompanySettings -UsersPermissionToUserConsentToAppEnabled $false
```

The downside to that solution is, users cannot self-provision add-ins, and the administrator would need to go and consent to every “legitimate” app that users wanted to add. That might be okay for you. But depending on the environment, that could also be a pain. So Cloud App Security can help you out.

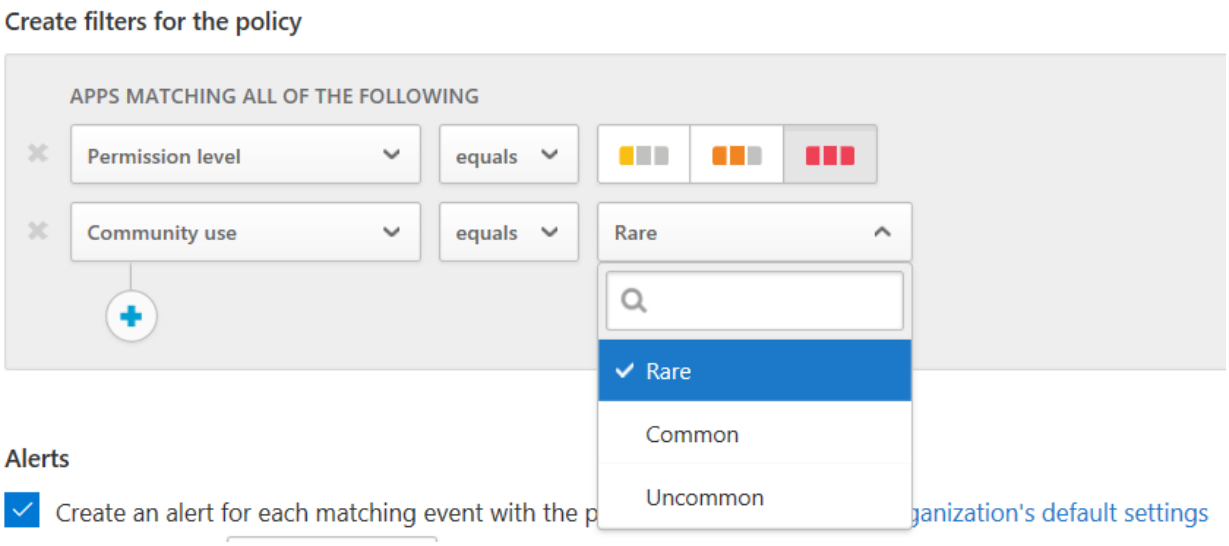
If ever a new application shows up in the environment, you can approve or block the app from **Investigate > Oauth apps** within the Cloud App Security portal.



As well, you can configure OAuth app alerts under **Control > Policies > Create policy**. Pick **Oauth app policy**.



For example, create a policy called *High severity apps* where the **Permission level** equals **High severity**. Configure it to alert. Now you will be notified when new apps show up that request a high level of access.



Closing comments

If you follow all of the steps and advice in this workbook and use the recommended baseline policies that I have described, then you will have among the safest Exchange Online tenants in Office 365.* You will also notice that your Secure Score still appears to have plenty of room for improvement! Like I said before, take that score with a grain of salt. That having been said, yes there is always room for improvement.

What about transport rules?

You might be thinking, "*Wait, this guy doesn't know as much as he pretends to—I mean he didn't even cover basic transport rules that add safeguards against phishing and ransomware!*"

Look, everyone is entitled to their opinion, and here is mine: I think transport rules are over-used and over-valued. For instance, perhaps the most annoying band-wagon phenomenon to bubble up in the past few years is the ubiquitous "External sender banner" that is added to every single email from an outside sender. We see it so frequently now that nobody even notices it anymore. I guarantee you that this practice has no impact on security.

So no, I don't recommend that rule, or any other transport rule that modifies the subject line or body of the email, for many reasons. It is better by far to dial in your Threat management policies (including ATP with PolicyTips), etc. Again, if you are following the advice in this workbook then you will be plenty protected without appending extraneous text to a subject line or email body.

Some people like to block certain types of attachments or whatever using a transport rule--I don't mind that, but I still think it isn't necessary if you have all the other protections enabled that we have discussed.

"Wait, wait! What about fake phishing tests? Doesn't Office 365 have a tool for that?"

Yes. But it's pretty terrible, so we didn't talk about it. A better one is KnowBe4.

Any other questions/complaints/suggestions/etc.—hit me up on Twitter. @vanvfields

If you would like the scripts that are documented in this guide, I have them on GitHub.

** No guarantee or implied warranties, and there is no such thing as bullet-proof. Author maintains no responsibility for your actions or what you choose to do with this information. Verify anything you read in this guide before implementing it in the real world.*