FORTITECH
Fortify Your Technology

How to Secure Microsoft 365

Microsoft 365

Contents

Security features available with (any) Microsoft 365 plan

Below are the security essentials you should implement if you have plans such as:

- Microsoft 365 Business Essentials, Premium or Microsoft 365 Business
- Microsoft 365 Enterprise E1 or E3

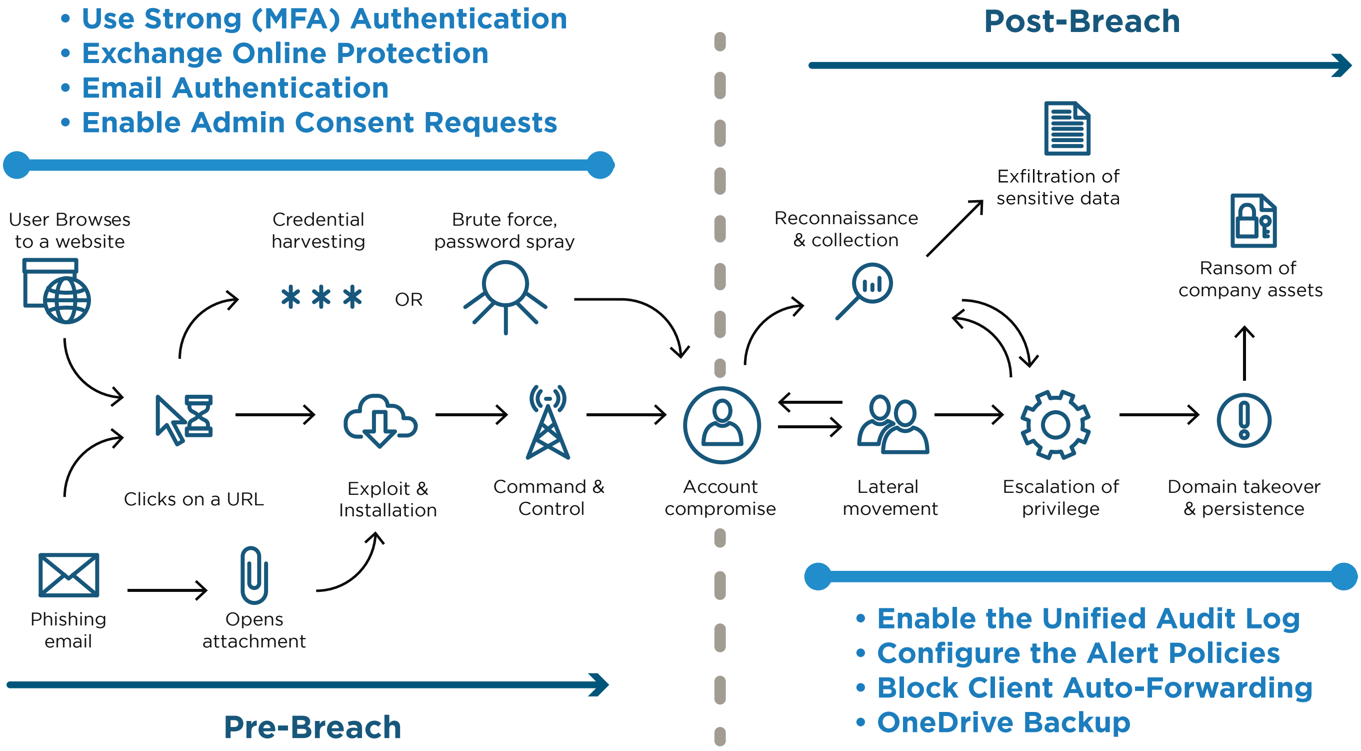
1. Implement Strong Multi-Factor Authentication (MFA)
2. Enable Audit Log Search + Alert Policies
3. Email Authentication: SPF, DKIM & DMARC
4. Exchange Online Protection Baseline
5. Disable Client Auto-Forwarding
6. Admin Consent Requests for Apps
7. Enable OneDrive Backup for Known Folders

View this as a baseline not the complete solution. This is a guide for you to follow and secure you own tenant. If you need consultation on this, please feel free to reach out.

Visualizing Protections on an Attack Kill Chain

Computer scientists at Lockheed-Martin corporation described a new “intrusion kill chain” framework or model to defend computer networks in 2011. They wrote that attacks may occur in phases and can be disrupted through controls established at each phase. Since then, the “cyber kill chain™” has been adopted by data security organizations to define phases of cyber-attacks.”
Source - https://en.wikipedia.org/wiki/Kill_chain#The_cyber_kill_chain

Each of the protections we are going to cover, can be an opportunity to disrupt this chain of events from unfolding (i.e. stopping the event).


• Use Strong (MFA) Authentication
• Exchange Online Protection
• Email Authentication
• Enable Admin Consent Requests
User Browses to a website
Credential harvesting
***
OR
Brute force, password spray
Clicks on a URL
Exploit & Installation
Command & Control
Phishing email
Opens attachment
Pre-Breach
Post-Breach
Exfiltration of sensitive data
Reconnaissance & collection
Ransom of company assets
Account compromise
Lateral movement
Escalation of privilege
Domain takeover & persistence
• Enable the Unified Audit Log
• Configure the Alert Policies
• Block Client Auto-Forwarding
• OneDrive Backup

Pre-Breach events:

- Strong Authentication severely reduces the risk of compromise by common identity- based attacks like password spray
- Exchange Online Protection filters out potential spam, malware and phishing emails
- Email Authentication prevents spoofing attempts using your domain names
- Admin Consent Requests prevent users from inadvertently granting permissions to hostile third-party applications

Post-Breach events:

- Audit log search + Alert policies will notify you about suspicious events in your tenant
- Block Auto-Forwarding prevents a common exfiltration method against email messages
- OneDrive Backup can be used to protect known folders on Windows devices, such as the Desktop, Documents and Pictures libraries.

1. Implement Strong Multi-Factor Authentication (MFA)

There are two approaches that you can take with regard to implementing stronger authentication such as Multi-factor (MFA), which is a highly effective mitigation against common identity-based attacks like password spray.

First option: You can use the "**easy button**" and let Microsoft manage security for you with the **Security defaults** feature. Presumably, the fact that you are reading this guide suggests you may not be the target market for this option.
Many people find that the defaults do not provide them with enough flexibility (for example, you cannot make exceptions). On the other hand, this feature is available in every single Microsoft 365 subscription and does not require any special or additional licensing.

Second option: When you are ready to take command of your own security journey, then you would disable the Security defaults and proceed to create your own custom **security policies** (e.g. using Conditional Access).

Note: Conditional Access requires specific subscription levels, such as Microsoft 365 Business or Enterprise plans, Azure AD Premium P1 or P2, or Enterprise Mobility + Security E3 or E5.

However, it is also possible to configure stronger authentication on a per-user basis, and this may be preferred for those customers who do not have one of the more comprehensive subscriptions but also do not want to use the Security defaults.

Either way, it is recommended to announce this change in advance at a staff meeting and also by all staff email. Consider flyers or other awareness raising techniques as well. Be sure to include helpful links to Microsoft support in your communications, e.g.:

Setup 2-step verification for Microsoft 365

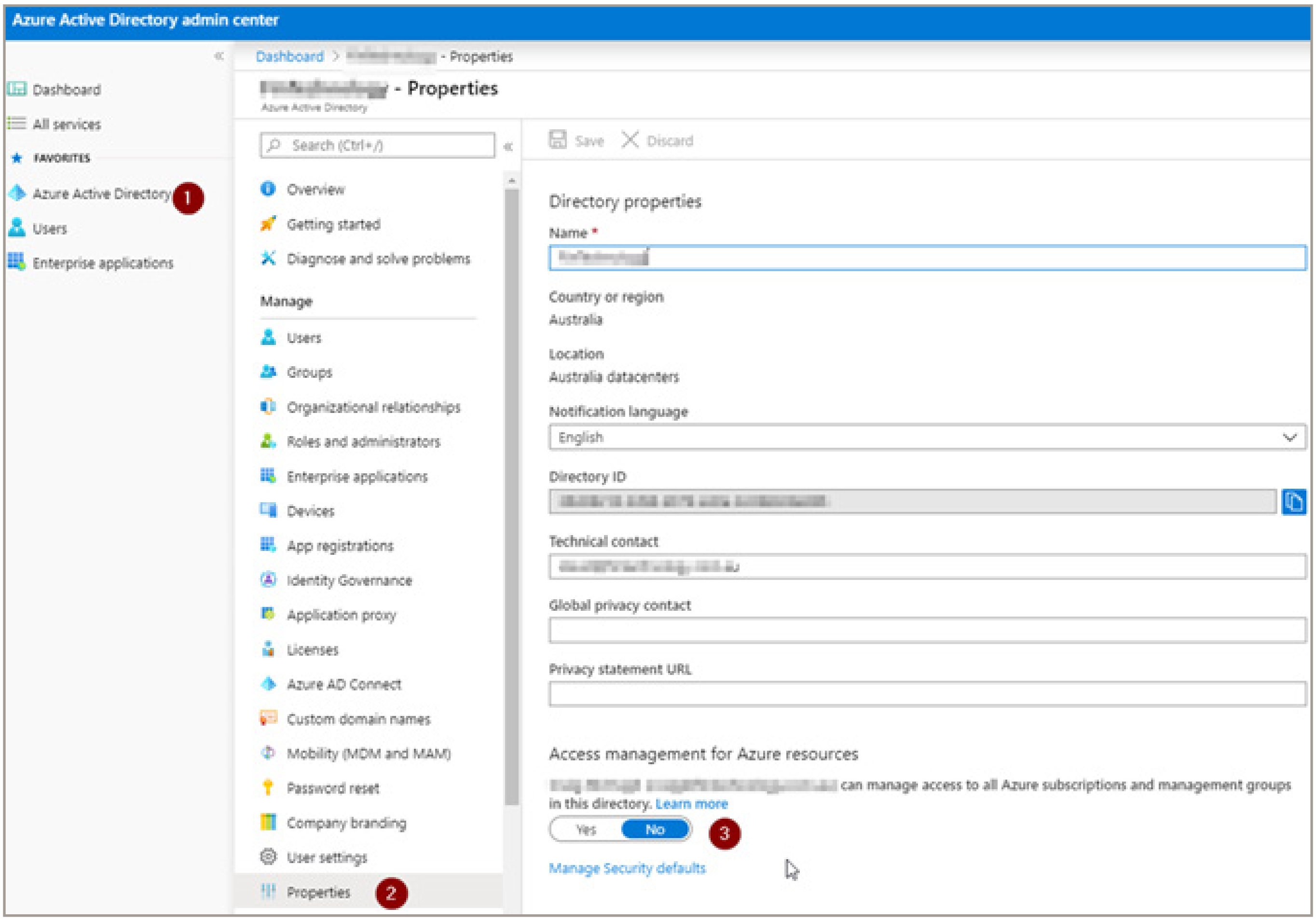
https://support.office.com/en-us/article/set-up-2-step-verification-for-office-365-ace1d096-61e5-449b-a875-58eb3d74de14?ui=en-US&rs=en-US&ad=US

Use the Microsoft Authenticator app

https://support.officce.com/en-us/article/use-microsoft-authenticator-with-office-365-1412611f-ad8d-43ab-807c-7965e5155411?ui=en-US&rs=en-US&ad=US&ID0EAADAAA=_Step_1

Option 1. Use the Security Defaults feature

In the future this will be on by default in new tenants. Currently, you can only use the web portal. In the Azure AD Admin center, find the toggle for Security defaults under **Azure AD > Properties > Manage Security defaults**.



Directory properties

Name * [redacted]

Country or region
Australia

Location
Australia datacenters

Notification language
English

Directory ID
[redacted]

Technical contact
[redacted]

Global privacy contact

Privacy statement URL

Access management for Azure resources

[redacted] can manage access to all Azure subscriptions and management groups in this directory. Learn more

Yes No

Manage Security defaults

The impacts of enabling the Security Defaults are as follows:

- **Block legacy authentication:** All accounts will be prevented from using legacy apps or protocols like SMTP, POP, IMAP, etc. Be careful services like Printers, CRM's may stop working

- **Require MFA for admins:** all admin accounts must use MFA, no exceptions
- **MFA for standard users:** All accounts must register for MFA within 14 days but will only be prompted or challenged for MFA if it is a "risky" logon attempt. Additionally, accounts with credentials found on the dark web will be required to change passwords
- **Require MFA for service management:** Any account signing into Azure services must use MFA whether admin or standard user

Remember: you cannot make any exceptions to the defaults. This feature must be disabled if you plan to configure your own security policies for greater control and functionality.

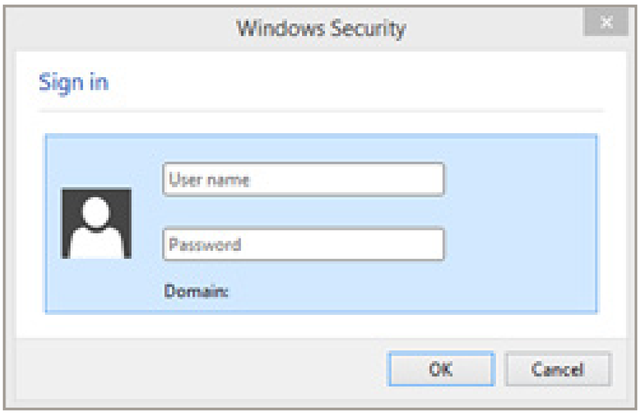
Option 2. Implement strong authentication on a per-user basis

Enabling stronger authentication is really two steps in one. First, you want to block legacy authentication protocols that do not support modern authentication and Multi-Factor. Second, you want to be sure to enable MFA for each and every active user account.

There is one more thing to be aware of here: Shared Mailboxes. When companies implement MFA, they often overlook these accounts. Worse yet, shared accounts most often have very poor passwords since multiple people might be using them. But users who need access to these resources can simply be given permissions to open those mailboxes from their own account (rather than signing in with a password). Therefore, we will also look at how to disable shared mailboxes for inter n-in to Microsoft 365.

