MICROSOFT 365 SECURITY CHECKLIST

A PRACTICAL GUIDE FOR THE TIME-STRAPPED ADMIN

BY PAUL SCHNACKENBURG

HORNETSECURITY

WELCOME TO THE MICROSOFT 365 SECURITY CHECKLIST

BROUGHT TO YOU BY HORNETSECURITY.

ABOUT HORNETSECURITY

This eBook is brought to you by Hornetsecurity, the leading global email cloud security and backup provider, which secures companies and organizations of all sizes across the world.

Its award-winning product portfolio covers all important areas of email security, including spam and virus filtering, protection against phishing and ransomware, legally compliant archiving and encryption — as well as email, endpoint and virtual machine backup, replication, and recovery.

Its flagship product, 365 Total Protection, is the most extensive cloud security solution for Microsoft 365 on the market.

BUSINESS 365
TOTAL PROTECTION
ENTERPRISE

The 365 Total Protection Suite seamlessly integrates security and compliance tools for Microsoft 365 and delivers comprehensive security package specifically for Microsoft 365 customers to securely and reliably protect their email communications and data in the cloud from the latest cyber threats.

FREE TRIAL

ABOUT THE AUTHOR

Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. And as much as the IT industry has evolved since then, so has Paul's expertise. He teaches virtualization, networking and cloud technologies at a Microsoft IT Academy. He also runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast in Australia.

Paul is a well-respected technology author and active in the community, writes in-depth technical articles, focused on Microsoft 365, Azure public cloud, Hyper-V, System Center, and private and hybrid cloud technologies. He has MCSE, MCSA and MCT certifications.

Read more articles written by Paul on the Altaro DOJO:

www.altaro.com/dojo/author/paul-schnackenburg/

Or follow his blog:

tellitasitis.com.au

MICROSOFT 365 SECURITY CHECKLIST - INTRODUCTION

There used to be a saying in the SMB IT space – "anyone can set up a Small Business Server (SBS), but only a professional can set it up right".

The same is true now, but instead of SBS it's an Office / Microsoft 365 tenant. A few minutes and a credit card and you can have enterprise-grade email and collaboration tools ready to go, with not a thought for security, governance, or best practices, because after all, "it's in the cloud so Microsoft takes care of it – right"? Well, that's not true and this eBook and accompanying checklist will show you all the settings you should consider configuring.

Depending on what your business is and what sector you operate, there might a minimum requirement of what should be in place to satisfy insurance policies, global data laws or general compliance. So, it's worth taking the time to figure out what your business needs and using this guide to ensure your business is compliant and protected.

Don't set it and forget it.

The reason every security setting isn't turned on by default is of course that every business has different needs and constraints and thus you must find the right balance for your business. And it keeps altering as attacks and the threat landscape, and available options and settings in Microsoft 365, keep changing so this isn't a "set it and forget" list – security is a journey with no end. We'll go through each setting, why you'd want to enable it, what the implications are and our recommended configuration, while the checklist simply lists each setting.

How to navigate this eBook.

This eBook has two intended audiences – a small business owner / IT Pro who is managing their own tenant, and Managed Service Providers (MSPs) who are managing other businesses' tenants, but a lot of the content will be relevant to pretty much all M365 admins. It's divided down into chapters for each major configuration area.

There are two levels of Microsoft 365 licensing, Business and Business Premium for SMBs up to 300 users, and Microsoft 365 E3 / E5 /F3 for larger businesses, or smaller ones that need advanced security features. There's also Office 365 E3 / E5 which doesn't offer device management and other security features.

Generally, every option in the main part of the book is available to Microsoft 365 Business Premium or Microsoft 365 E3 tenants and where there are exceptions, we'll call them out. If your organization is using **Office 365** E3 / E5 most of this book is relevant but you should seriously consider upgrading to Microsoft 365 – the security benefits are huge. If you're an SMB on Business but not Business Premium – there's really no excuse – the amount of security features baked into Premium are well worth it today and will be even more so when Defender for Business is included.

The final chapter is the checklist itself, also available as an Excel sheet to download here, broken down by licensing level.

Following that is an appendix with the acronyms used in the book spelled out (they're also spelled out in the main text the first time they're used) plus a short explanation for each of them.

Let's get started!

TABLE OF CONTENTS

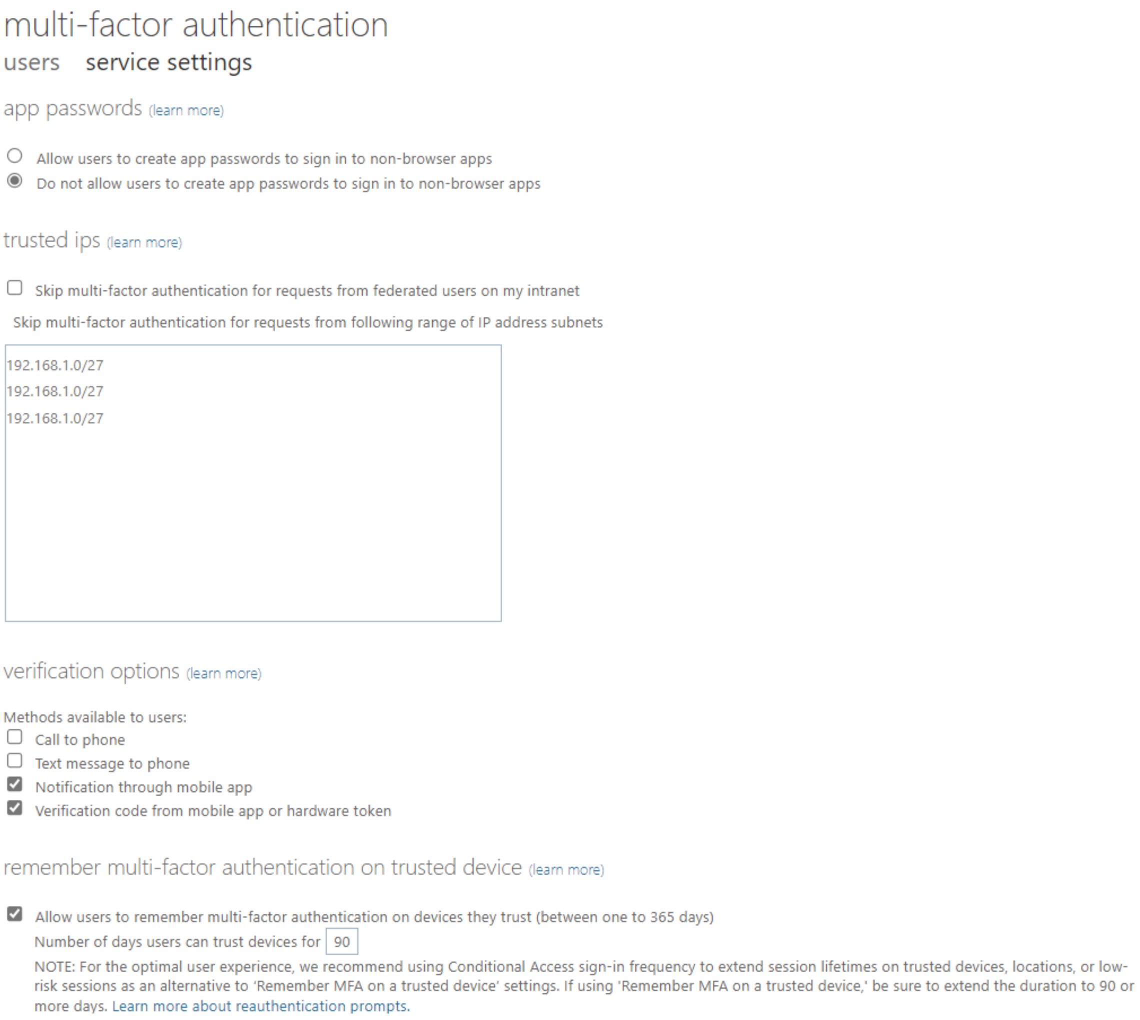
CHAPTER 1 - IDENTITY

MULTI FACTOR AUTHENTICATION

It should be no surprise that we start with identity, it's the new security perimeter or the new firewall and having a strong identity equals strong security. The first step to take here is implementing Multi Factor Authentication (MFA). It's free for all Office / Microsoft tenants. If you want to use Conditional Access (CA) to enforce it (rather than just enabling users "in bulk"), you need Azure AD Premium P1+ licensing. A username and a simple password are no longer adequate (it never was, we just never had a simple, affordable, easy to use alternative) to protect your business.

Hand-in-hand with MFA you need user training. If your business is relying on users doing the right thing when they get the prompt on their phone – they MUST also know that if they get a prompt when they're NOT logging in anywhere, they must click Block / No / Reject.

To enable MFA on a per user basis, go to aad.portal.azure.com, login as an administrator, click Azure Active Directory – Security – MFA and click on the blue link "Additional cloud-based MFA settings".



multi-factor authentication

users   service settings

app passwords (learn more)

○ 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

trusted ips (learn more)

□ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

```
192.168.1.0/27
192.168.1.0/27
192.168.1.0/27
```

verification options (learn more)

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 on trusted device (learn more)

☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 90

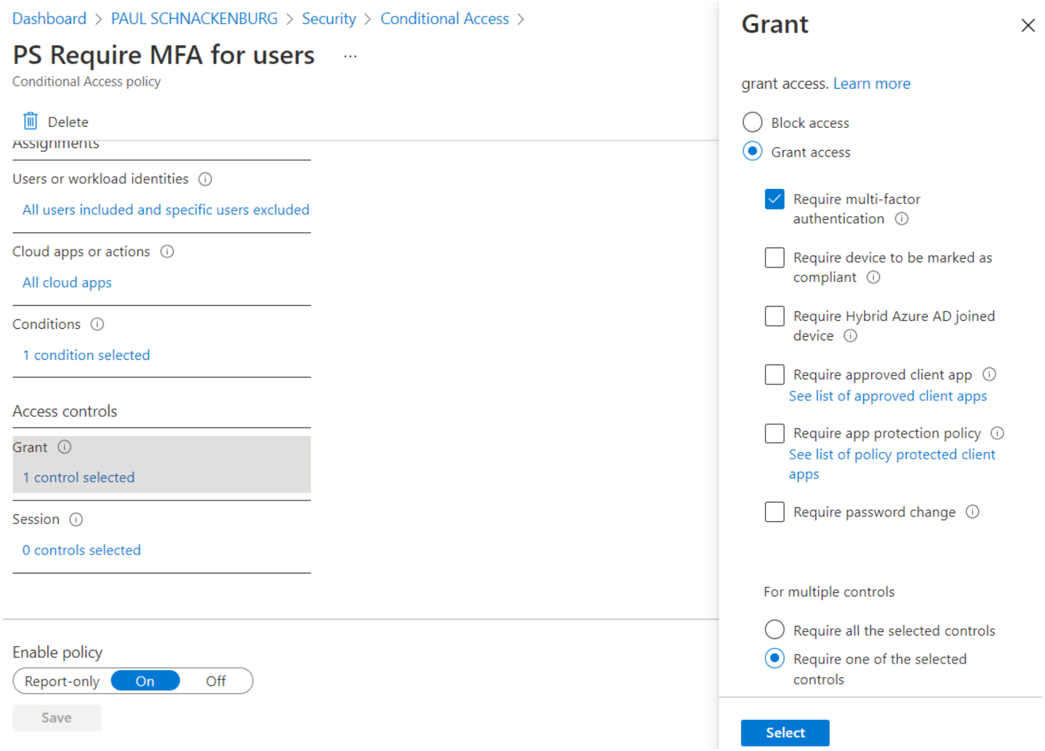
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

Additional MFA settings

There are two parts (tabs) on this page, "service settings" where you should disable app passwords (a workaround for legacy clients that don't support MFA, shouldn't be necessary in 2022), add trusted public IP addresses (so that users aren't prompted when they're in the corporate office – we and Microsoft recommend not using this setting), disabling Call and Text message to phone and remember MFA on trusted devices setting (1-365 days), Microsoft recommends either using CA policies to manage Sign-In frequency or setting this to 90 days. Phone call / text message MFA are not strong authentication methods and should not be used unless there's no other choice.