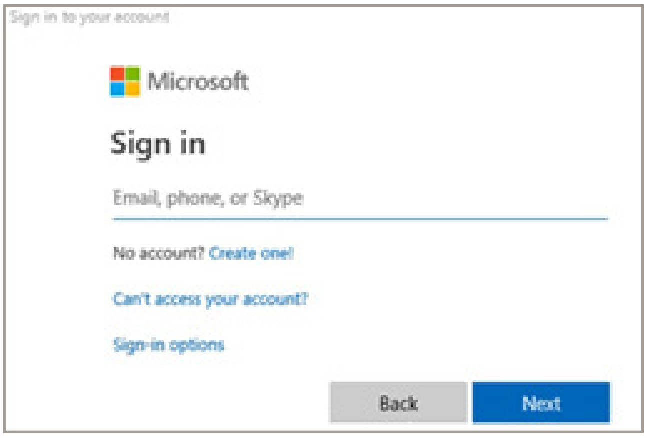
What is legacy vs. modern authentication?

Legacy Authentication



No multi factor authenication

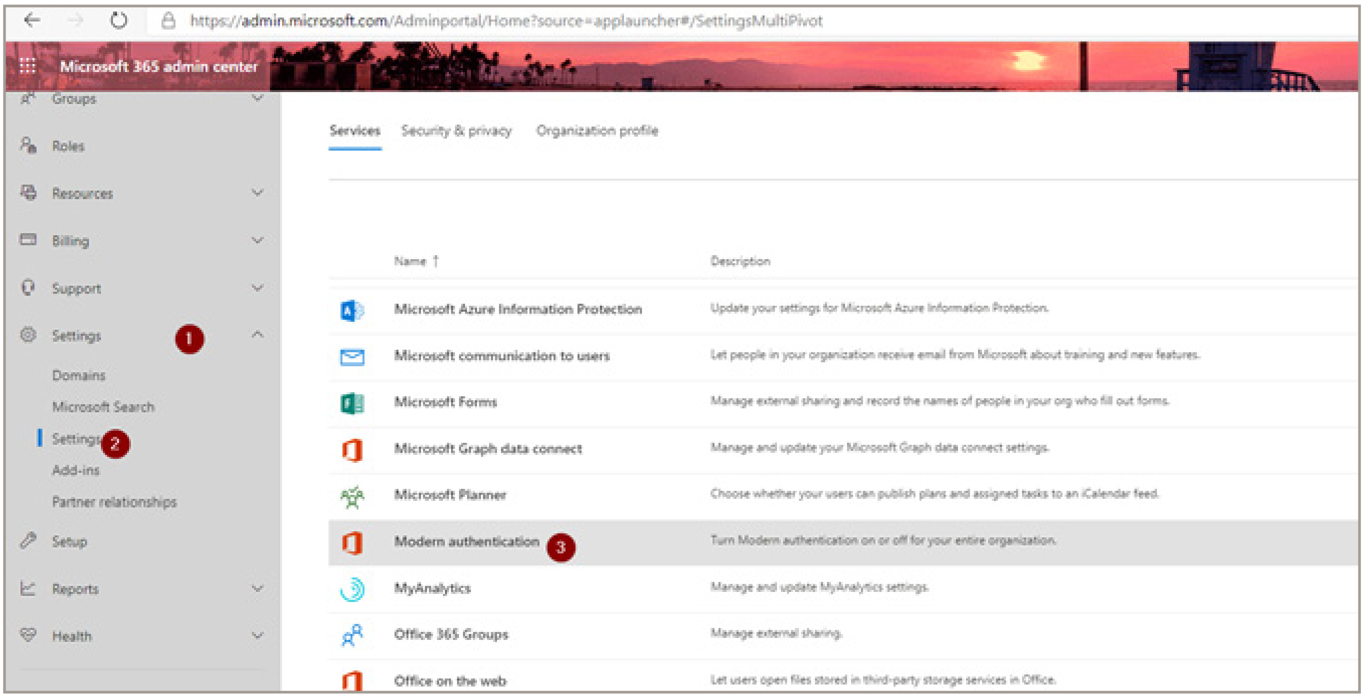
Modern Authentication



Supports Multi-factor prompts

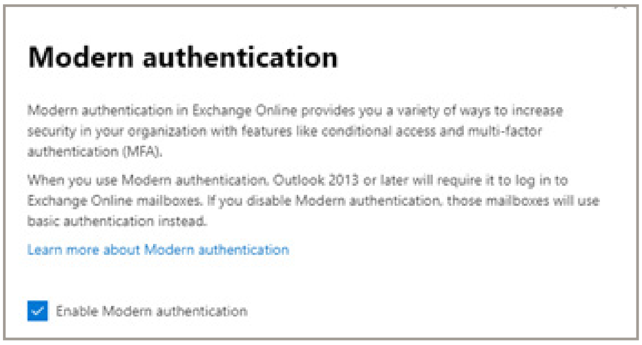
All tenants should have Modern authentication enabled by default (and soon legacy authentication will be disabled by default everywhere as well). From the Microsoft 365 admin center, go to **Settings**, and find **Modern authentication** in the list to confirm.

What it should looks like (Make sure it is ticked)



Name ↑	Description
Microsoft Azure Information Protection	Update your settings for Microsoft Azure Information Protection.
Microsoft communication to users	Let people in your organization receive email from Microsoft about training and new features.
Microsoft Forms	Manage external sharing and record the names of people in your org who fill out forms.
Microsoft Graph data connect	Manage and update your Microsoft Graph data connect settings.
Microsoft Planner	Choose whether your users can publish plans and assigned tasks to an iCalendar feed.
Modern authentication	Turn Modern authentication on or off for your entire organization.
MyAnalytics	Manage and update MyAnalytics settings.
Office 365 Groups	Manage external sharing.
Office on the web	Let users open files stored in third-party storage services in Office.

Issues with Blocking legacy authentication



Modern authentication

Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA).

When you use Modern authentication, Outlook 2013 or later will require it to log in to Exchange Online mailboxes. If you disable Modern authentication, those mailboxes will use basic authentication instead.

Learn more about Modern authentication

☑ Enable Modern authentication

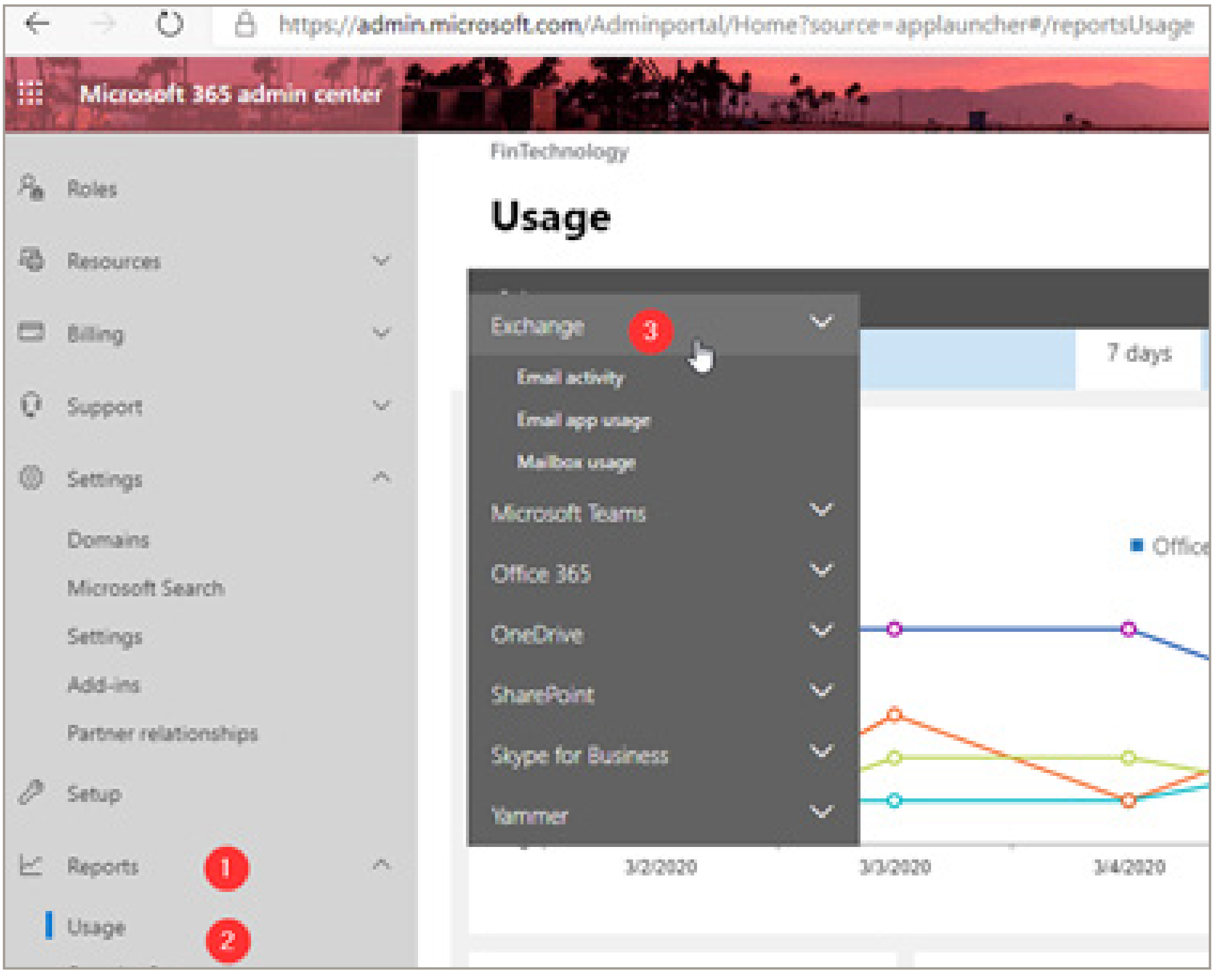
Legacy clients such as Outlook 2010 are not compatible with modern auth. Even 2013 clients aren't compatible without making a modification to the registry. Older versions may have other security and performance issues, install the newer Microsoft 365 Office instead from the Microsoft portal.

Aside from client apps, you might also find apps or devices (e.g. MFP's that scan to email) which are using legacy authentication protocols and other programs like CRM may use IMAP to access the emails. But in October of 2020, many of these protocols will be disabled anyways, so it is best to find alternative means that support modern authentication.

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

1. Disable legacy protocols such as SMTP, POP, IMAP on mailboxes individually
2. Create an Authentication policy that blocks legacy authentication by default (recommended)

Before you proceed, it is a good practice to review the usage reports in the Microsoft 365 admin center under **Reports > Usage**. Select the **Email app usage** report. This report will display which user accounts, if any, have recently connected to Exchange Online using the older protocols (so you can get an idea of impact in advance of the change).



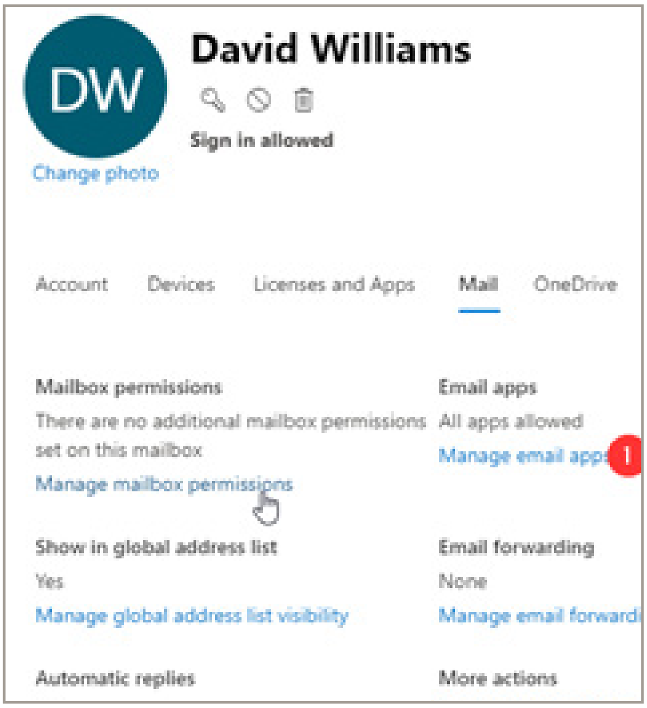
When you look at the table that comes with the report, add columns for SMTP, POP and IMAP to see whether there are any sign-ins related to these legacy protocols.

Note: the report may not show you everything using basic auth out there, but it is a pretty good indicator. Ideally, you will only see modern Outlook clients across your organization. Either move to more modern apps first, or plan to make exceptions for them as we proceed.

Exchange Online Option 1: Disable legacy protocols such as POP and IMAP per mailbox

This is an easy, low-risk place to start, and it is accomplished per-user (rather than via policy). This make it easier to undo. You should try to block the use of legacy protocols (such as SMTP, POP and IMAP) wherever possible. Attacks on these protocols are launched against your tenant daily.

From the Microsoft 365 admin center under **Users > Active users**, select a user account. Go to the **Mail** tab and select the option to **Manage email apps.**



David Williams

Sign in allowed

Mailbox permissions
There are no additional mailbox permissions set on this mailbox

Email apps
All apps allowed

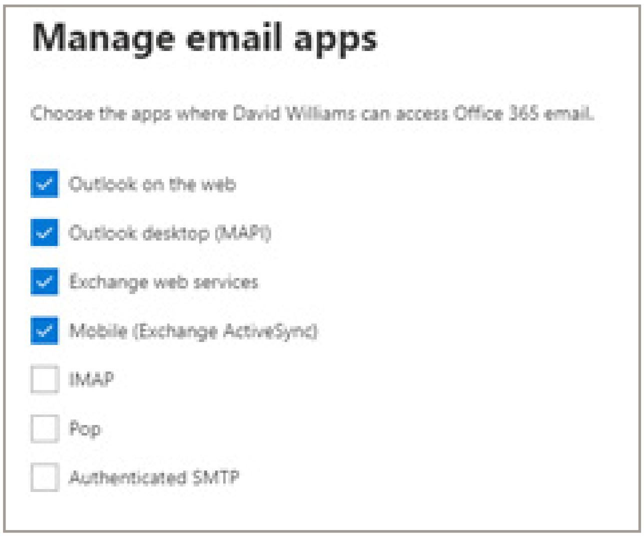
Show in global address list
Yes

Email forwarding
None

Automatic replies

More actions

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



Manage email apps

Choose the apps where David Williams can access Office 365 email.

☑ Outlook on the web
☑ Outlook desktop (MAPI)
☑ Exchange web services
☑ Mobile (Exchange ActiveSync)
☐ IMAP
☐ Pop
☐ Authenticated SMTP

SMTP is by far the most targeted legacy protocol, followed by **IMAP** and then **POP**, so removing those at a bare minimum is a good idea. **Exchange ActiveSync** (EAS) is also not needed as long as end users move to the new Outlook mobile app (rather than a native app like Apple Mail). It is also unlikely that users would need **Exchange Web Services** (EWS), however, some applications that integrate with Exchange Online may still need one or more of these services.

Therefore, it is helpful to refer to the usage report in case exceptions need to be made (but the better thing to do is to update your apps to use modern authentication).

Exchange Online Option 2: Block via an Authentication Policy

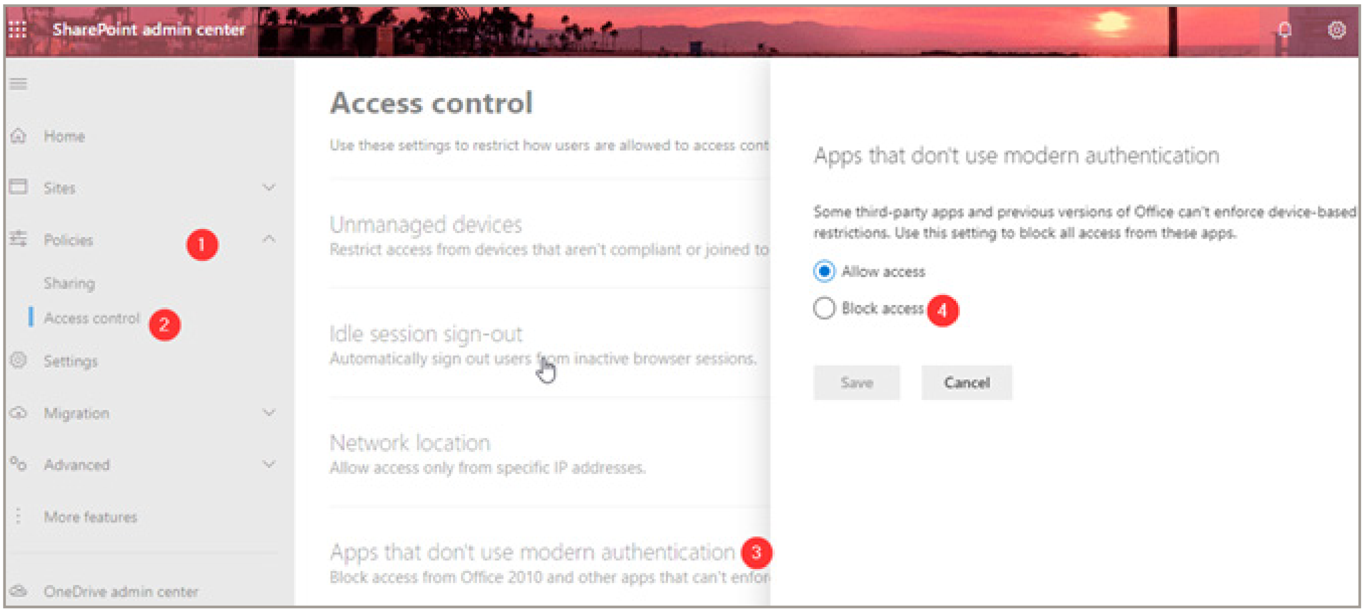
To completely eliminate basic authentication in Exchange Online, we simply have to create a new authentication policy with no additional parameters, and assign it as the default policy for the organization.

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

Mailboxes that have a specific policy assigned will override the default that you set for the organization. The org-wide policy is applied only if there is no specific policy assigned to the mailbox.

Block legacy authentication for SharePoint

You should also disable basic authentication for **SharePoint Online**. Navigate to the SharePoint admin center, and find **Policies > Access control > Apps that don't use modern authentication** and choose **Block access**.



Access control

Use these settings to restrict how users are allowed to access cont

Unmanaged devices
Restrict access from devices that aren't compliant or joined to

Idle session sign-out
Automatically sign out users from inactive browser sessions.

Network location
Allow access only from specific IP addresses.

Apps that don't use modern authentication
Block access from Office 2010 and other apps that can't enfor

Apps that don't use modern authentication

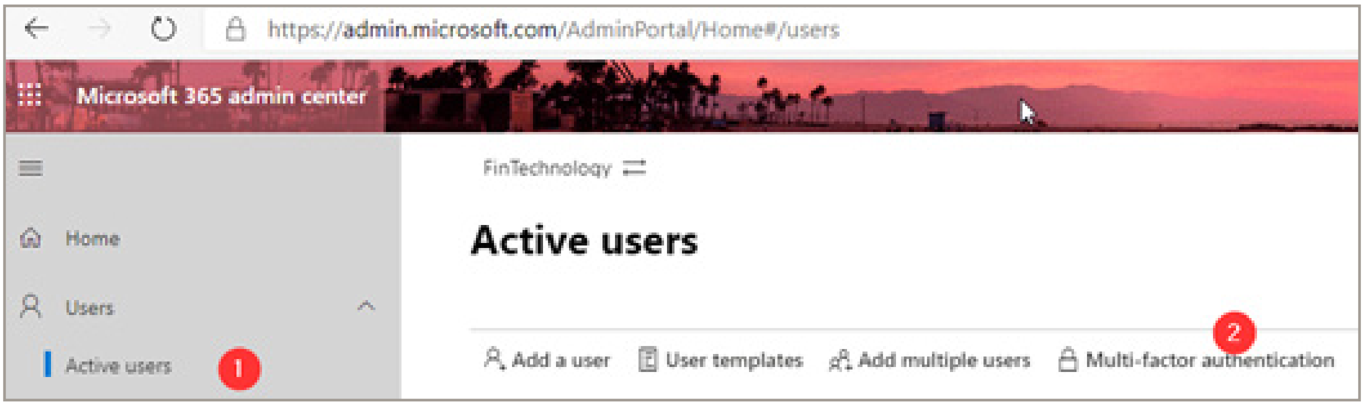
Some third-party apps and previous versions of Office can't enforce device-based restrictions. Use this setting to block all access from these apps.

● Allow access
○ Block access

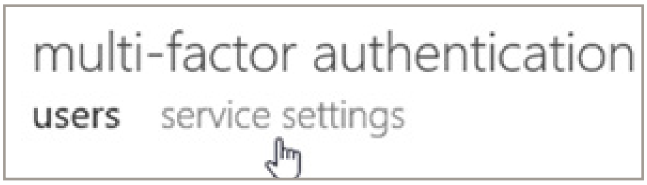
Setup MFA per-user account

Besides disabling the legacy authentication methods, it is recommended to implement Multi- factor authentication (MFA) for all admin and standard user accounts alike. This method works with any Microsoft 365 subscription.

Go to the Microsoft 365 Admin Center and navigate to **Users > Active users**. Find **Multi-factor authentication** (if you don't have the new admin center experience enabled this might be under the "ellipses" or "More" button)


https://admin.microsoft.com/AdminPortal/Home#/users
Microsoft 365 admin center
Home
Users
Active users
1
FinTechnology
Active users
Add a user
User templates
Add multiple users
Multi-factor authentication
2

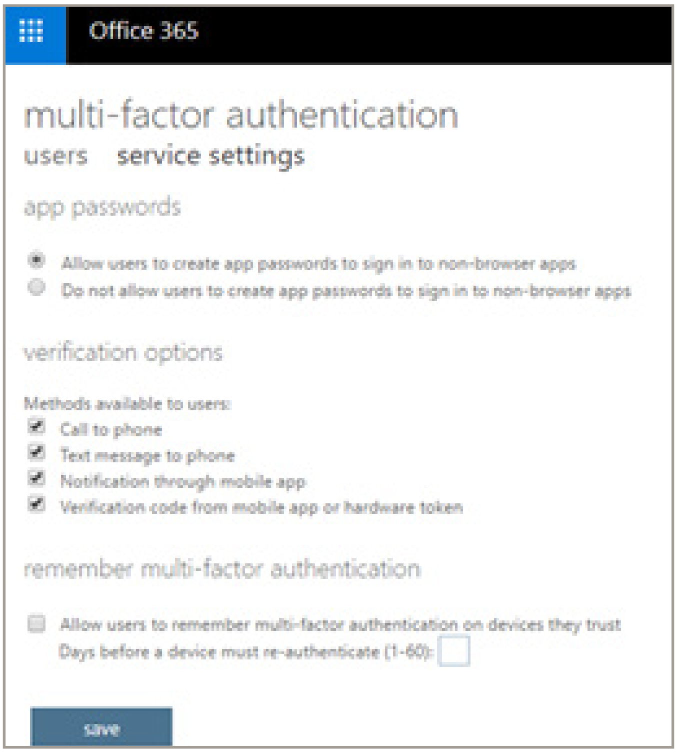
You can see your users listed here, but before you enable MFA for anyone in particular, check out the service settings area.



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 Microsoft apps, Apple Mail, etc.).

NOTE: App passwords will not work if you have disabled basic authentication for these services anyway, so I normally just turn them off.

Implement Strong Multi-Factor Authentication (MFA)



multi-factor authentication

users service settings

app passwords

● Allow users to create app passwords to sign in to non-browser apps

○ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

☑ Call to phone

☑ Text message to phone

☑ Notification through mobile app

☑ Verification code from mobile app or hardware token

remember multi-factor authentication

□ Allow users to remember multi-factor authentication on devices they trust

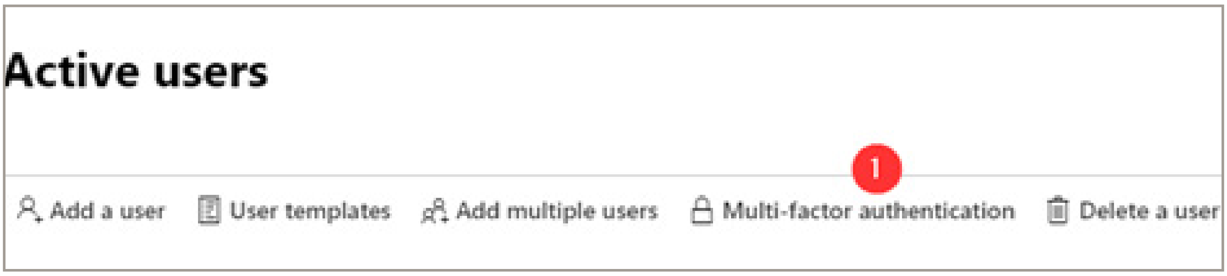
Days before a device must re-authenticate (1-60): □

When you have access to Azure AD Premium P1 and Conditional access (standard Microsoft 365 subscriptions will not include this however Microsoft 365 subscriptions will), you gain access to another option in here to exclude **trusted IPs** (e.g. corporate locations). Please note, this means the <u>external</u> IP addresses, not the internal IP subnets.

If you get this wrong, you can lock yourself OUT of your own Microsoft 365 subscription

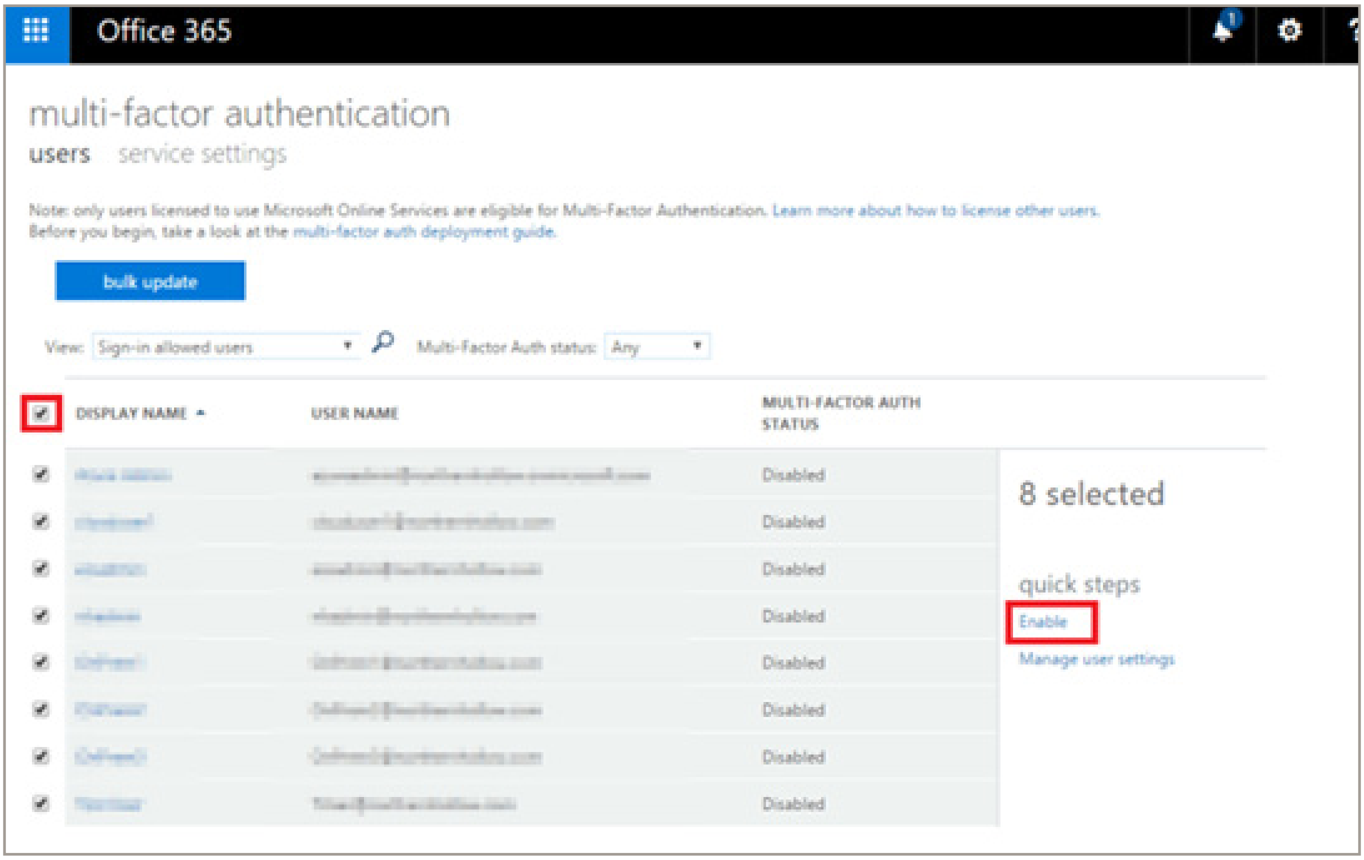
Change all users

Simply log into the 365 and select Users



Active users

Select all users and enable



multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users ▾ Multi-Factor Auth status: Any ▾

☑	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled
☑	[illegible]	[illegible]	Disabled

8 selected

quick steps

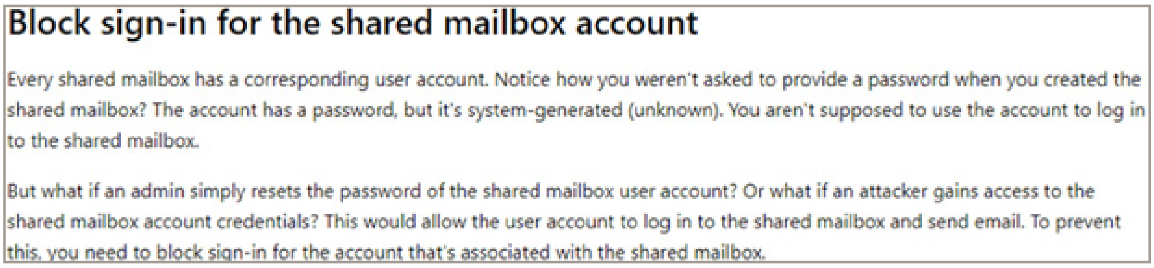
Enable

Manage user settings

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.