On the user's tab you can enable MFA for individual users or click bulk update and upload a CSV file with user accounts.

If you have AAD Premium P1, it's better to use a CA policy to enforce MFA, it's more flexible and the MFA settings page will eventually be retired.



Dashboard > PAUL SCHNACKENBURG > Security > Conditional Access >

PS Require MFA for users ···

Conditional Access policy

Delete

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

Report-only [✓ On] Off

Save

Grant ×

grant access. Learn more

○ Block access

● Grant access

☑ Require multi-factor authentication ⓘ

□ Require device to be marked as compliant ⓘ

□ Require Hybrid Azure AD joined device ⓘ

□ Require approved client app ⓘ
See list of approved client apps

□ Require app protection policy ⓘ
See list of policy protected client apps

□ Require password change ⓘ

For multiple controls

○ Require all the selected controls

● Require one of the selected controls

Select

Enforcing MFA with a Conditional Access Policy

A few words of caution, enabling MFA for all your administrators is a given today. Seriously, if you aren't requiring every privileged account to use MFA (or 2FA / passwordless, see below), stop reading and go and do that right now. Yes, it's an extra step and yes, you'll get push back but there's just no excuse – it's simply unprofessional and you don't belong in IT if you're not using it. For what it is worth, I've been using Azure MFA for over seven years and require it for administrators at my clients – no exceptions.

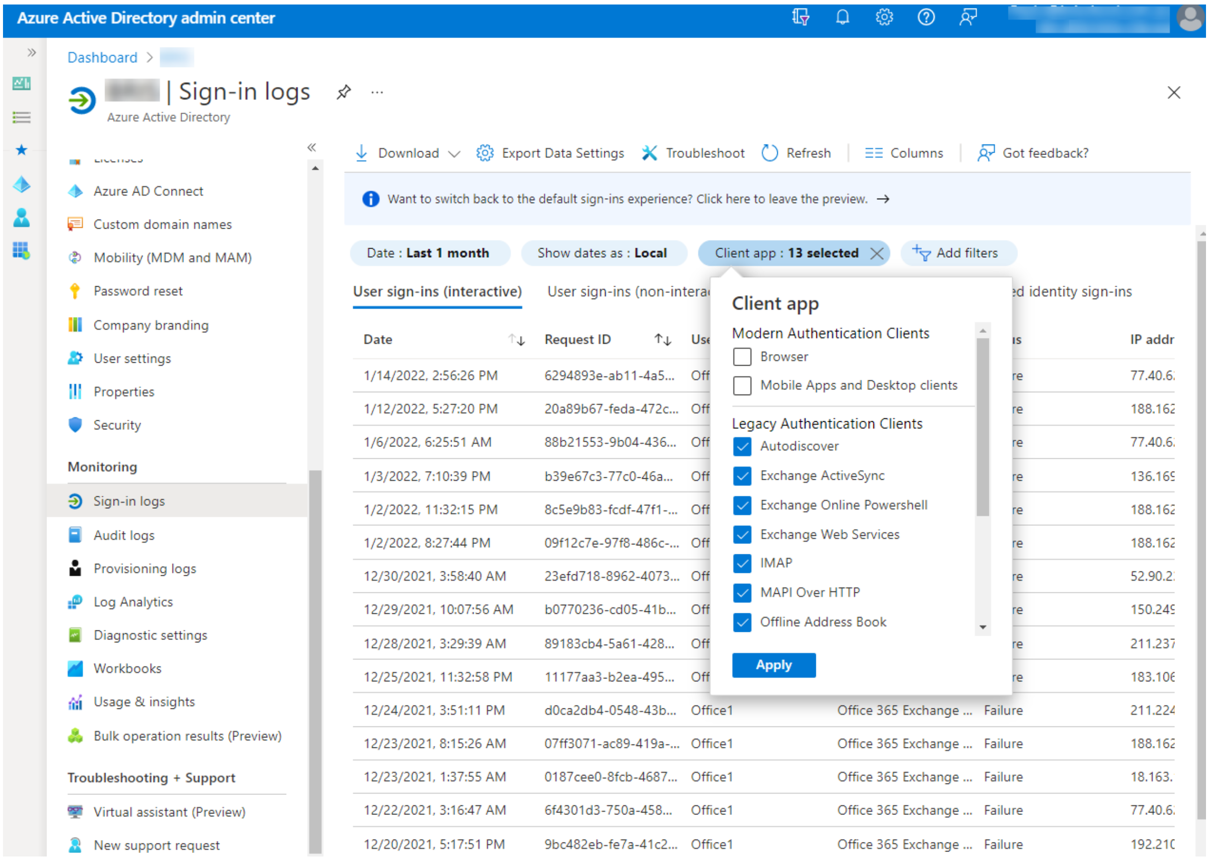
Enabling MFA for all users is also incredibly important but takes some planning. You may have some users who refuse to run the Microsoft Authenticator app on their personal phone – ask for it to be put it in their hiring contract. You need to train them as to **why** MFA is being deployed, what to do, both for authentic logins and malicious ones. Furthermore, you need to have a smooth process for enrolling new users and offboarding people who are leaving.

You should also strongly consider creating separate (cloud only) accounts for administrators. They don't require a license and it separates the day-to-day work of a person who only performs administrative actions in your tenant occasionally (or use PIM, Chapter 10).

MFA protects you against 99.9% of identity based attacks but it's not unphishable. Stronger alternatives include biometrics such as Windows Hello for Business (WHFB) and 2FA hardware keys which bring you closer to the ultimate in identity security: passwordless.

LEGACY AUTHENTICATION

However, it's not enough to enable MFA for all administrators and users, the bad guys can still get in with no MFA prompt in sight. The reason is that Office 365 still supports legacy protocols that don't support modern authentication / MFA. You need to disable these; you can't just turn them off, you need to check if there are legitimate applications / workflows / scripts that use any of them. Go to aad.portal.azure.com, login as a Global Administrator, click Azure Active Directory – Monitoring – Sign-in logs. Change the time to last one month, and click Add filters, then click Client app and then None Selected, in the drop down pick all 13 checkboxes under Legacy Authentication Clients and click Apply.



Want to switch back to the default sign-ins experience? Click here to leave the preview. →

Date : **Last 1 month**

Show dates as : **Local**

Client app : **13 selected**

Client app

Modern Authentication Clients

- □ Browser
- □ Mobile Apps and Desktop clients

Legacy Authentication Clients

- ☑ Autodiscover
- ☑ Exchange ActiveSync
- ☑ Exchange Online Powershell
- ☑ Exchange Web Services
- ☑ IMAP
- ☑ MAPI Over HTTP
- ☑ Offline Address Book

Date	Request ID	Use		ıs	IP addr
1/14/2022, 2:56:26 PM	6294893e-ab11-4a5...	Off		re	77.40.6.
1/12/2022, 5:27:20 PM	20a89b67-feda-472c...	Off		re	188.162
1/6/2022, 6:25:51 AM	88b21553-9b04-436...	Off		re	77.40.6.
1/3/2022, 7:10:39 PM	b39e67c3-77c0-46a...	Off		re	136.169
1/2/2022, 11:32:15 PM	8c5e9b83-fcdf-47f1-...	Off		re	188.162
1/2/2022, 8:27:44 PM	09f12c7e-97f8-486c-...	Off		re	188.162
12/30/2021, 3:58:40 AM	23efd718-8962-4073...	Off		re	52.90.2.
12/29/2021, 10:07:56 AM	b0770236-cd05-41b...	Off		re	150.249
12/28/2021, 3:29:39 AM	89183cb4-5a61-428...	Off		re	211.237
12/25/2021, 11:32:58 PM	11177aa3-b2ea-495...	Off		re	183.106
12/24/2021, 3:51:11 PM	d0ca2db4-0548-43b...	Office1	Office 365 Exchange ...	Failure	211.224
12/23/2021, 8:15:26 AM	07ff3071-ac89-419a-...	Office1	Office 365 Exchange ...	Failure	188.162
12/23/2021, 1:37:55 AM	0187cee0-8fcb-4687...	Office1	Office 365 Exchange ...	Failure	18.163.
12/22/2021, 3:16:47 AM	6f4301d3-750a-458...	Office1	Office 365 Exchange ...	Failure	77.40.6.
12/20/2021, 5:17:51 PM	9bc482eb-fe7a-41c2...	Office1	Office 365 Exchange ...	Failure	192.210

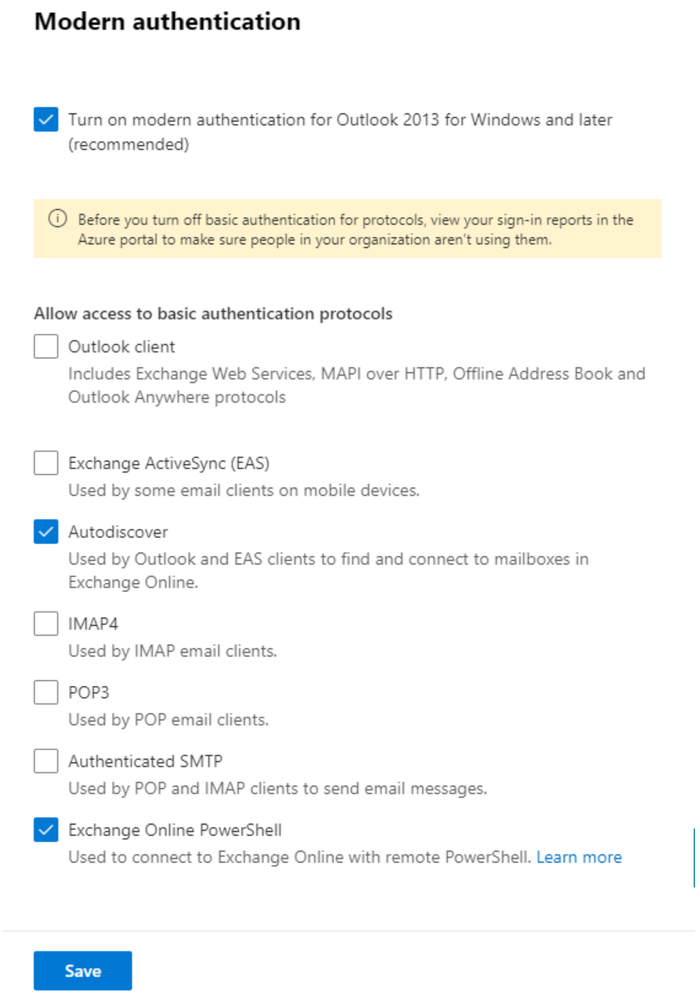
Filtering Azure AD Sign-in logs for legacy authentication

This will show you all the logins over the last month that used any of the legacy protocols. If you get a lot of results, add a filter for Status and add Success to filter out password stuffing attacks that failed. Make sure you check the four different tabs for interactive / non-interactive, service principals and managed identity sign-ins.