Block sign-in for all shared mailboxes

Shared mailboxes (including Resource mailboxes) should 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. But hardly anyone thinks to enable these for MFA.

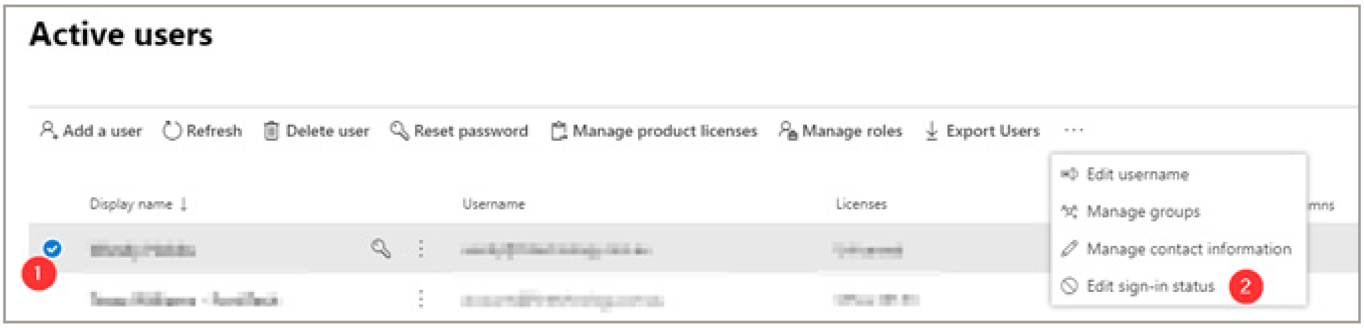


Block sign-in for the shared mailbox account

Every shared mailbox has a corresponding user account. Notice how you weren't asked to provide a password when you created the shared mailbox? The account has a password, but it's system-generated (unknown). You aren't supposed to use the account to log in to the shared mailbox.

But what if an admin simply resets the password of the shared mailbox user account? Or what if an attacker gains access to the shared mailbox account credentials? This would allow the user account to log in to the shared mailbox and send email. To prevent this, you need to block sign-in for the account that's associated with the shared mailbox.

Really though, you should be blocking sign-in for 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.



It is best to audit your accounts to be positive that any “non-real-person” sign-ins are disabled.

OK the basic setup is complete. Now it’s time to get your hands dirty

2. Enable Audit Log Search + Alert Policies

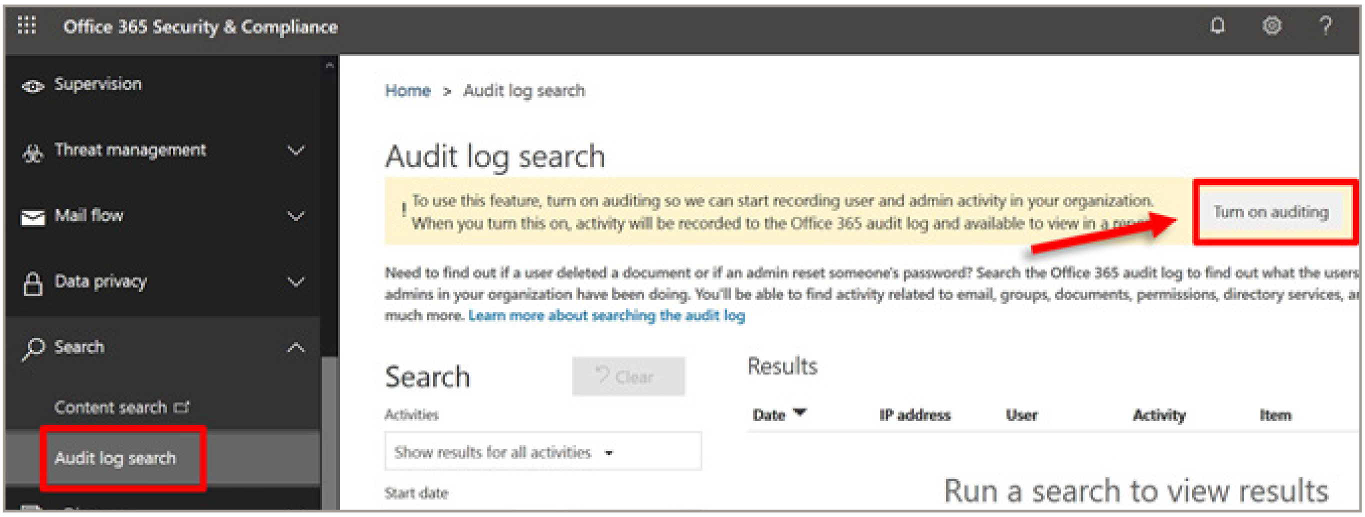
Auditing is crucial. If there ever is a breach, you want logging enabled in order to understand what happened and when. Not to mention it is usually required for compliance with various laws and regulations. And of course, you need to turn this on. This is not on by default

While auditing is enabled by default for mailboxes now, the unified audit log is not enabled by default. But having this turned on is necessary so that you can record the audit log information in one central place, and then search and also generate alerts on it.

Enable Audit Log Search + Alert Policies

Enable the audit log to light up search and alerting capabilities

From protection.office.com go to **Search > Audit** log search and click **Turn on auditing**.



Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a repo

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, a much more. Learn more about searching the audit log

Search

Results

Date	IP address	User	Activity	Item

Run a search to view results

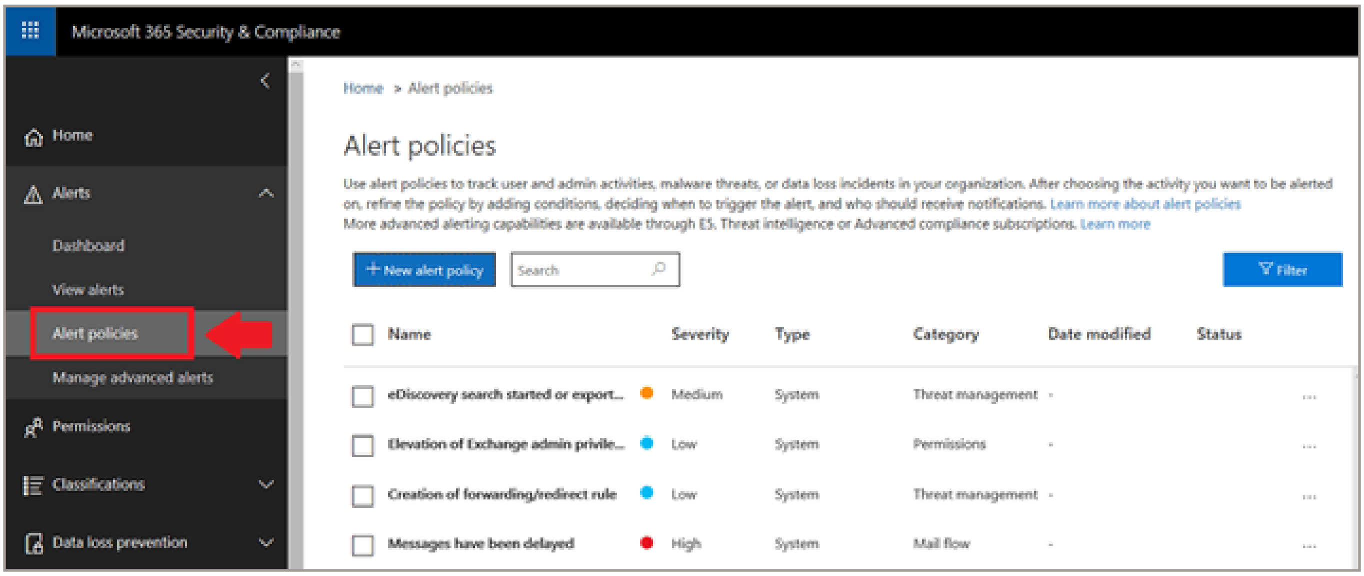
If you can not see it, it means it is already turned on. That's a good thing.

It may be a few hours for this to take effect.

Enable the default Alert Policies

Alert Policies is something that should be on your radar. These will generate email notifications (alerts) when certain types of high-risk events happen in Microsoft 365.

From protection.office.com choose **Alerts > Alert policies**.



Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications. Learn more about alert policies
More advanced alerting capabilities are available through E5, Threat intelligence or Advanced compliance subscriptions. Learn more

□	Name	Severity	Type	Category	Date modified	Status
□	eDiscovery search started or export...	● Medium	System	Threat management	-	...
□	Elevation of Exchange admin privile...	● Low	System	Permissions	-	...
□	Creation of forwarding/redirect rule	● Low	System	Threat management	-	...
□	Messages have been delayed	● High	System	Mail flow	-	...

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

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

FortiTech offers a Managed Support Service that covers this type of monitoring

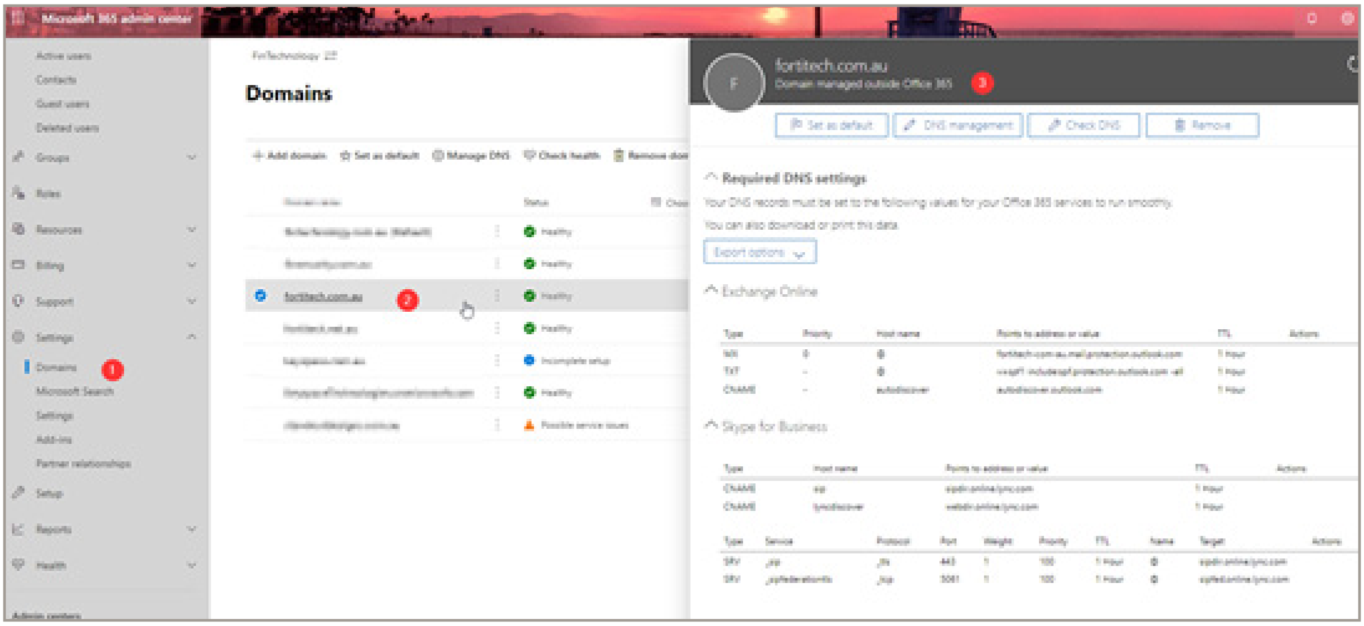
3. Configure Email Authentication

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 (SPF)

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-spf-in-office-365-to-help-prevent-spoofing

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



fortitech.com.au
Domain managed outside Office 365

Required DNS settings
Your DNS records must be set to the following values for your Office 365 services to run smoothly.
You can also download or print this data.
Export options

Exchange Online

Type	Priority	Host name	Points to address or value	TTL	Actions
MX	0	@	fortitech-com-au.mail.protection.outlook.com	1 Hour	
TXT	-	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour	
CNAME	-	autodiscover	autodiscover.outlook.com	1 Hour	

Skype for Business

Type	Host name	Points to address or value	TTL	Actions
CNAME	sip	sipdir.online.lync.com	1 Hour	
CNAME	lyncdiscover	webdir.online.lync.com	1 Hour	

Type	Service	Protocol	Port	Weight	Priority	TTL	Name	Target	Actions
SRV	_sip	_tls	443	1	100	1 Hour	@	sipdir.online.lync.com	
SRV	_sipfederationtls	_tcp	5061	1	100	1 Hour	@	sipfed.online.lync.com	

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 Microsoft 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 Microsoft 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)

DKIM is an authentication system based on an asymmetric cryptographic key pair–a private and public key. When a message leaves Microsoft 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. This proves to recipient servers that your 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.

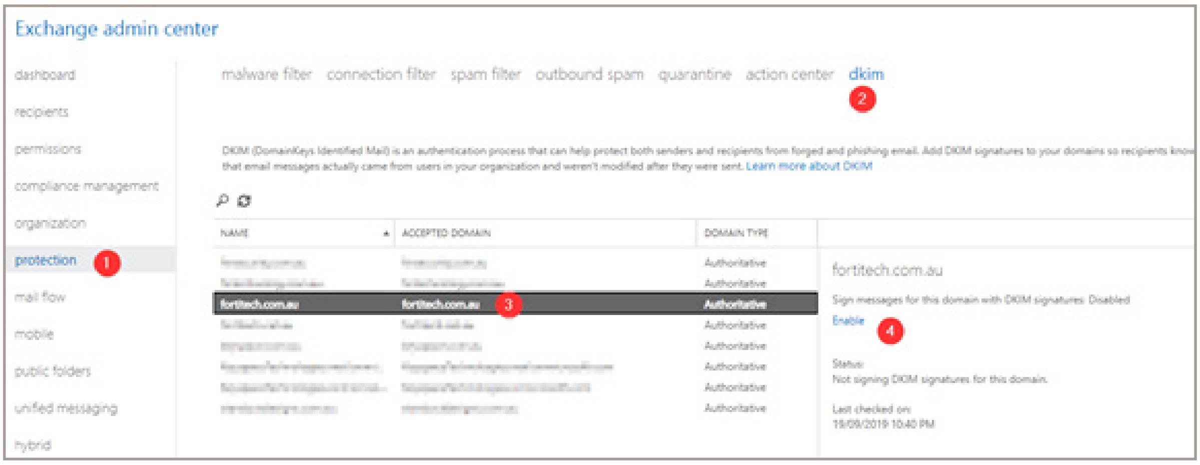
You will need to build two CNAME records per domain for DKIM. The format is:

```
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: Your domain is separated by a hyphen instead of a period; it should match the domain as depicted in the MX record that is given to you by Microsoft 365 (e.g.: contoso-com.mail.protection.outlook.com).

Also, the tenant name (TenantName.onmicrosoft.com) can be found under Settings > Domains in the Microsoft 365 admin center.

Therefore, contoso.com, whose tenant name is "contoso.onmicrosoft.com" looks like this:



DKIM (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organization and weren't modified after they were sent. Learn more about DKIM

NAME	ACCEPTED DOMAIN	DOMAIN TYPE
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
fortitech.com.au	fortitech.com.au	Authoritative
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative
[redacted]	[redacted]	Authoritative

fortitech.com.au

Sign messages for this domain with DKIM signatures: Disabled

Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
19/09/2019 10:40 PM

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

Another example is myfavoritecharity.org with a tenant name of charityrocks.onmicrosoft.com:

Host name: selector1._domainkey
Points to: selector1-myfavoritecharity-org._domainkey.charityrocks.onmicrosoft.com
Host name: selector2._domainkey
Points to: selector2- myfavoritecharity-org._domainkey.charityrocks.onmicrosoft.com

Next, in the **Exchange admin center**, go to **protection > dkim**, and 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.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

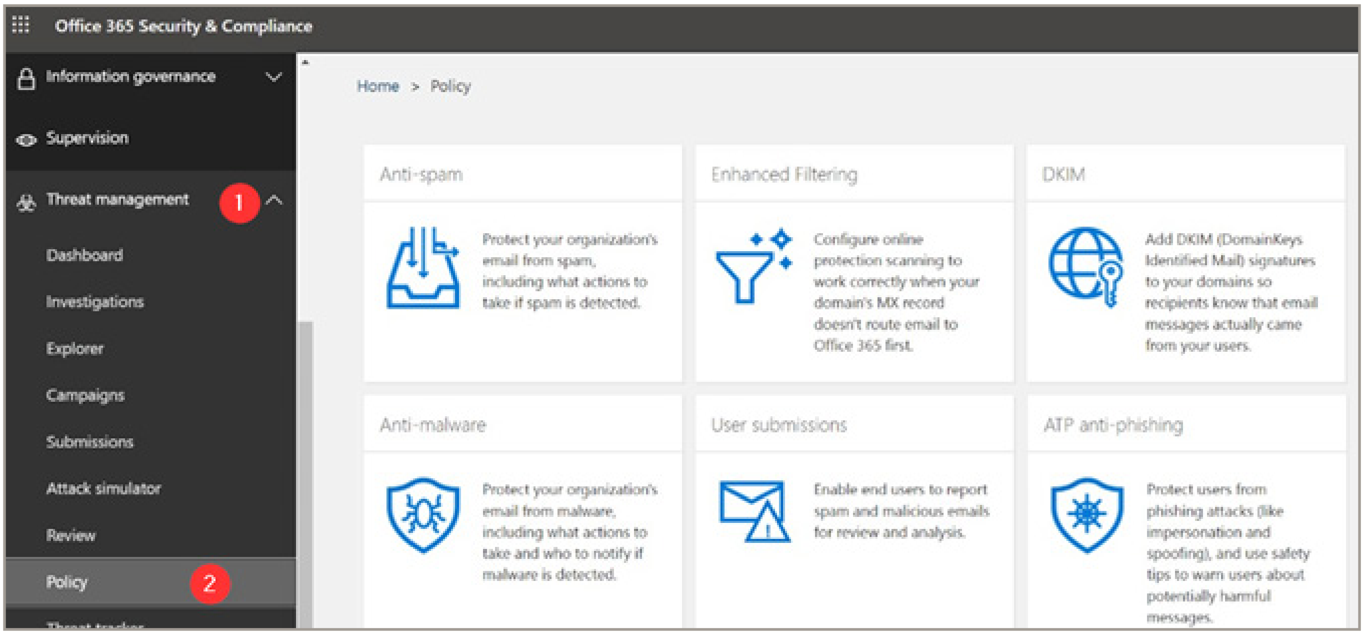
DMARC is a DNS record that tells recipient servers how to treat unauthenticated messages that come from your domain, based on policy. It can also communicate where to send reports about mail from your domain.

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