You'll now need to investigate the logins. In my experience there will be some users who are using Android / Apple mail on smartphones; point them to the free Outlook app instead (Apple mail can be configured to use modern authentication).

There's also likely to be line-of-business (LOB) applications and printers / scanners that send emails via Office 365, so you'll need updates for these. Alternatively, you can use another email service for these such as smtp2go.

Once you have eliminated all legitimate legacy authentication protocol usage you can disable it in two ways, it's best to use both. Start by creating a Conditional Access policy based on the new template to block it, also go to admin.microsoft.com, Settings – Org settings – Services – Modern authentication and turn off basic authentication protocols.



Modern authentication

☑ Turn on modern authentication for Outlook 2013 for Windows and later (recommended)

ⓘ Before you turn off basic authentication for protocols, view your sign-in reports in the Azure portal to make sure people in your organization aren't using them.

Allow access to basic authentication protocols

☐ Outlook client
Includes Exchange Web Services, MAPI over HTTP, Offline Address Book and Outlook Anywhere protocols

☐ Exchange ActiveSync (EAS)
Used by some email clients on mobile devices.

☑ Autodiscover
Used by Outlook and EAS clients to find and connect to mailboxes in Exchange Online.

☐ IMAP4
Used by IMAP email clients.

☐ POP3
Used by POP email clients.

☐ Authenticated SMTP
Used by POP and IMAP clients to send email messages.

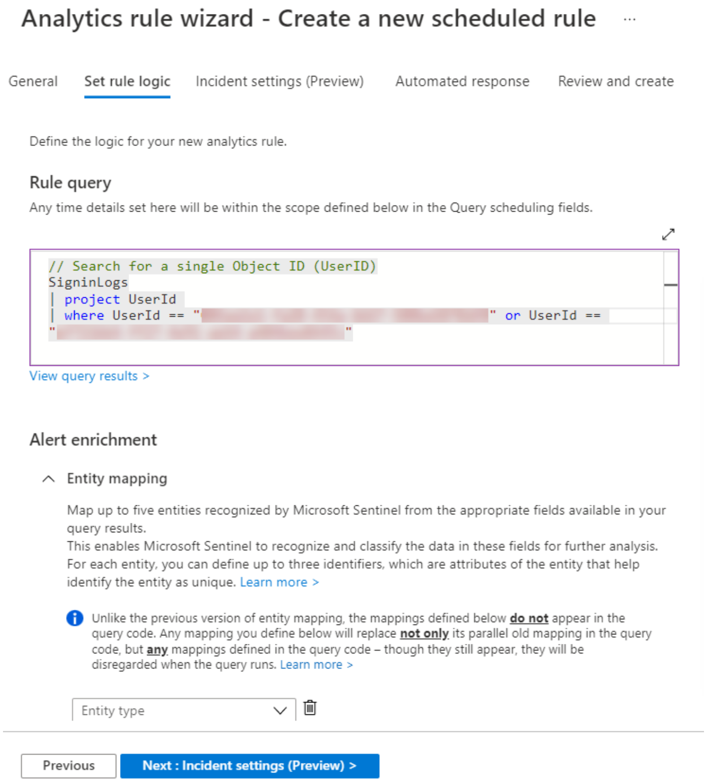
☑ Exchange Online PowerShell
Used to connect to Exchange Online with remote PowerShell. Learn more

Disable legacy authentication protocols in the M365 Admin Center

BREAK GLASS ACCOUNTS

Create at least one, preferably two break glass accounts, also known as emergency access accounts. These accounts are exempted from MFA, all CA policies and PIM (see below) and have very long (40 characters+), complex passwords. They're only used if AAD MFA is down for example, to gain access to your tenant to temporarily disable MFA or a similar setting, depending on the outage.

A second part to this is that you want to be notified if these accounts are ever used. One way to do this is to send your Azure AD sign-in logs to Azure Monitor (also known as Log Analytics), with instructions here. Another option is to use Microsoft Sentinel (which is built on top of Log Analytics) and to create an Analytics rule.