```
TXT Name: _dmarc.contoso.com
Value: "v=DMARC1; p=quarantine; pct=100”
```

However, 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 take time to find legitimate sources of email and update SPF and DKIM before moving the DMARC policy up to a setting of **quarantine**, or even **reject** (the strongest setting).

4. Configure Exchange Online Protection



Anti-spam: Protect your organization's email from spam, including what actions to take if spam is detected.

Enhanced Filtering: Configure online protection scanning to work correctly when your domain's MX record doesn't route email to Office 365 first.

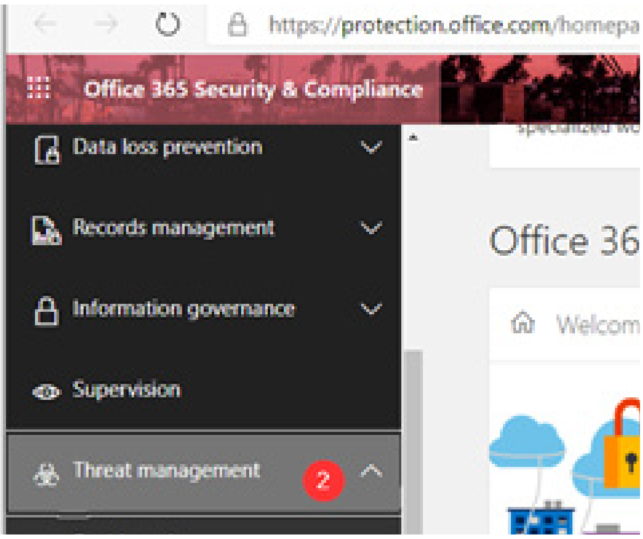
DKIM: Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.

Anti-malware: Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

User submissions: Enable end users to report spam and malicious emails for review and analysis.

ATP anti-phishing: Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.

Exchange Online Protection provides some filtering of spam, phishing and malware emails sent to and from your organization's mailboxes. In the Security & Compliance center, navigate to **Threat Management > Policy**.



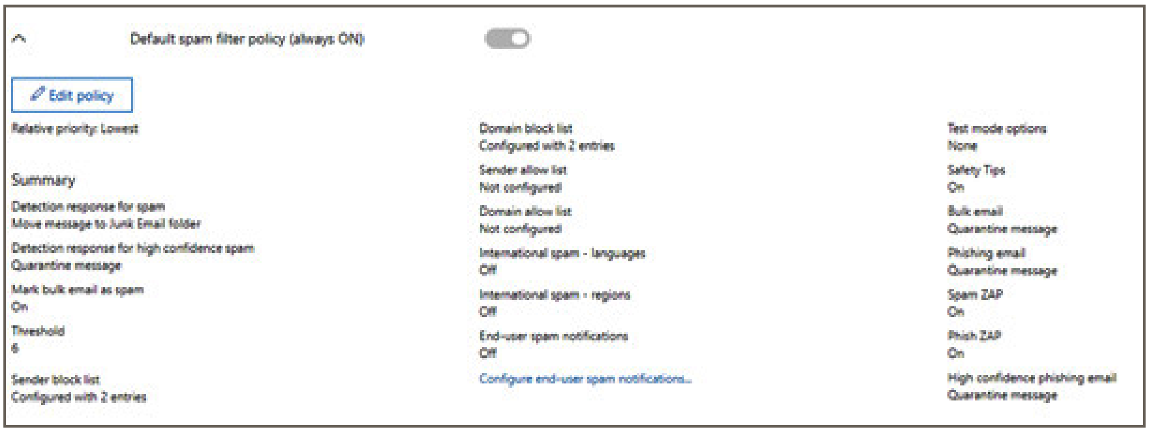
Be sure to configure all of the following:

- Anti-spam AND Outbound spam
- Anti-malware
- Anti-phishing
- Install the Report Message add-in for end users

FortiTech also provides an independent SPAM and Mail filter

Configure the anti-spam policy

Click on **Anti-spam**, and choose **Edit policy**. Below is a screenshot of the modified default anti-spam policy using Microsoft's recommended settings at the time of this writing:



Relative priority: Lowest

Summary

Detection response for spam
Move message to Junk Email folder

Detection response for high confidence spam
Quarantine message

Mark bulk email as spam
On

Threshold
6

Sender block list
Configured with 2 entries

Domain block list
Configured with 2 entries

Sender allow list
Not configured

Domain allow list
Not configured

International spam - languages
Off

International spam - regions
Off

End-user spam notifications
Off

Configure end-user spam notifications...

Test mode options
None

Safety Tips
On

Bulk email
Quarantine message

Phishing email
Quarantine message

Spam ZAP
On

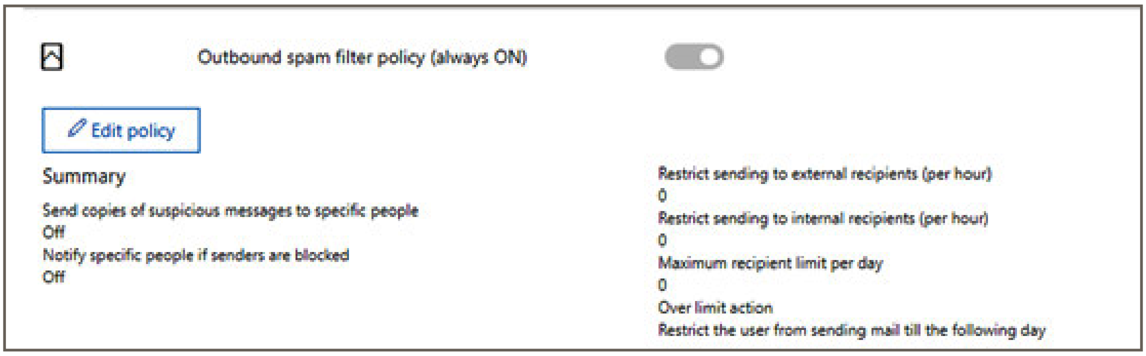
Phish ZAP
On

High confidence phishing email
Quarantine message

Regular spam and bulk messages are configured to go to the Junk Email folder. This is also the most likely destination for false positive messages. High confidence spam and phishing emails will be quarantined. Optionally you can turn on end-user spam notifications so that users get a summary by email of messages that have been trapped in the quarantine, with an option to release messages.

Configure the outbound spam policy

As seen from the UI, just scroll down further past the connection policy to find the **Outbound spam filter policy**.



Summary

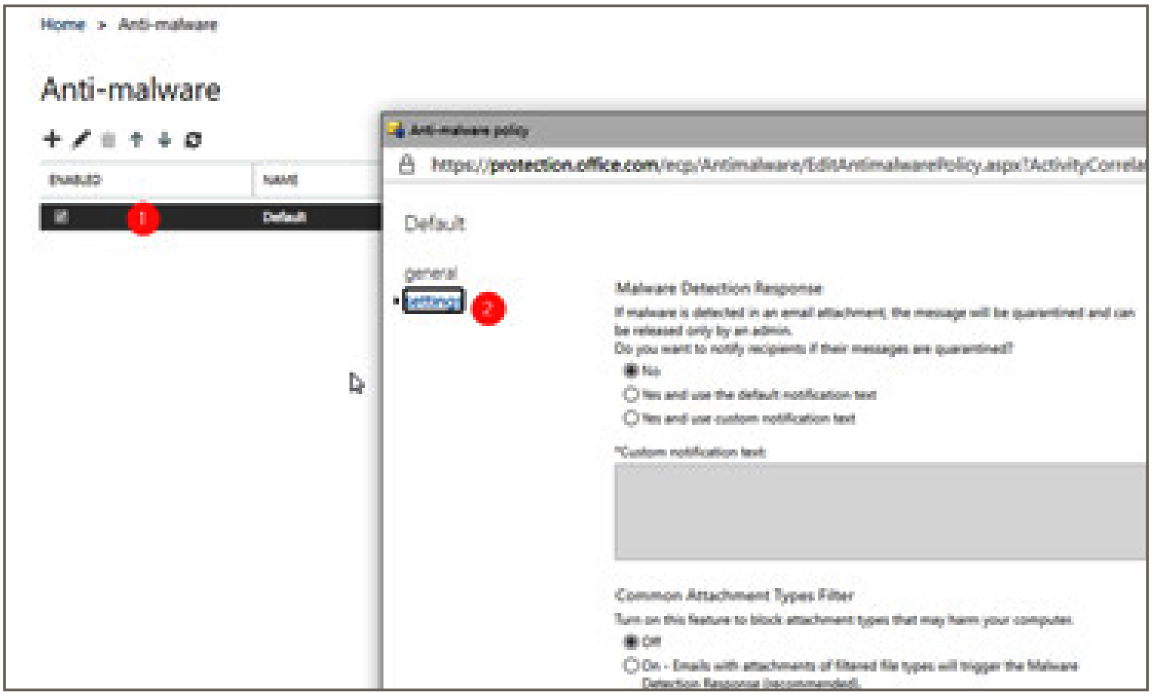
Send copies of suspicious messages to specific people
Off
Notify specific people if senders are blocked
Off

Restrict sending to external recipients (per hour)
0
Restrict sending to internal recipients (per hour)
0
Maximum recipient limit per day
0
Over limit action
Restrict the user from sending mail till the following day

This has been configured to impose daily sending limits, and to send an alert to a specified mailbox when outbound mail is suspected as spam.

Configure the malware filter policy

From **Threat Management > Policy**, open the **Default** Anti-malware policy.



Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

● No
○ Yes and use the default notification text
○ Yes and use custom notification text

*Custom notification text:

Common Attachment Types Filter

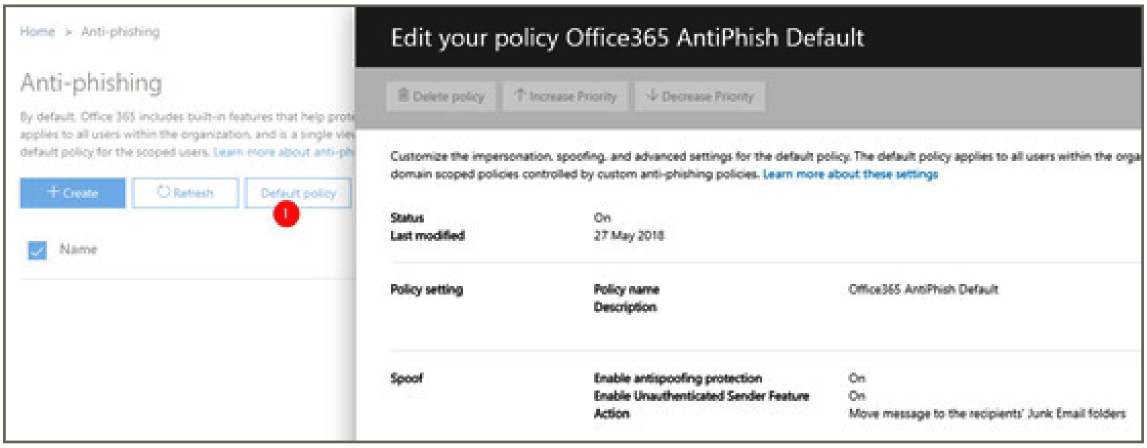
Turn on this feature to block attachment types that may harm your computer.

● Off
○ On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

Enable the **Common Attachment Types Filter** as well as the **Malware Zero-hour Auto Purge (ZAP)**. You can also add other Common Attachment Types using the Plus **(+)**, and select from a list of 96 common attachment types that you might want to block (hardly any of these attachments are typical file types required by the average end user in their day-to-day work).

Configure default anti-phish policy

Go back to **Threat Management > Policy**. Pick the **Anti-phishing policy**, click **Default policy** and **Edit** the **Spoof** settings. Verify that **Spoofing protection** and **Unauthenticated Sender** feature are both enabled, and that spoofed messages are being moved to Junk or Quarantine as you prefer.



By default, Office 365 includes built-in features that help prote applies to all users within the organization, and is a single vie default policy for the scoped users. Learn more about anti-ph

Edit your policy Office365 AntiPhish Default

Customize the impersonation, spoofing, and advanced settings for the default policy. The default policy applies to all users within the orga domain scoped policies controlled by custom anti-phishing policies. Learn more about these settings

Status: On
Last modified: 27 May 2018

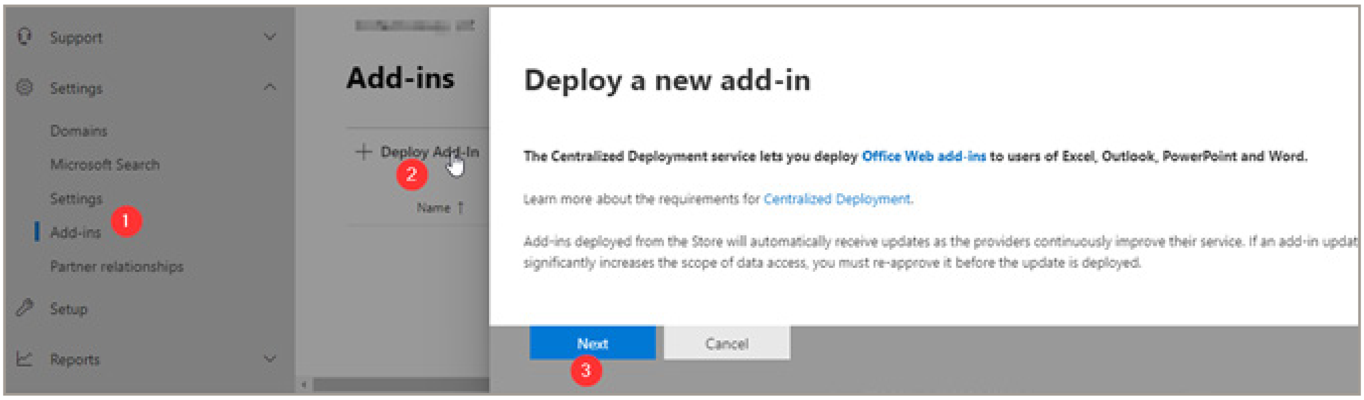
Policy setting
Policy name: Office365 AntiPhish Default
Description

Spoof
Enable antispoofing protection: On
Enable Unauthenticated Sender Feature: On
Action: Move message to the recipients' Junk Email folders

Install the Report Message add-in for end users

You should give end users the ability to self-report mail that they believe is junk or phishing related, by providing them with the **Report Message** add-in.

From the Admin center, go to **Settings > Add-ins** and click **Deploy Add-ins**. Click **Next** then **Choose from Store**. You can find the **Report Message** add-in here and click **Add**.

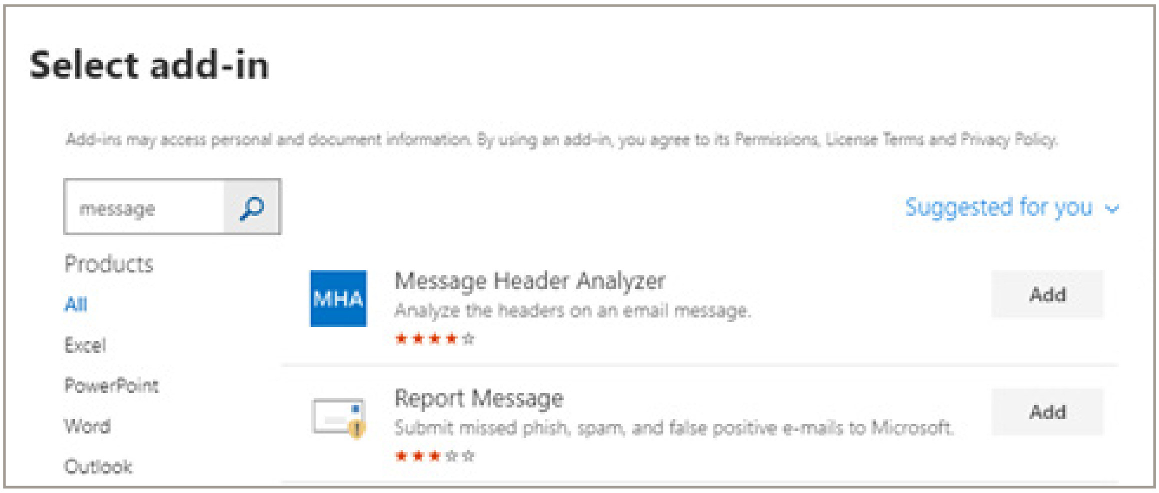


Deploy a new add-in

The Centralized Deployment service lets you deploy Office Web add-ins to users of Excel, Outlook, PowerPoint and Word.

Learn more about the requirements for Centralized Deployment.

Add-ins deployed from the Store will automatically receive updates as the providers continuously improve their service. If an add-in updat significantly increases the scope of data access, you must re-approve it before the update is deployed.



Select add-in

Add-ins may access personal and document information. By using an add-in, you agree to its Permissions, License Terms and Privacy Policy.

message

Suggested for you

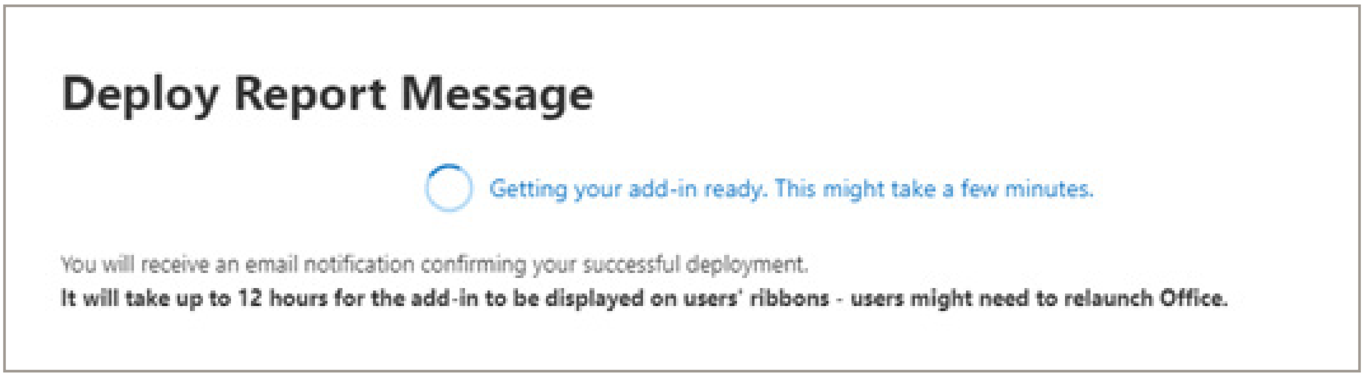
Products
All
Excel
PowerPoint
Word
Outlook

Message Header Analyzer
Analyze the headers on an email message.
★★★★☆
Add

Report Message
Submit missed phish, spam, and false positive e-mails to Microsoft.
★★★☆☆
Add

Message Header is also very useful add in

Accept the terms, then choose your deploy options (**Everyone** and **Fixed**). Click **Deploy** to finish (but note that it can take up to 12 hours to appear for users).



Deploy Report Message

Getting your add-in ready. This might take a few minutes.

You will receive an email notification confirming your successful deployment.
It will take up to 12 hours for the add-in to be displayed on users' ribbons - users might need to relaunch Office.

5. Disable Mailbox auto-forwarding to remote domains

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. In fact, one of the default Alert policies that we enabled in step 2 will notify you when new rules like this show up.

There are two things I would recommend that you do to defend against this:

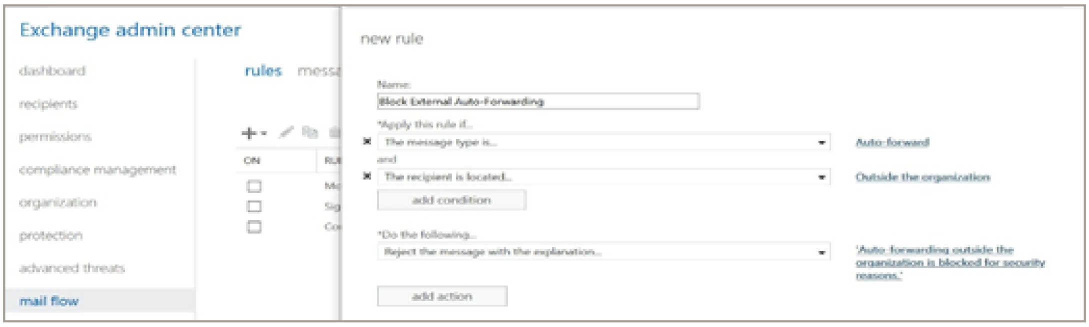
- Create a transport rule that will reject auto-forwarded messages with a notification
- Disable the auto-forward capability globally

Disable Mailbox auto-forwarding to remote domains

To manually create a transport rule in the web portal, go to the E**xchange Admin Center**.

- Under **mail flow**, select **rules**.
- Select **+**, and then **Create a new rule**.
- Select More options at the bottom of the dialog box to see the full set of options.
- **Apply** the settings in the following table.
- Select **Save**.

Setting	Prevent auto forwarding of email
Name	Block External Auto-Forwarding
Apply this rule if ...	The message properties . . . include the message type . . . Auto-forward
Add condition	The recipient . . . is external/internal . . . outside the organization
Do the following ...B	lock the message . . . reject the message and include an explanation.
Provide message text	Auto-forwarding outside the organization is blocked for security reasons.



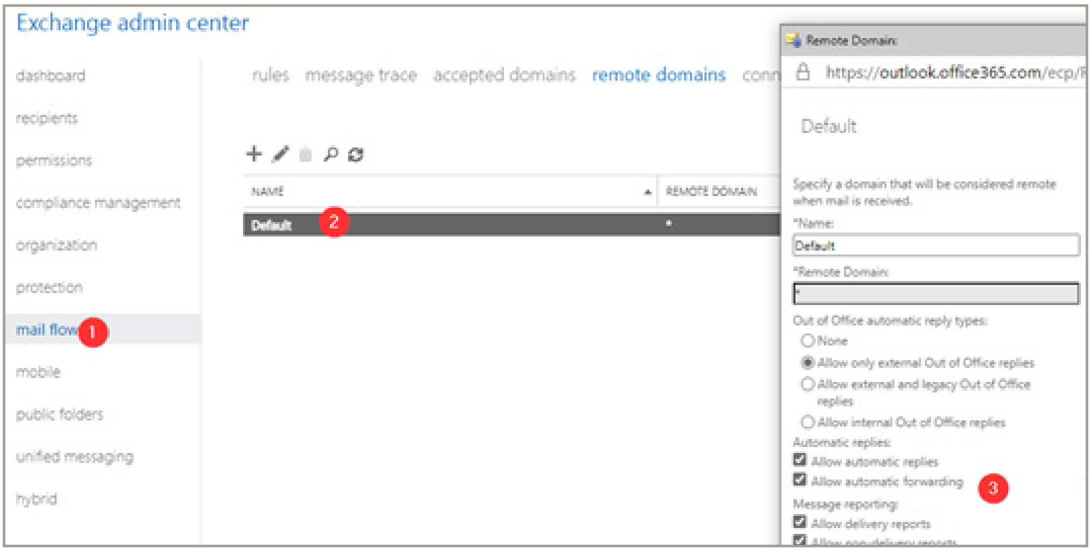
new rule

Name:
Block External Auto-Forwarding

*Apply this rule if...
The message type is... — Auto-forward
and
The recipient is located... — Outside the organization

*Do the following...
Reject the message with the explanation... — 'Auto-forwarding outside the organization is blocked for security reasons.'

Next, in the Exchange admin center also under **mail flow > remote domains**. Edit the **Default** remote domain object **(*)**.



Default *

https://outlook.office365.com/ecp/R

Default

Specify a domain that will be considered remote when mail is received.

*Name:
Default

*Remote Domain:
*

Out of Office automatic reply types:
○ None
● Allow only external Out of Office replies
○ Allow external and legacy Out of Office replies
○ Allow internal Out of Office replies

Automatic replies:
☑ Allow automatic replies
☑ Allow automatic forwarding

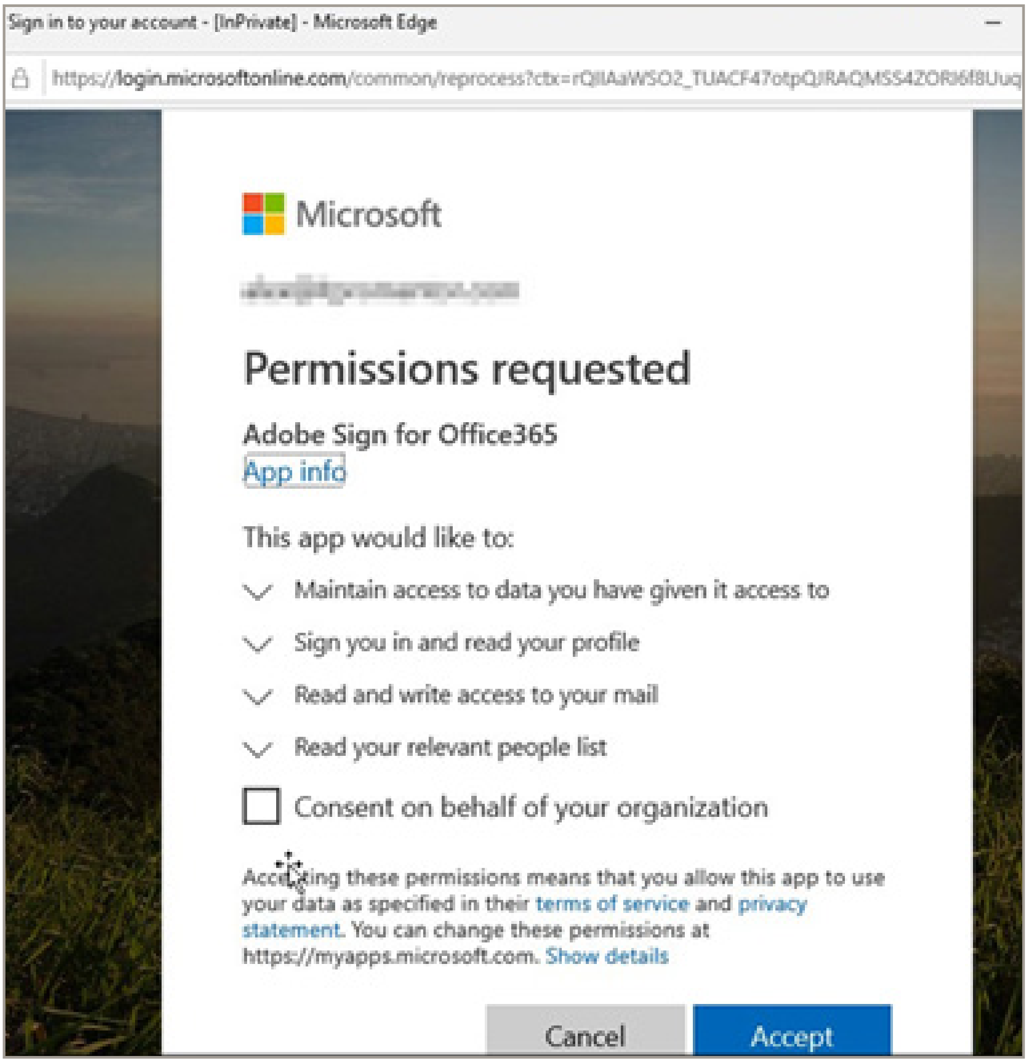
Message reporting:
☑ Allow delivery reports
☑ Allow non-delivery reports

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

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.

6. Enable Admin Consent Requests for Apps

Third-party add-ins and applications for Microsoft 365 may sometimes prompt end users to consent to granting access to Microsoft 365. Example below



Sign in to your account - [InPrivate] - Microsoft Edge

https://login.microsoftonline.com/common/reprocess?ctx=rQIIAaWSO2_TUACF47otpQJRAQMSS4ZORI6f8Uuq

Microsoft

[redacted]

Permissions requested

Adobe Sign for Office365
App info

This app would like to:

- Maintain access to data you have given it access to
- Sign you in and read your profile
- Read and write access to your mail
- Read your relevant people list

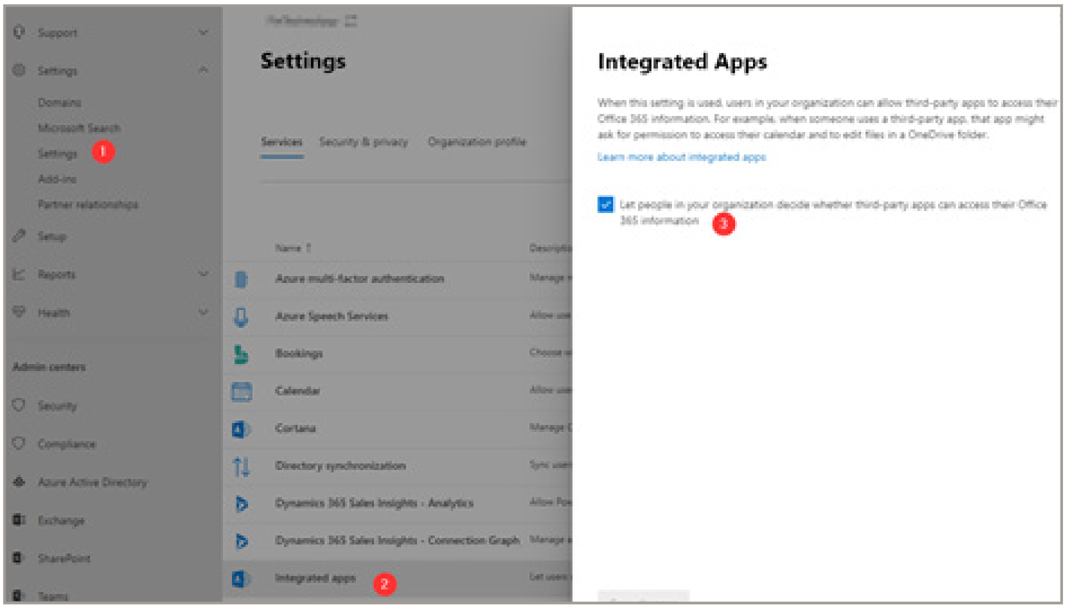
□ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

The reason this is risky is because phishing emails may contain links to malicious apps that trigger this type of workflow, asking the user to grant permissions to their Microsoft 365 data. And this 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).

Now it is possible to prevent users from being able to consent to these requests in the first place. Navigate to the Microsoft 365 admin center, find **Settings > Settings** and then click **Integrated apps**. Clear the checkmark box for **Let people in your organization decide whether third-party apps can access their Microsoft 365 information**.

Enable Admin Consent Requests for Apps



Integrated Apps

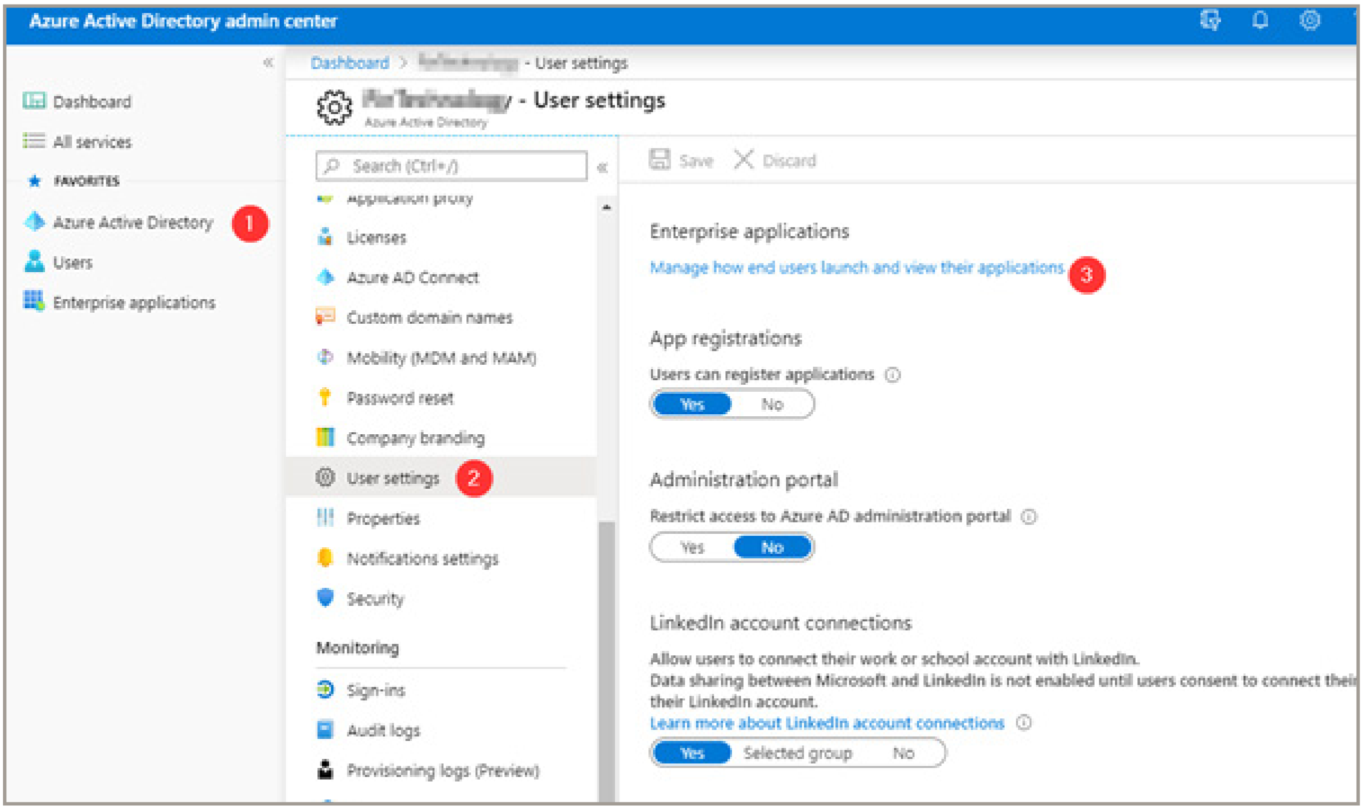
When this setting is used, users in your organization can allow third-party apps to access their Office 365 information. For example, when someone uses a third-party app, that app might ask for permission to access their calendar and to edit files in a OneDrive folder.

Learn more about integrated apps

☑ Let people in your organization decide whether third-party apps can access their Office 365 information

And even that by itself will remove the risk—although users will not be able to integrate with third-party apps in this configuration.

However, there is a new feature available in the Azure AD Admin center which also allows us to enable an “approval process” where admins can review and then approve requests when users attempt to add applications. Set this up in the **Azure AD admin center** under **Enterprise Applications > User Settings > Admin consent requests**.



[redacted] - User settings