Analytics rule wizard - Create a new scheduled rule ···
General
Set rule logic
Incident settings (Preview)
Automated response
Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
// Search for a single Object ID (UserID)
SigninLogs
| project UserId
| where UserId == "[redacted]" or UserId ==
"[redacted]"
```

Alert enrichment

Entity mapping

Map up to five entities recognized by Microsoft Sentinel from the appropriate fields available in your query results.
This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis.
For each entity, you can define up to three identifiers, which are attributes of the entity that help identify the entity as unique. Learn more >

Unlike the previous version of entity mapping, the mappings defined below **do not** appear in the query code. Any mapping you define below will replace **not only** its parallel old mapping in the query code, but **any** mappings defined in the query code – though they still appear, they will be disregarded when the query runs. Learn more >

Microsoft Sentinel alert rule when a Break Glass account is used

SECURITY DEFAULTS

If yours is a very small business, with few requirements for flexibility, the easiest way to set up Azure AD with MFA for everyone, plus several other security features enabled, is to turn on Security Defaults. Note that you can't have break glass accounts or other service accounts with Security Defaults as there's no way to configure exceptions. Go to Properties for your Azure AD tenant and scroll to the bottom, and click on Manage Security defaults, here you can enable and disable it.

PRIVILEGED IDENTITY MANAGEMENT

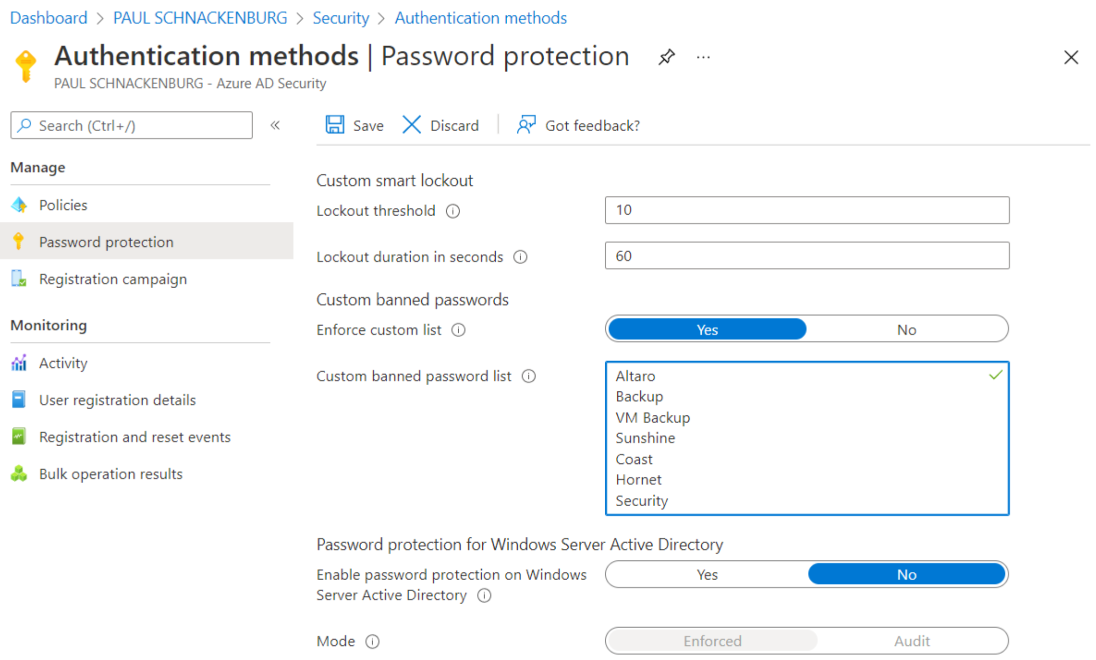
It's worth investing in Azure Active Directory (AAD) Premium P2 for your administrator's accounts and enabling Privileged Identity Management (PIM). This means their accounts are ordinary user accounts who are eligible to elevate their privileges to whatever administrator type they are assigned (see Chapter 10).

If you're not using PIM, create dedicated admin accounts in AAD only. Don't sync these accounts from on-premises but enforce MFA and strong passwords. Since they won't be used for day-to-day work, they won't require a M365 license.

PASSWORD PROTECTION

After MFA, your second most important step is banning bad passwords. You're probably aware that we've trained users to come up with bad passwords over the last few decades with "standard" policies (at least 8 characters, uppercase, lowercase, special character and numbers) which results in P@ssw0rd1 and when they're forced to change it every 30 days, P@ssw0rd2. Both NIST in the US and GHCQ in the UK now recommends allowing (but not enforcing) the use of upper / lowercase etc., but not mandating frequent password changes and instead checking the password at the time of creation against a list of known, common bad passwords and blocking those. In Microsoft's world that's called Password protection which is enabled for cloud accounts by default. There's a global list of about 2000 passwords (and their variants) that Microsoft maintains, based on passwords they find in dumps, and you should add (up to 1000) company specific words (brands, locations, C-suite people's names, local sports teams, etc.) for your organization.

You find Password protection in the AAD portal – Security – Authentication Methods.


Dashboard > PAUL SCHNACKENBURG > Security > Authentication methods
Authentication methods | Password protection
PAUL SCHNACKENBURG - Azure AD Security
Search (Ctrl+/)
Save
Discard
Got feedback?
Manage
Policies
Password protection
Registration campaign
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:
Altaro
Backup
VM Backup
Sunshine
Coast
Hornet
Security

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes [✓ No]

Mode: Enforced Audit

Password protection settings

Remember, you don't have to add common passwords to the list, they're already managed by Microsoft, just add company / region specific words that your staff are likely to use.

If you're syncing accounts from Active Directory on-premises to AAD, you should also extend Password protection to your DCs. It involves the installation of an agent on each DC, a proxy agent, and a reboot of each DC.

CONTINUOUS ACCESS EVALUATION

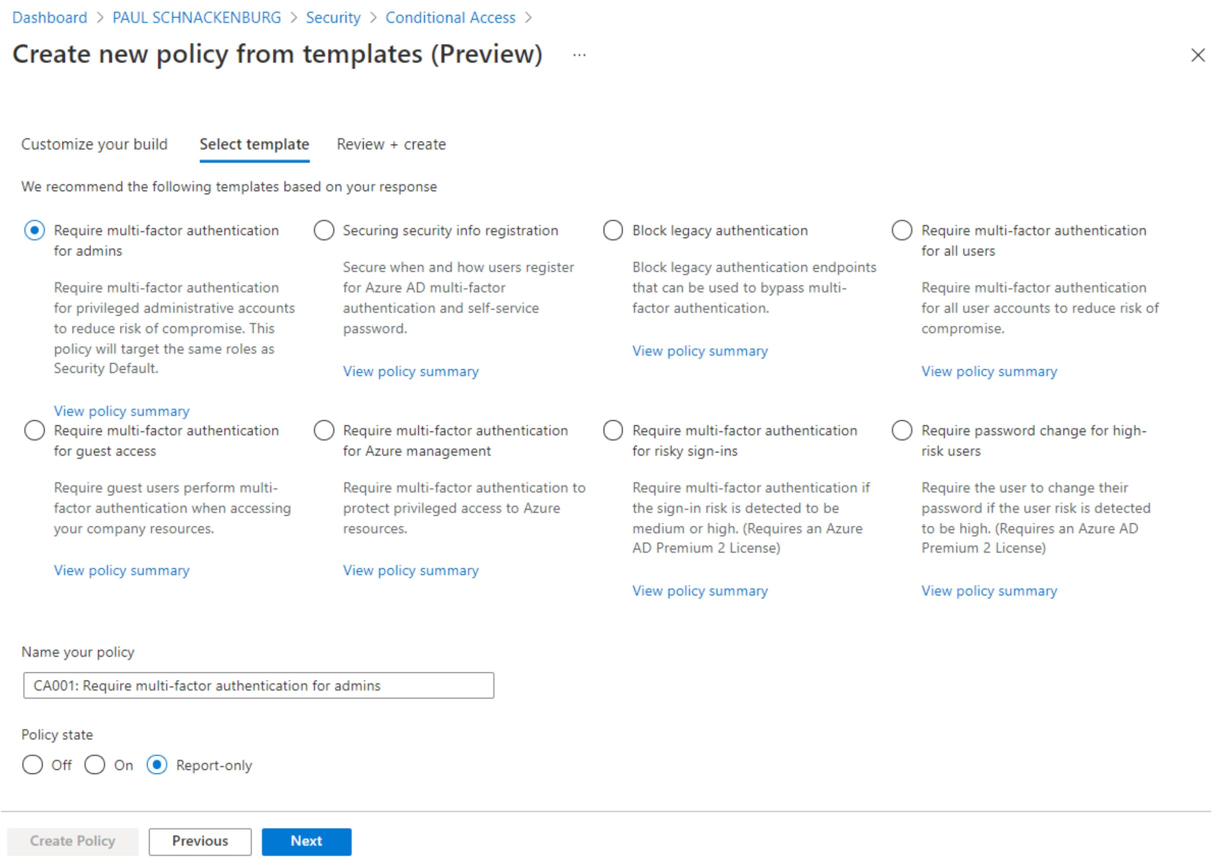
This feature has been in preview for quite some time but is now in general availability. Before Continuous Access Evaluation (CAE), when you disabled a user's account, or they changed location (from the office to a public Wi-Fi for example) it could be up to one hour before their state was re-evaluated and new policies applied, or they were blocked from accessing services. With CAE, this time is much shorter, in most cases in the order of a few minutes. It's turned on by default for all tenants (unless you were part of the preview and intentionally disabled it). Another benefit of CAE is that tokens are now valid for 28 hours, letting people keep working during a shorter Azure AD outage. You can disable CAE in a CA policy, but it's not recommended.

CONDITIONAL ACCESS POLICIES

We've mentioned Conditional Access (CA) policies several times already as it's a crucial component of strong identity security and Zero Trust. Unlike other recommendations, there isn't a one size fit all set of CA policies we can give you, however (at a minimum) you should have policies for:

- Require MFA for admins (see MFA above)
- Require MFA for users (see MFA above)
- Require MFA for Azure management
- Block legacy authentication (see MFA above)
- Require compliant or Hybrid AAD joined device for admins
- Require compliant or Hybrid AAD joined device for users
- Block access to M365 from outside your country
- Require MFA for risky sign-ins (if you have AAD Premium P2)
- Require password change for high-risk users (if you have AAD Premium P2)

This is all going to be a lot easier going forward with the new policy templates for identity and devices. Go to Azure AD – Security – Conditional Access – New policy – Create new policy from templates. Another step to take is to create a system for managing the lifecycle of policies and there's an API for backing up and updating policies, that you can access several ways, including PowerShell. There's even a tutorial to set up a backup system using a Logic App.


Dashboard > PAUL SCHNACKENBURG > Security > Conditional Access >

Create new policy from templates (Preview)

Customize your build
Select template
Review + create

We recommend the following templates based on your response

● Require multi-factor authentication for admins

Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.

View policy summary

○ Securing security info registration

Secure when and how users register for Azure AD multi-factor authentication and self-service password.

View policy summary

○ Block legacy authentication

Block legacy authentication endpoints that can be used to bypass multi-factor authentication.

View policy summary

○ Require multi-factor authentication for all users

Require multi-factor authentication for all user accounts to reduce risk of compromise.

View policy summary

○ Require multi-factor authentication for guest access

Require guest users perform multi-factor authentication when accessing your company resources.

View policy summary

○ Require multi-factor authentication for Azure management

Require multi-factor authentication to protect privileged access to Azure resources.

View policy summary

○ Require multi-factor authentication for risky sign-ins

Require multi-factor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)

View policy summary

○ Require password change for high-risk users

Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)

View policy summary

Name your policy

CA001: Require multi-factor authentication for admins

Policy state

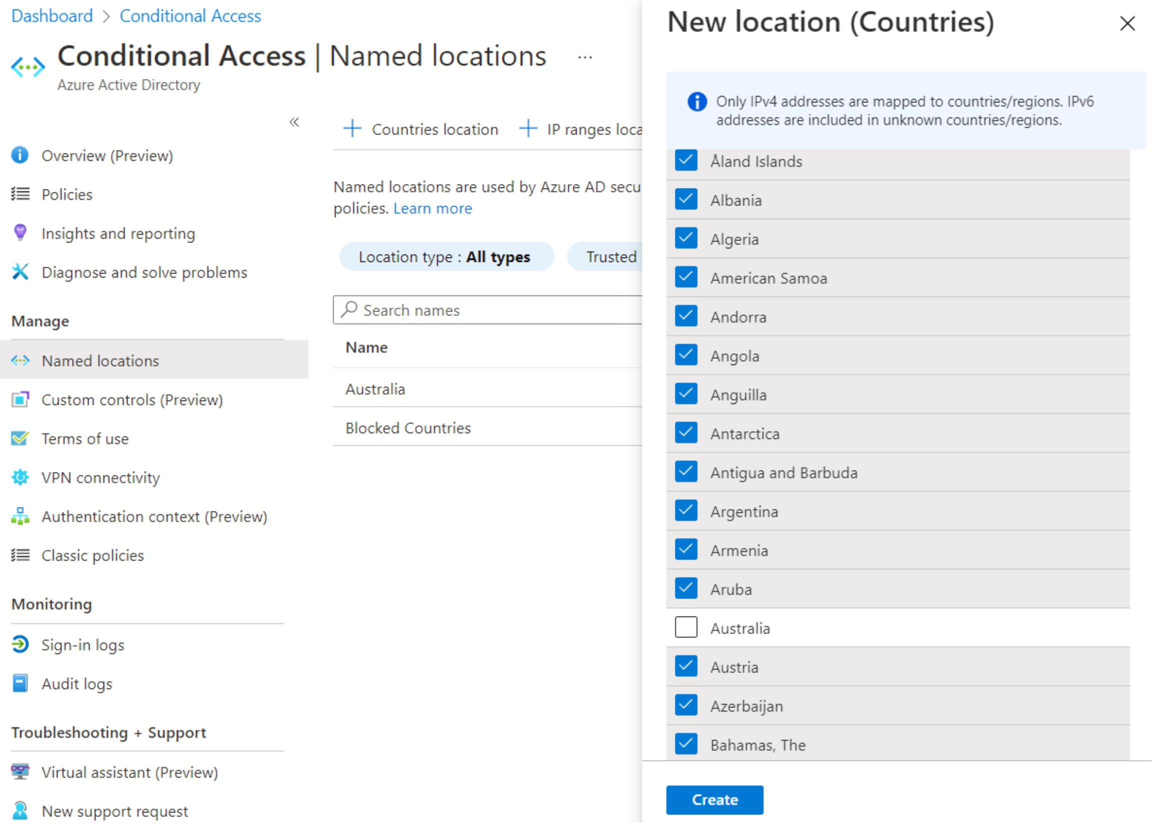
○ Off ○ On ● Report-only

Conditional Access policy templates for identity

A common question is if there's a priority when policies are evaluated and there isn't, they're all processed together for a particular sign-in, from a specific device and location to an individual application. If there are multiple policies with different controls (MFA + compliant device), all controls must be fulfilled for access. And if there are conflicting policies with different access (block vs grant), block access will win.

To get you started, here are the step-by-step instructions for a policy blocking access to M365 from outside your country, appropriate for most small and medium businesses that only operate in one or a few countries. Keep in mind that traveling staff may be caught out by this so make sure you align with business objectives and be aware that this won't stop every attack as a VPN or TOR exit node can make it appear as if the attacker is in your country, but it's one extra step they must take. Remember, you don't have to run faster than the Fancy Bear, just faster than other companies around you.

Start by going to Azure AD – Security – Conditional Access – Named locations and click +Countries location and call the location Blocked countries. Leave Determine location by IP address, a new feature is using GPS location from the Microsoft Authenticator app which will be more accurate once all your users are using Azure AD MFA (and therefore can be located via GPS). Click the box next to Name to select all countries, then find the one(s) that you need to allow login from and click Create.



Dashboard > Conditional Access

Conditional Access | Named locations ···

Azure Active Directory

- Overview (Preview)
- Policies
- Insights and reporting
- Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

+ Countries location + IP ranges loca

Named locations are used by Azure AD secu policies. Learn more

Location type : **All types** Trusted

Search names

Name
Australia
Blocked Countries

New location (Countries) ×

Only IPv4 addresses are mapped to countries/regions. IPv6 addresses are included in unknown countries/regions.

☑ Åland Islands
☑ Albania
☑ Algeria
☑ American Samoa
☑ Andorra
☑ Angola
☑ Anguilla
☑ Antarctica
☑ Antigua and Barbuda
☑ Argentina
☑ Armenia
☑ Aruba
□ Australia
☑ Austria
☑ Azerbaijan
☑ Bahamas, The

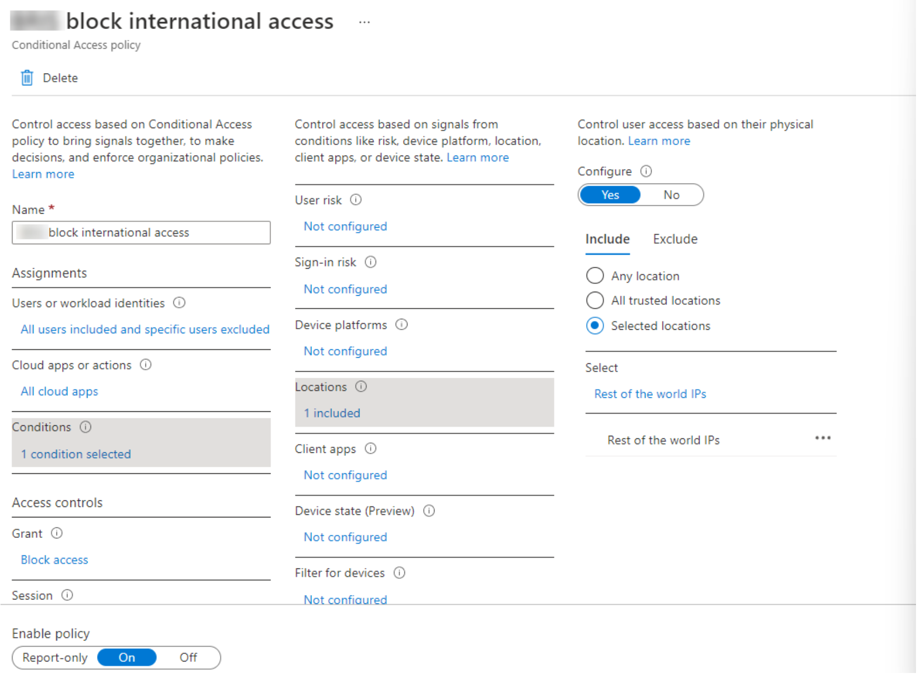
Create

Creating a Named Location for a Conditional Access Policy

Go to Azure AD – Security – Conditional Access – New policy – Create new policy and name your policy with a name that clearly defines what the policy does and adheres to your naming standard. Click on All Users… and Include All users and Exclude your Break Glass accounts.

Click on No cloud apps… and select All cloud apps. Select 0 conditions… and click Not configured under Locations. Pick Selected locations under Include and select your newly created location. Finally, under Access controls – Grant, click 0 controls selected and then Block access.

CA policies can be either in Report-only mode where you can look at reports of what they would have blocked and control they would have enforced, or they can be turned on / off. Report-only can be handy to make sure you don't get fired for accidentally locking everyone out but turn this policy on as soon as possible.



[redacted] block international access ···

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

[redacted] block international access

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk ⓘ

Not configured

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

1 included

Client apps ⓘ

Not configured

Device state (Preview) ⓘ

Not configured

Filter for devices ⓘ

Not configured

Control user access based on their physical location. Learn more

Configure ⓘ

[✓ Yes] No

Include Exclude

○ Any location

○ All trusted locations

● Selected locations

Select

Rest of the world IPs

Rest of the world IPs ···

Enable policy

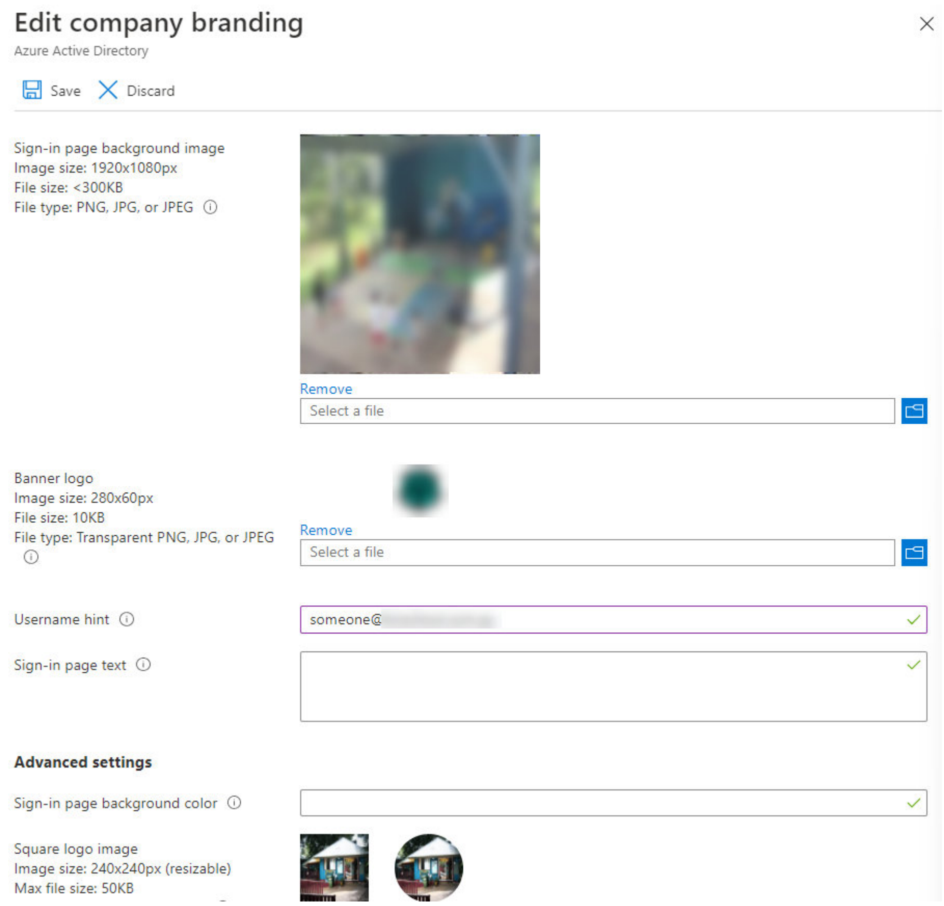
Report-only [✓ On] Off

Conditional Access policy to block logins from outside Australia

A common question is, how can I control how often users are prompted for MFA or signing in again? While it might be counter intuitive the default in Azure AD is a rolling windows of 90 days. Remember, if you change a user's password, block non-compliant devices, or disable an account (plus any number of other CA policies you have in place that might affect the security posture of the session), it'll automatically require new authentications. Don't prompt the users for authentication when nothing has changed because if you do it too frequently, they're more likely to approve a malicious login.

BRANDING LOGON PAGES

While in the Azure AD portal, click on Company branding and add a company specific Sign-in page background image (1920x1080px) and a Banner logo (280x60px). Note that these files have to be small (300 KB and 10 KB respectively) so you may have to do some fancy compression. This isn't just a way to make users feel at home when they see a login page, in most cases when attackers send phishing emails to harvest credentials, they'll send users to a fake login page that looks like the generic Office 365 one, not your custom one which is another clue that should alert your users to the danger. Also – Windows Autopilot doesn't work unless you have customized AAD branding.



Edit company branding

Azure Active Directory

Save Discard

Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG, JPG, or JPEG

Remove

Select a file

Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG, JPG, or JPEG

Remove

Select a file

Username hint: someone@[redacted]

Sign-in page text

Advanced settings

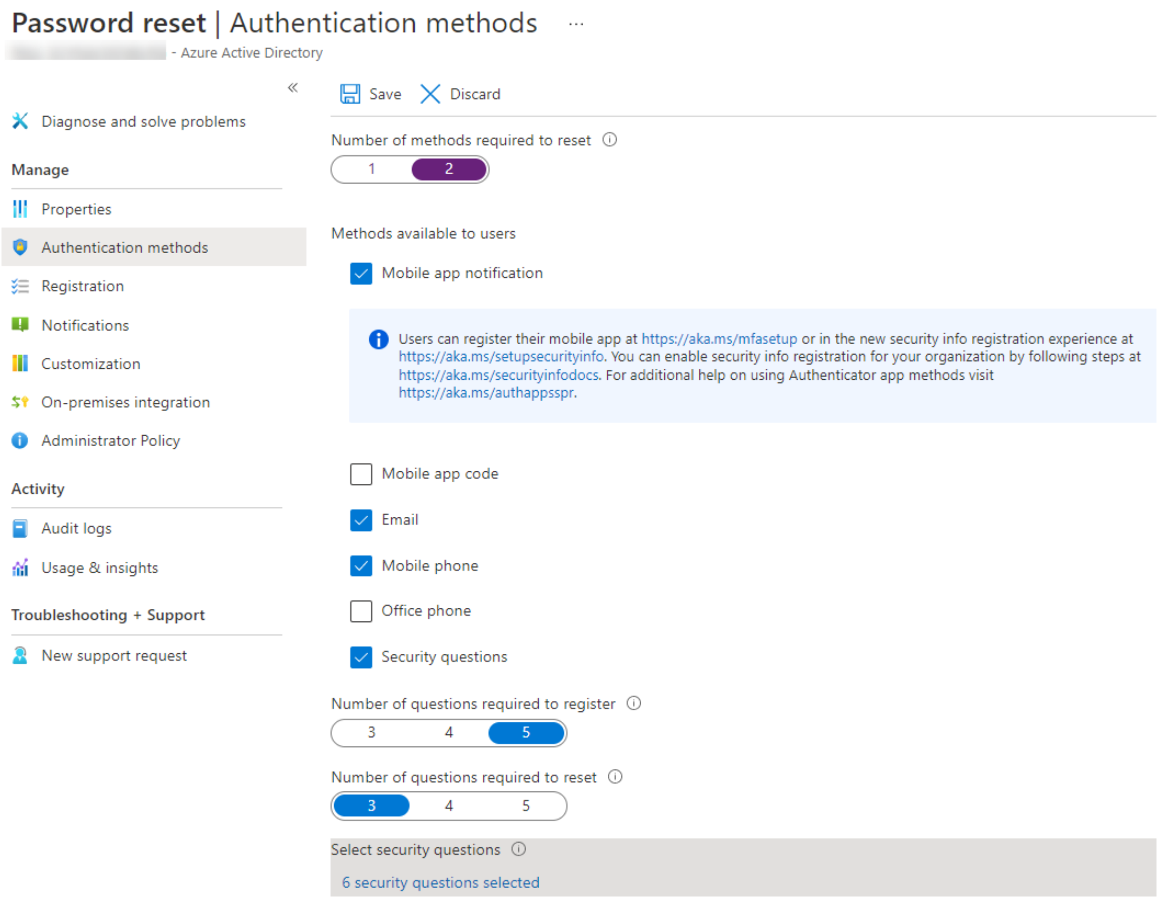
Sign-in page background color

Square logo image
Image size: 240x240px (resizable)
Max file size: 50KB

Edit Azure AD Company Branding images

SELF SERVICE PASSWORD RESET

The benefit of Self Service Password Reset (SSPR) is to lower the load on your help desk to manage password resets for users. Once enabled, users must register various ways of being identified when they're resetting their password, mobile app notification / code, email (non-Office 365), mobile / office phone call, security questions (not available to administrators, plus you can create custom questions). If you are synchronizing user accounts from AD to Azure AD, take care in setting up SSPR as the passwords must be written back to AD from the cloud once changed.



Password reset | Authentication methods ...

[redacted] - Azure Active Directory

Number of methods required to reset ⓘ

1 [✓ 2]

Methods available to users

☑ Mobile app notification

Users can register their mobile app at https://aka.ms/mfasetup or in the new security info registration experience at https://aka.ms/setupsecurityinfo. You can enable security info registration for your organization by following steps at https://aka.ms/securityinfodocs. For additional help on using Authenticator app methods visit https://aka.ms/authappsspr.

☐ Mobile app code

☑ Email

☑ Mobile phone

☐ Office phone

☑ Security questions

Number of questions required to register ⓘ

3 4 [✓ 5]

Number of questions required to reset ⓘ

[✓ 3] 4 5

Select security questions ⓘ

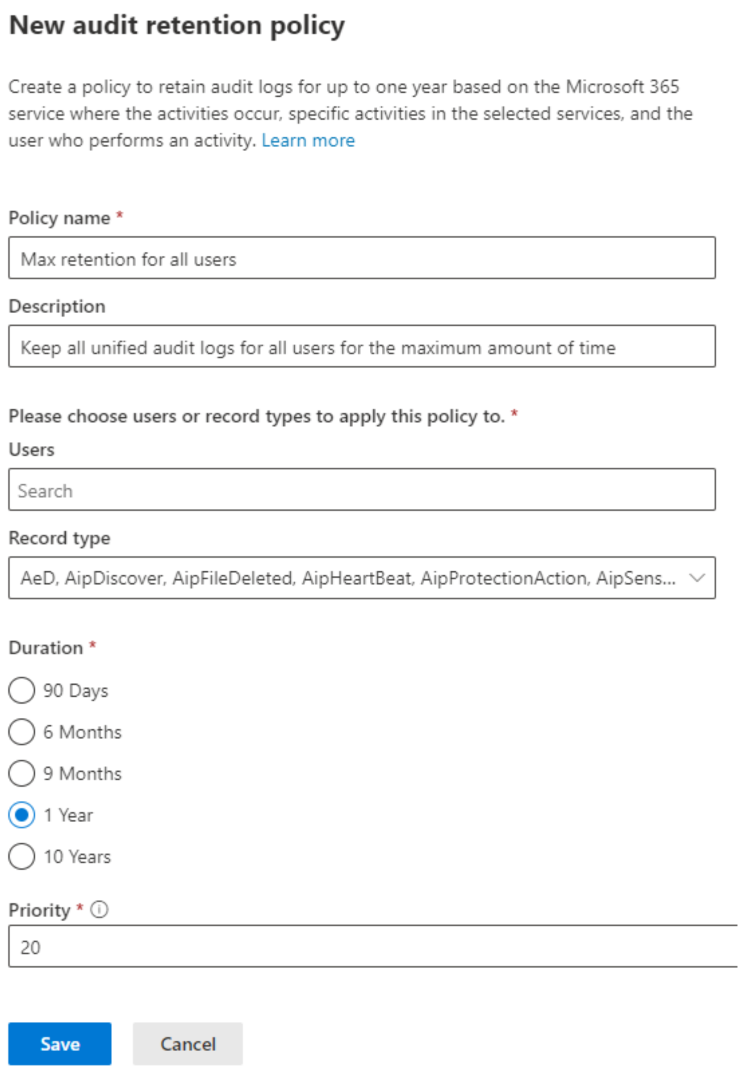
6 security questions selected

Configuring Self Service Password Reset in Azure AD

UNIFIED AUDITING

Not restricted to security but nevertheless a fundamental building block is auditing across Microsoft 365. Go to the Microsoft 365 Defender portal and find Audit in the left-hand menu (it's almost at the end). If for some reason unified auditing isn't enabled in your tenant a yellow banner will give you a button to turn it on (it's on by default for new tenants). Once enabled, click the Audit retention policies tab, and create a policy for your tenant. You want to ensure that you have logs to investigate if there's a breach and you want them kept for as long as possible.

With Business Premium you get a maximum of 90 days retention and Microsoft 365 E5 gives you one year, but you want to make sure to create a policy to set this, rather than rely on the default policy (which you can't see). Give the policy a name, a description and add all the record types, one by one. This policy will now apply to all users (including new ones that are created) for all activities. Only use the Users option when you want to have a specific policy for a particular user. Give the policy a priority, 1 is the highest and 10,000 is the lowest.



New audit retention policy

Create a policy to retain audit logs for up to one year based on the Microsoft 365 service where the activities occur, specific activities in the selected services, and the user who performs an activity. Learn more

Policy name *
Max retention for all users

Description
Keep all unified audit logs for all users for the maximum amount of time

Please choose users or record types to apply this policy to. *

Users
Search

Record type
AeD, AipDiscover, AipFileDeleted, AipHeartBeat, AipProtectionAction, AipSens...

Duration *

○ 90 Days
○ 6 Months
○ 9 Months
● 1 Year
○ 10 Years

Priority *
20

Create an audit retention policy for maximum retention

INTEGRATING APPLICATIONS INTO AZURE AD

One of the most powerful but often overlooked features (at least in SMBs) is the ability to use Azure AD to publish applications to your users. Users can go to myapps.microsoft.com (or office.com) and see tiles for all applications they have access to. But there's more to that story. Say, for example, you have a shared, corporate Twitter account that a few executives and marketing staff should have access to. Instead of sharing a password amongst them all and having to remember to reset it if someone leaves the organization, you can create a security group in AAD, add the relevant users, link Twitter to the group and they'll automatically have access – without knowing the password to the account. There are a lot more actions you can take here to simplify access and secure management of applications, here's more information.

AZURE AD CONNECT

If you're synchronizing accounts from Active Directory to Azure Active Directory (AAD), check the configuration of AAD Connect and make sure you're not replicating an entire domain or forest to AAD. There's no reason that service accounts etc. should be exposed in both directories, start the AAD Connect wizard on the server where it's installed and doublecheck that only relevant OUs are synchronized. One other thing to note here is the fact that any machine running Azure AD Connect should be treated with the same care (in terms of security) as a domain controller. This is because AAD Connect requires the same level of access as AD itself and has the ability to read password hashes.

Making sure security best practices for access, patching, etc. are followed to the letter for the system running AAD connect is critically important.

Identity checklist >

Use the identity checklist to ensure you and your team have implemented strong identity protocols.

CHAPTER 2 – EMAIL

Email persists as one of the most common attack vectors and many high-profile breaches started with a simple phishing email that harvested an ordinary user's credentials. There are two "levels" of protection, Exchange Online Protection (EOP) that everyone enjoys and then Defender for Office 365 P1 and P2.

A dedicated and more secure alternative to EOP and Defender for Office 365 (see below) is 365 Total Protection that offers all the email hygiene services you'll ever need.

Let's start with EOP settings. But first, a word about portals. The main one you should be using is security.microsoft.com, plus compliance.microsoft.com, and maybe admin.exchange.microsoft.com for Exchange specific settings. The old protection.office.com is going to be retired soon, so if you need a list of ALL of them, check out msportals.io.

MAILBOX AUDITING

While auditing of mailbox activities is now turned on for all tenants by default, if you have mailboxes older than 2019, it's a good idea to check that it's turned on. Go to the Admin Center and click on the Cloud Shell icon (>_) in the top right, select PowerShell and then create storage in an Azure subscription.

Alternatively, open a remote PowerShell session to Exchange online.

In Cloud Shell type Connect-EXOPSSession or in PowerShell on your PC type:

```
Connect-ExchangeOnline
```

Followed by:

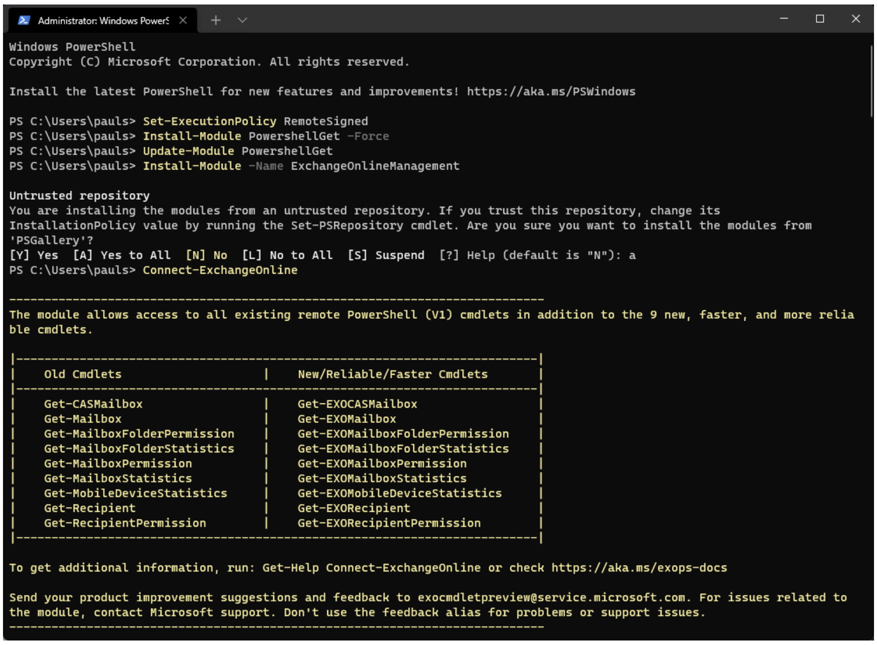
```
Get-Mailbox -Identity nameofmailbox | FL
AuditEnabled
```

Cycle through all your mailboxes with:

```
Get-Mailbox | FL Identity, AuditEnabled
```

And if it’s not enabled, use:

```
Set-Mailbox -Identity nameofmailbox -AuditEnabled
$true
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\pauls> Set-ExecutionPolicy RemoteSigned
PS C:\Users\pauls> Install-Module PowershellGet -Force
PS C:\Users\pauls> Update-Module PowershellGet
PS C:\Users\pauls> Install-Module -Name ExchangeOnlineManagement

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): a
PS C:\Users\pauls> Connect-ExchangeOnline

----------------------------------------------------------------------------
The module allows access to all existing remote PowerShell (V1) cmdlets in addition to the 9 new, faster, and more relia
ble cmdlets.

|--------------------------------------------------------------------------|
|    Old Cmdlets                    |    New/Reliable/Faster Cmdlets       |
|--------------------------------------------------------------------------|
|    Get-CASMailbox                 |    Get-EXOCASMailbox                 |
|    Get-Mailbox                    |    Get-EXOMailbox                    |
|    Get-MailboxFolderPermission    |    Get-EXOMailboxFolderPermission    |
|    Get-MailboxFolderStatistics    |    Get-EXOMailboxFolderStatistics    |
|    Get-MailboxPermission          |    Get-EXOMailboxPermission          |
|    Get-MailboxStatistics          |    Get-EXOMailboxStatistics          |
|    Get-MobileDeviceStatistics     |    Get-EXOMobileDeviceStatistics     |
|    Get-Recipient                  |    Get-EXORecipient                  |
|    Get-RecipientPermission        |    Get-EXORecipientPermission        |
|--------------------------------------------------------------------------|

To get additional information, run: Get-Help Connect-ExchangeOnline or check https://aka.ms/exops-docs