Azure Active Directory

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications ⓘ

[✓ Yes] No

Administration portal

Restrict access to Azure AD administration portal ⓘ

Yes [✓ No]

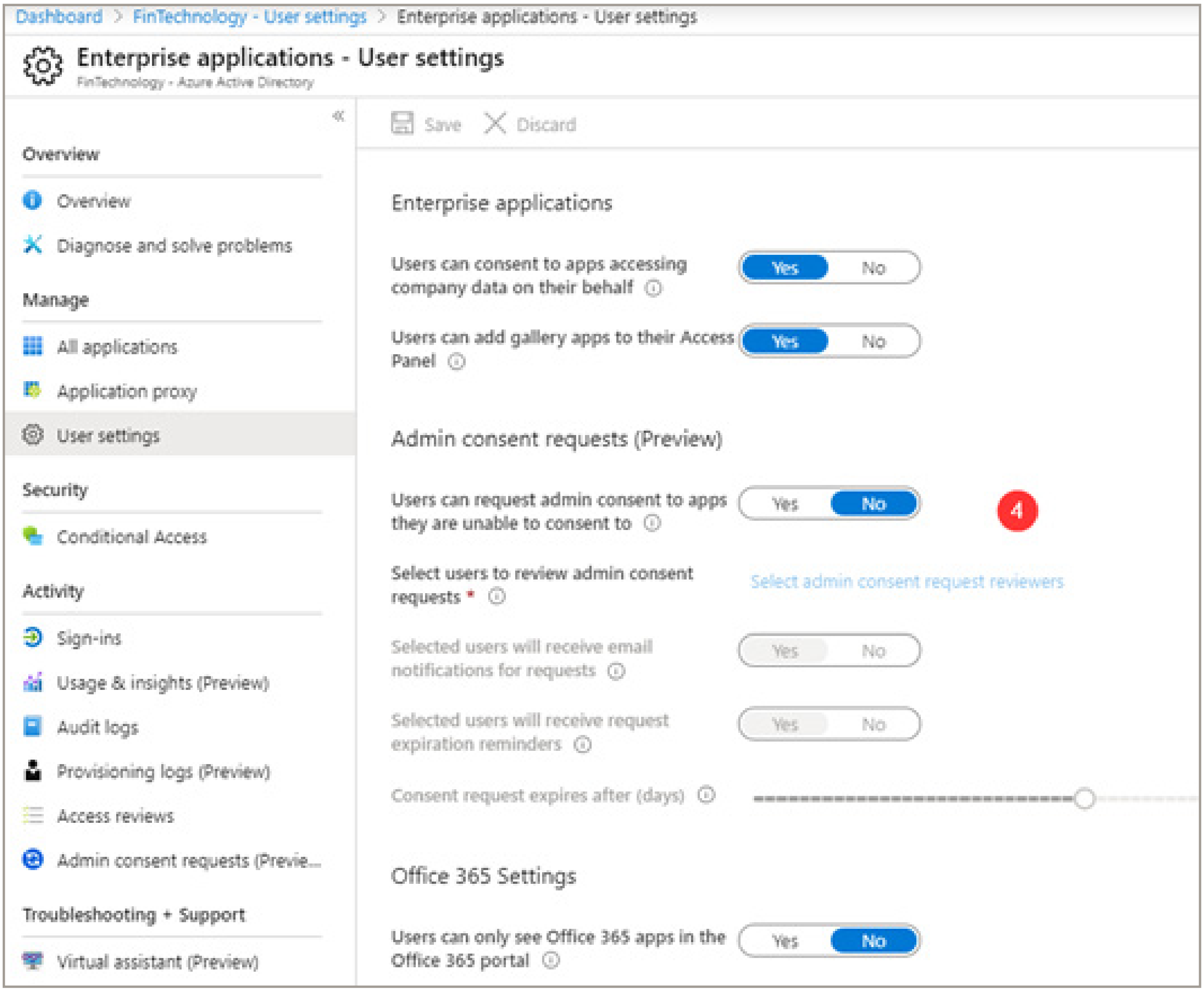
LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their LinkedIn account.

Learn more about LinkedIn account connections ⓘ

[✓ Yes] Selected group No

Enable Admin Consent Requests for Apps



Dashboard > FinTechnology - User settings > Enterprise applications - User settings

Enterprise applications - User settings

FinTechnology - Azure Active Directory

«
Save
Discard
Overview
Overview
Diagnose and solve problems
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Activity
Sign-ins
Usage & insights (Preview)
Audit logs
Provisioning logs (Preview)
Access reviews
Admin consent requests (Previe...
Troubleshooting + Support
Virtual assistant (Preview)
4

Enterprise applications

Users can consent to apps accessing company data on their behalf ⓘ [✓ Yes] No

Users can add gallery apps to their Access Panel ⓘ [✓ Yes] No

Admin consent requests (Preview)

Users can request admin consent to apps they are unable to consent to ⓘ Yes [✓ No]

Select users to review admin consent requests * ⓘ Select admin consent request reviewers

Selected users will receive email notifications for requests ⓘ Yes No

Selected users will receive request expiration reminders ⓘ Yes No

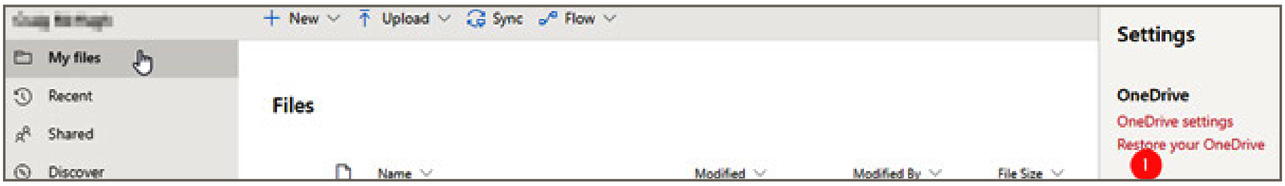
Consent request expires after (days) ⓘ

Office 365 Settings

Users can only see Office 365 apps in the Office 365 portal ⓘ Yes [✓ No]

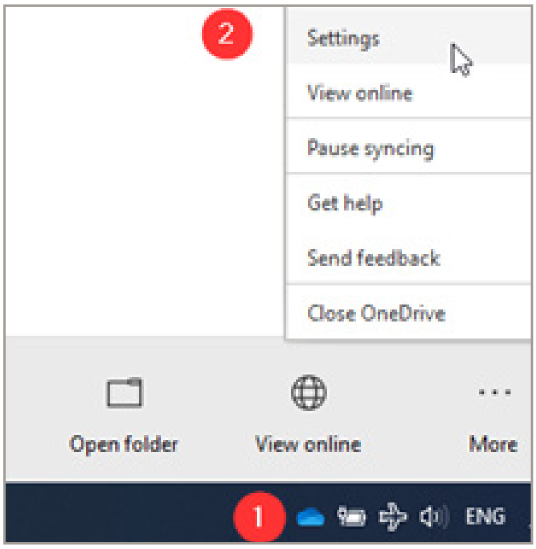
7. Enable OneDrive Backup for Known Folders

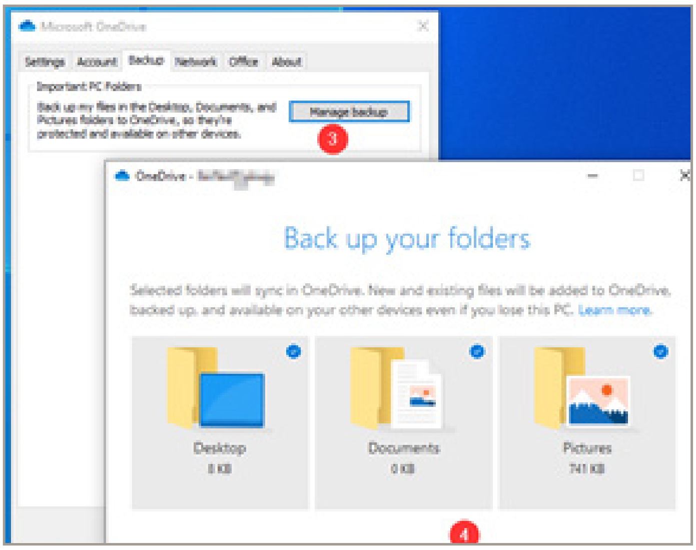
OneDrive includes a fantastic "self-service restore" option that most people don't know about. Self-restore from a major delete or File Encryption! Just be careful it will over write everything. Like turning back the clock. Any created today will be lost if you restored from yesterday.



Just click the gear icon (settings) in the top ribbon and click **Restore your OneDrive**. It is worth noting that this is the only place end users have a "self-service" restore option that is effective against attacks like ransomware.

For the Desktop / Laptop





Back up my files in the Desktop, Documents, and Pictures folders to OneDrive, so they're protected and available on other devices.

Selected folders will sync in OneDrive. New and existing files will be added to OneDrive, backed up, and available on your other devices even if you lose this PC. Learn more.

But the other good news is that you can use the OneDrive client on your Windows 10 endpoints to enable a "Backup" feature that will sync all of the contents of the Desktop, Documents and Pictures library so that these items can also be protected against ransomware in the cloud, and of course have the side-benefit of being made available everywhere (even your mobile device)!

Just click on the OneDrive icon in your tray (near the clock in the lower right corner of the screen), then pick **More > Settings**. On the Backup tab, click Manage backup to configure this feature.
A quick wizard and you will be on your way to cloud backup for your computer's Desktop, Documents and Pictures libraries.

Advanced Security features available with Microsoft 365 plans

The following sections will detail what is possible with more advanced subscriptions such as:

- Microsoft 365 Enterprise E5
- Microsoft 365 Business or Enterprise plans
- Enterprise Mobility + Security plans

If you don't have one of these listed above, I would suggest at least one or two security add-ons for increased protection as well as better visibility into the events within your tenant.

Specifically, I encourage you to consider (in this order):

- Microsoft 365 Advanced Threat Protection P1
- Microsoft Cloud App Security

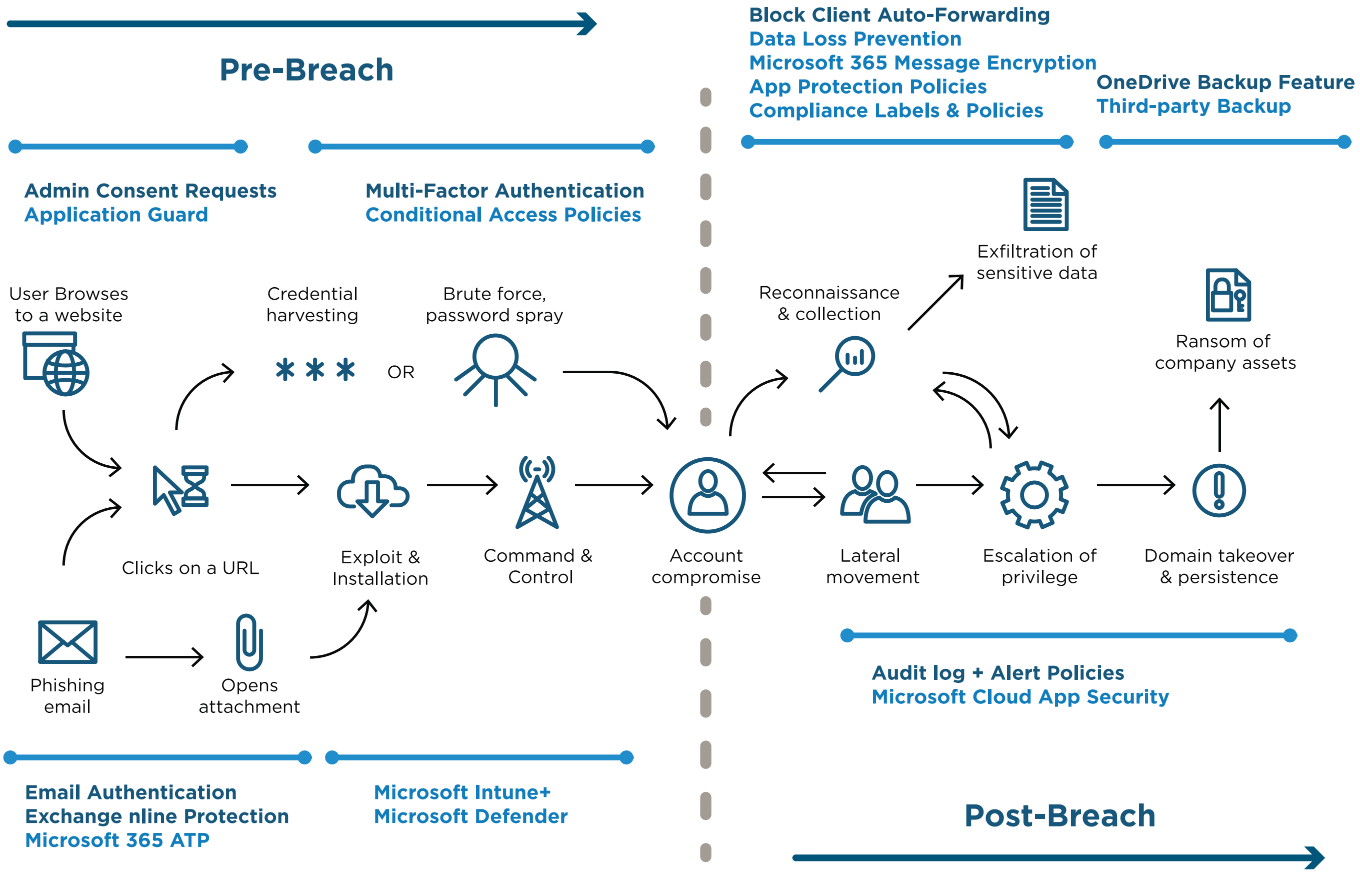
Many features are available with which subscriptions as we proceed. Also, see fortitech staff if more information is required to understand what is included with each major bundle.

1. Microsoft 365 Advanced Threat Protection (ATP)
2. Replace Security Defaults with Conditional Access
3. Configure App Protection Policies (WIP + MAM)
4. Define Compliance Labels & Policies
5. Use Microsoft 365 Message Encryption (OME)
6. Configure a Data Loss Prevention (DLP) Policy
7. Advanced Alerts in Microsoft Cloud App Security

Once again, this is not an exhaustive list.

Advanced Security features available with Microsoft 365 Plans

Now we have additional detail in our visualization of the Attack Kill Chain:



The items in blue can be accomplished only with more advanced subscriptions such as Microsoft 365 or by adding the individual products to another Microsoft 365 subscription.

Pre-Breach events:

- **Microsoft 365 ATP** includes additional AI-assisted protection against phishing and malware.
- **Conditional Access** will replace the Security Defaults and allow you to control how corporate data is accessed from specific devices, apps and locations.
- **Microsoft Intune** and **Microsoft Defender** products, including **Application Guard, Exploit Guard** and other advanced Defender features, will not be covered in this guide. Please refer to my guide on Windows 10 for Business for more details.

Post-Breach events:

- **Data Loss Prevention, Microsoft 365 Message Encryption, App Protection Policies**, and **Compliance Labels** can all work together to wrap boundaries around apps and data— preventing sensitive information and assets from falling into the wrong hands.
- **Microsoft Cloud App Security** contains advanced, intelligent alert policies that clue you into extremely suspicious events like impossible travel, mass download and so on

IS YOUR BUSINESS FORTIFIED?

Get in touch to discover how safe your business is from digital threats, and whether you're making full use of your technology potential.

FORTITECH
Fortify Your Technology

1300 778 078

SALES@FORTITECH.COM.AU

WWW.FORTITECH.COM.AU