Send your product improvement suggestions and feedback to exocmdletpreview@service.microsoft.com. For issues related to
the module, contact Microsoft support. Don't use the feedback alias for problems or support issues.
----------------------------------------------------------------------------
```

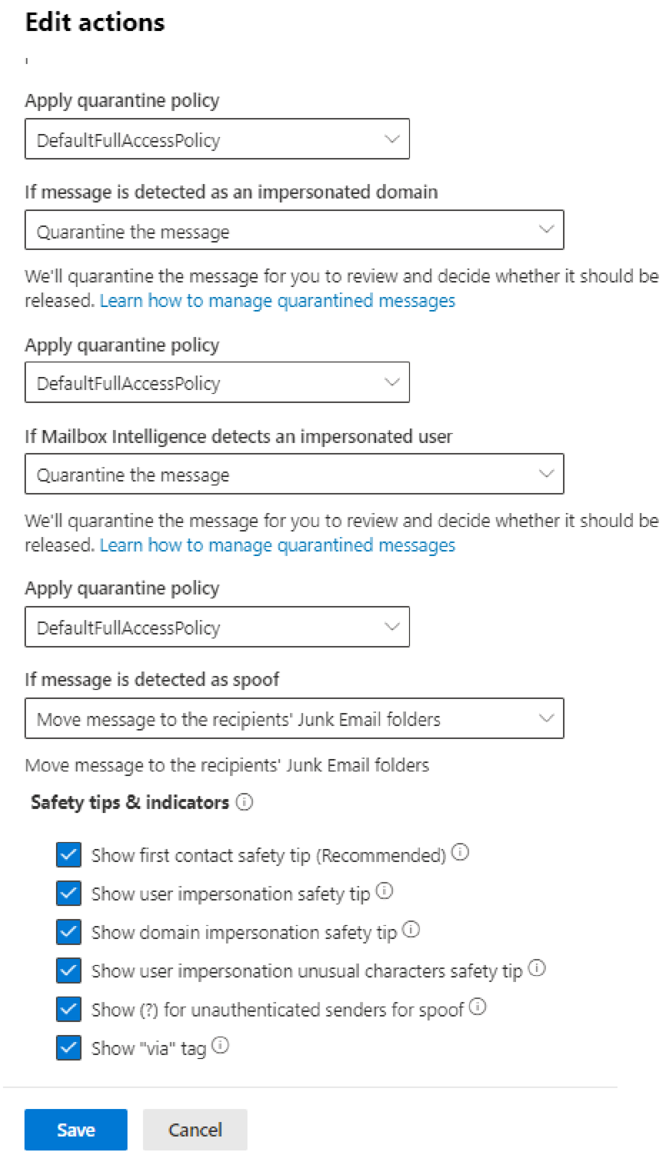
Connecting to Exchange Online with PowerShell

THREAT POLICIES

POLICIES

Go to Policies & rules under Email & collaboration – Threat policies. Click on Anti-phishing and click on the Office365 AntiPhish Default (it might have a different name in your tenant). Scroll down and click on Edit protection settings.
Make sure Include domains I own, don't use trusted senders and domains, enable mailbox intelligence, including for impersonation (it'll look at normal email traffic patterns using Machine Learning and flag anomalous email traffic) and Enable spoof intelligence (some of these settings may only be available if you have Defender for Office 365, see below). That last one may take some extra work, click on the link for Tenant Allow / Block list to see emails that are sent "on behalf" of your organization. There may be legitimate uses, like a monthly email newsletter processed by an outsourced emailing service so make sure they're included in the allow list but block everyone else. Click Save.

Scroll further down and click Edit actions. Here you'll decide what happens to emails that are coming from an impersonated domain / user, and what happens with those messages, we recommend quarantining them with FullAccess by users, but you can also limit access to administrators only. Turn on Safety tips as appropriate for your business.



Edit actions

Apply quarantine policy

DefaultFullAccessPolicy

If message is detected as an impersonated domain

Quarantine the message

We'll quarantine the message for you to review and decide whether it should be released. Learn how to manage quarantined messages

Apply quarantine policy

DefaultFullAccessPolicy

If Mailbox Intelligence detects an impersonated user

Quarantine the message

We'll quarantine the message for you to review and decide whether it should be released. Learn how to manage quarantined messages

Apply quarantine policy

DefaultFullAccessPolicy

If message is detected as spoof

Move message to the recipients' Junk Email folders

Move message to the recipients' Junk Email folders

Safety tips & indicators

- ☑ Show first contact safety tip (Recommended)
- ☑ Show user impersonation safety tip
- ☑ Show domain impersonation safety tip
- ☑ Show user impersonation unusual characters safety tip
- ☑ Show (?) for unauthenticated senders for spoof
- ☑ Show "via" tag

Anti-phishing policy actions and safety tips

Back in Threat policies, click on Anti-spam policies and then the default inbound policy. Start by editing spam threshold and properties. There are many settings here that you can customize based on your specific appetite for spam. The most important one is the threshold, sliding it towards a lower number will lower the amount of spam your users receive, at the cost of maybe quarantining the occasional legitimate message. There are two other settings that you might want to consider setting, if your business only ever deals with English speaking email users or receive email from specific countries, you can mark others as spam. Start typing a language name and a filtered list will appear, the same applies for countries and you can add as many as required to your lists. Another setting you can consider is marking emails that fail an SPF check (see below) as high confidence spam.

Next edit Actions to configure what happens with spam/ high confidence spam / phishing and bulk ("legitimate" advertising emails). Make sure spam safety tips and Zero-hour auto purge (ZAP) is enabled. ZAP basically means that if spam or phish is delivered to some of your users' mailboxes and is later identified as malicious, those messages will be automatically deleted from your users' inboxes.

Connection filtering lets you define IP allow and block lists, again use these only when necessary, even a trusted email sender may be compromised down the track.

The one thing you need to configure in the outbound policy is a group to notify if an internal sender is blocked due to sending outbound spam.

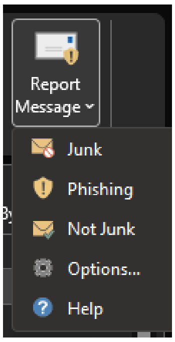
For Anti-malware, open the default policy and select Edit protection settings. Make sure the common attachments filter is enabled and click on customize file types. Most likely there are only 10 selected out of 96 as Microsoft expanded this list recently. Click on the box next to File type to select all of them (unless you have a business reason to allow one) and click Add. Enable ZAP for malware and ensure that only admins have access to quarantined messages. Optionally configure notifications for senders and admins.

RULES

Under Rules you can edit the Allow / Block list and configure DKIM signing (see below). Advanced delivery lets you configure mailboxes for your security teams that can receive any emails, even ones identified as malicious for further analysis, and add domains / IPs and URLs for phishing simulations so that the built-in defenses don't stop your fake phishing emails from reaching your users' inboxes and your fake webpages aren't blocked. An in-depth look at cyber awareness training is beyond the scope of this book but good security is composed of **people**, **process**, and **technology**. Training your users with simulations and follow up training should be done regularly (not just once a year) – see chapter 10.

Enhanced filtering should be configured if you're using a third-party email filtering service and the Quarantine policy lets you customize the policies that we looked at above for spam and phish.

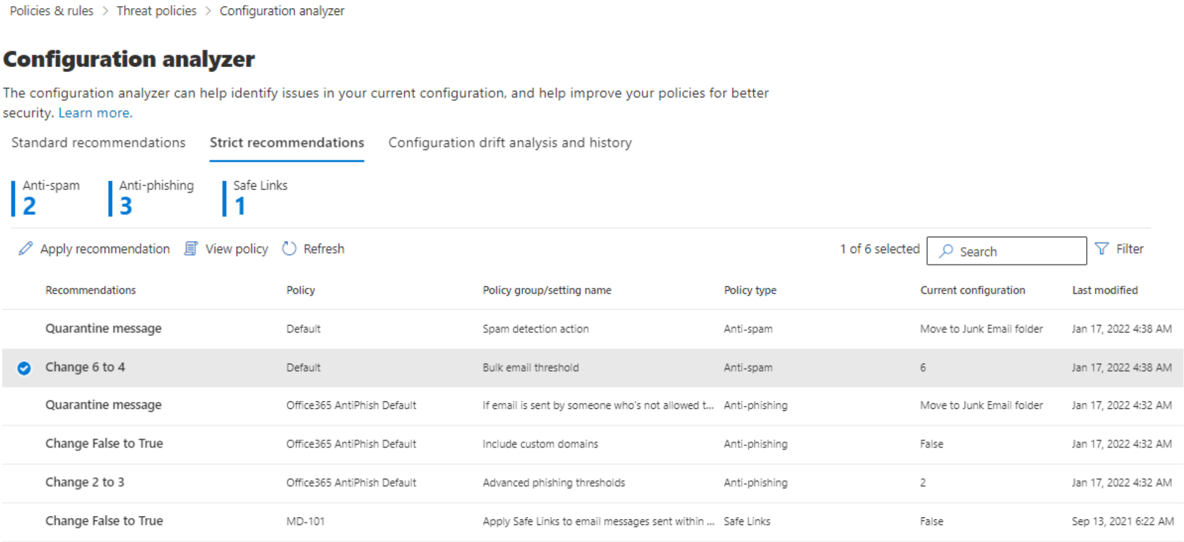
Under Others is another hidden gem – the Outlook Report Message add-in settings. Unless you're using a third-party equivalent solution, turn this on, which will deploy this add-in to every Outlook installation in your tenant. Configure it to send suspicious messages to Microsoft and your organization's mailbox (or only to the org mailbox) and let users choose if they want to report. You can optionally configure the user experience when they report messages. You can also enable a trial of Defender for Office 365 – see below.



Report Message add-in

TEMPLATED POLICIES

Instead of configuring each of the settings above individually you can use the preset security policies to apply Standard or Strict policies OR if you'd like more control, you can use Configuration analyzer to compare your current settings against the Standard / Strict settings and enable each recommendation with a single click. Here I'm changing the bulk email threshold from 6 to 4 based on a recommendation from the Configuration analyzer.


Policies & rules > Threat policies > Configuration analyzer

Configuration analyzer

The configuration analyzer can help identify issues in your current configuration, and help improve your policies for better security. Learn more.

Standard recommendations | **Strict recommendations** | Configuration drift analysis and history

Anti-spam 2 | Anti-phishing 3 | Safe Links 1

Apply recommendation | View policy | Refresh | 1 of 6 selected | Search | Filter

	Recommendations	Policy	Policy group/setting name	Policy type	Current configuration	Last modified
	Quarantine message	Default	Spam detection action	Anti-spam	Move to Junk Email folder	Jan 17, 2022 4:38 AM
✓	Change 6 to 4	Default	Bulk email threshold	Anti-spam	6	Jan 17, 2022 4:38 AM
	Quarantine message	Office365 AntiPhish Default	If email is sent by someone who's not allowed t...	Anti-phishing	Move to Junk Email folder	Jan 17, 2022 4:32 AM
	Change False to True	Office365 AntiPhish Default	Include custom domains	Anti-phishing	False	Jan 17, 2022 4:32 AM
	Change 2 to 3	Office365 AntiPhish Default	Advanced phishing thresholds	Anti-phishing	2	Jan 17, 2022 4:32 AM
	Change False to True	MD-101	Apply Safe Links to email messages sent within ...	Safe Links	False	Sep 13, 2021 6:22 AM

Applying Configuration analyzer recommendation to Threat policies

You can also look at settings changes over time and who performed them.

WARN AND BLOCK EMAILS WITH DANGEROUS ATTACHMENTS

If you're not using Defender for Office 365 you can consider creating mail flow (formerly known as transport rules) to warn users when they receive emails with attachments that are commonly used as a vector for malware and ransomware. Microsoft has recommended steps here.

Be aware that this might protect your organization against "traditional" ransomware, a malicious attachment with code that encrypts all local and network share files that the user has access to and demands a bitcoin ransom for the key. Due to the big administrative overhead and relatively low yields however, this isn't a common type of attack today. More common is big game ransomware where attackers phish your users for credentials or buy them on the dark web, gain access and infiltrate your business thoroughly, possibly corrupting your backups and exfiltrating your data so that when they do launch the attack you can't recover and as an extra incentive to pay, they can dump the sensitive data they stole publicly. And they'll ask for as large a ransom as they know you can pay, after researching your organization's financial position.

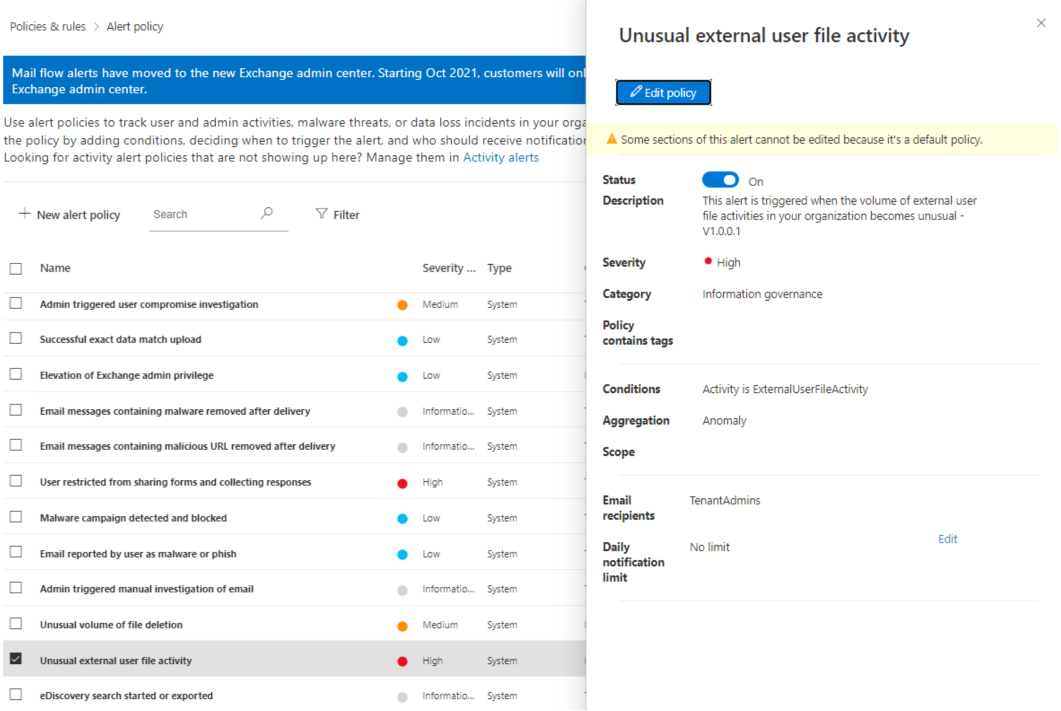
OFFICE MESSAGE ENCRYPTION

Sending emails is like sending a postcard, anyone along the way can read it. Office Message Encryption (OME) comes with two different options, Do not forward and Encrypt, and lets you send protected emails to any email address. It's very easy to use in Outlook / Outlook Web App so train your users, additionally you can create Mail flow rules to automatically encrypt emails for specific domains or recipients.

If you have a regulation that requires the use of S/MIME for email encryption you can do this in Exchange Online as well. There's a lot more set up to do before your users can email others using the digital signatures and optional encryption offered by this legacy protocol, but it's available if required.

ALERT POLICY

Configuring the right settings is only half the battle. You also need to know when things happen in your environment, so go back to Policies & rules and click Alert policy. Here you can look at the built-in policies and add your own. The default policies will email all Tenant admins when they're triggered. Click +New alert policy and investigate the options available, including the extensive list of actions that you can trigger an alert on.



Mail flow alerts have moved to the new Exchange admin center. Starting Oct 2021, customers will onl
Exchange admin center.

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your orga
the policy by adding conditions, deciding when to trigger the alert, and who should receive notificatior
Looking for activity alert policies that are not showing up here? Manage them in Activity alerts

□	Name		Severity ...	Type
□	Admin triggered user compromise investigation	●	Medium	System
□	Successful exact data match upload	●	Low	System
□	Elevation of Exchange admin privilege	●	Low	System
□	Email messages containing malware removed after delivery	●	Informatio...	System
□	Email messages containing malicious URL removed after delivery	●	Informatio...	System
□	User restricted from sharing forms and collecting responses	●	High	System
□	Malware campaign detected and blocked	●	Low	System
□	Email reported by user as malware or phish	●	Low	System
□	Admin triggered manual investigation of email	●	Informatio...	System
□	Unusual volume of file deletion	●	Medium	System
☑	Unusual external user file activity	●	High	System
□	eDiscovery search started or exported	●	Informatio...	System

Unusual external user file activity

⚠ Some sections of this alert cannot be edited because it's a default policy.

Status	On
Description	This alert is triggered when the volume of external user file activities in your organization becomes unusual - V1.0.0.1
Severity	● High
Category	Information governance
Policy contains tags	
Conditions	Activity is ExternalUserFileActivity
Aggregation	Anomaly
Scope	
Email recipients	TenantAdmins
Daily notification limit	No limit

Alert Policy in Microsoft 365 Defender

DEFENDER FOR OFFICE 365

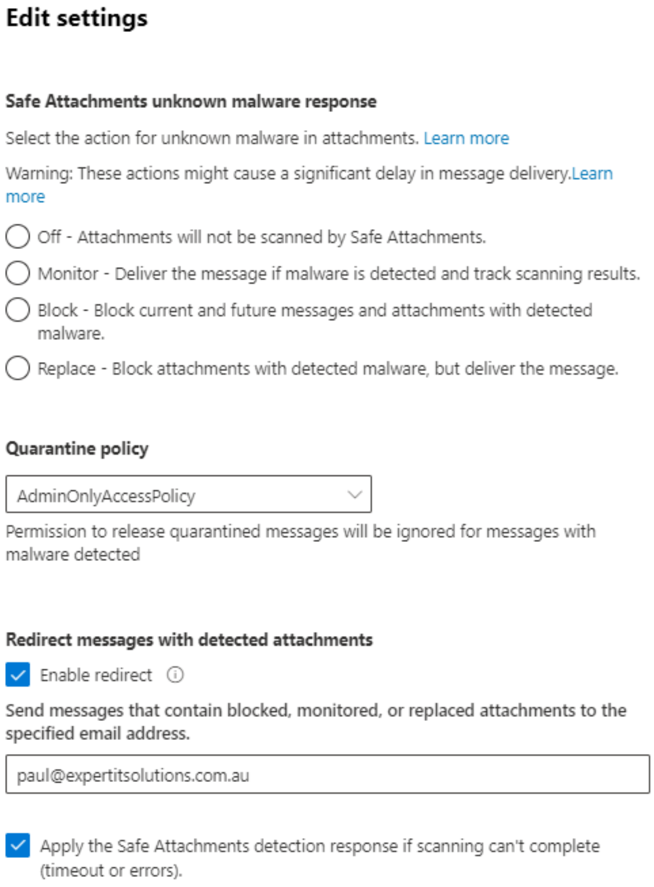
On top of EOP sits Microsoft Defender for Office 365 (MDO), specifically policies for Safe attachments and Safe links. There are three licensing levels, P1, P2 and Microsoft 365 E5. Plan 2 is included in Office 365 E5 and Microsoft 365 E5, whereas Plan 1 is part of Microsoft 365 Business Premium.

Here we're going to look at P1 and what it brings to the table. P2 adds Threat trackers, Threat Explorer, Automated investigation, and response (AIR) and Attack simulation training – see Chapter 10.

An alternative and more cost effective offering to MDO is 365 Total Protection from Hornetsecurity that provides complete email protection for both SMBs and Enterprises and optionally backup as well.

SAFE ATTACHMENTS

All incoming emails and their attachments to your tenant are scanned by three independent AV engines and any known malware is filtered out by Exchange Online Protection (EOP). For never-before-seen attachments that pass the AV scanning however, if you have a Safe attachment policy, they'll be activated in a VM to catch zero-day attacks. Head back to Threat policies and click Safe attachments and click +Create. Add a name, description, and the domains in your tenant and select Dynamic delivery and optionally redirect emails with identified malware to a security team inbox. Dynamic delivery will show the email in the user's inbox, and they can even preview the attached document as they're waiting for the scan to complete, usually less than a minute in my experience.



Edit settings

Safe Attachments unknown malware response

Select the action for unknown malware in attachments. Learn more

Warning: These actions might cause a significant delay in message delivery.Learn more

○ Off - Attachments will not be scanned by Safe Attachments.

○ Monitor - Deliver the message if malware is detected and track scanning results.

○ Block - Block current and future messages and attachments with detected malware.

○ Replace - Block attachments with detected malware, but deliver the message.

Quarantine policy

AdminOnlyAccessPolicy

Permission to release quarantined messages will be ignored for messages with malware detected

Redirect messages with detected attachments

☑ Enable redirect

Send messages that contain blocked, monitored, or replaced attachments to the specified email address.

paul@expertitsolutions.com.au

☑ Apply the Safe Attachments detection response if scanning can't complete (timeout or errors).

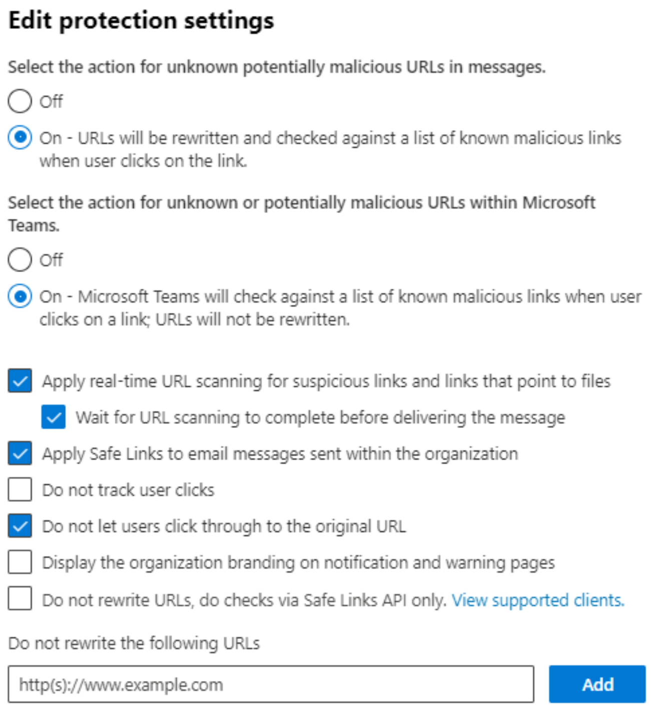
Safe attachment policy settings

Back on the Safe attachments page, look the Global settings and enable MDO for SharePoint, OneDrive, and Teams and if you have M365 E5 – enable Safe Documents which will use the same VM scanning technology on untrusted documents when they're opened in Protected View in Office desktop.

SAFE LINKS

This is another great protection against malicious URLs in emails and Teams messages, again create your own policy and add your domains. Turn it on for both URLs in messages and Teams and enable real-time URL scanning so that they're scanned at the time of click (often attackers will compromise a website, send emails with links to the benign pages, wait until the emails have been delivered and the URLs scanned and declared safe and then weaponize the URLs). Make sure you select "Do not let users click through to the original URL", you can also scan internal email messages and specify URLs that won't be rewritten.

Once Safe links is enabled the URLs are rewritten to be passed through Microsoft's servers but if you hover the cursor over them in an email the original URL is still shown so that users can make a judgement call as to their legitimacy.



Edit protection settings

Select the action for unknown potentially malicious URLs in messages.

○ Off

● On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

Select the action for unknown or potentially malicious URLs within Microsoft Teams.

○ Off

● On - Microsoft Teams will check against a list of known malicious links when user clicks on a link; URLs will not be rewritten.

☑ Apply real-time URL scanning for suspicious links and links that point to files

  ☑ Wait for URL scanning to complete before delivering the message

☑ Apply Safe Links to email messages sent within the organization

□ Do not track user clicks

☑ Do not let users click through to the original URL

□ Display the organization branding on notification and warning pages

□ Do not rewrite URLs, do checks via Safe Links API only. View supported clients.

Do not rewrite the following URLs

http(s)://www.example.com

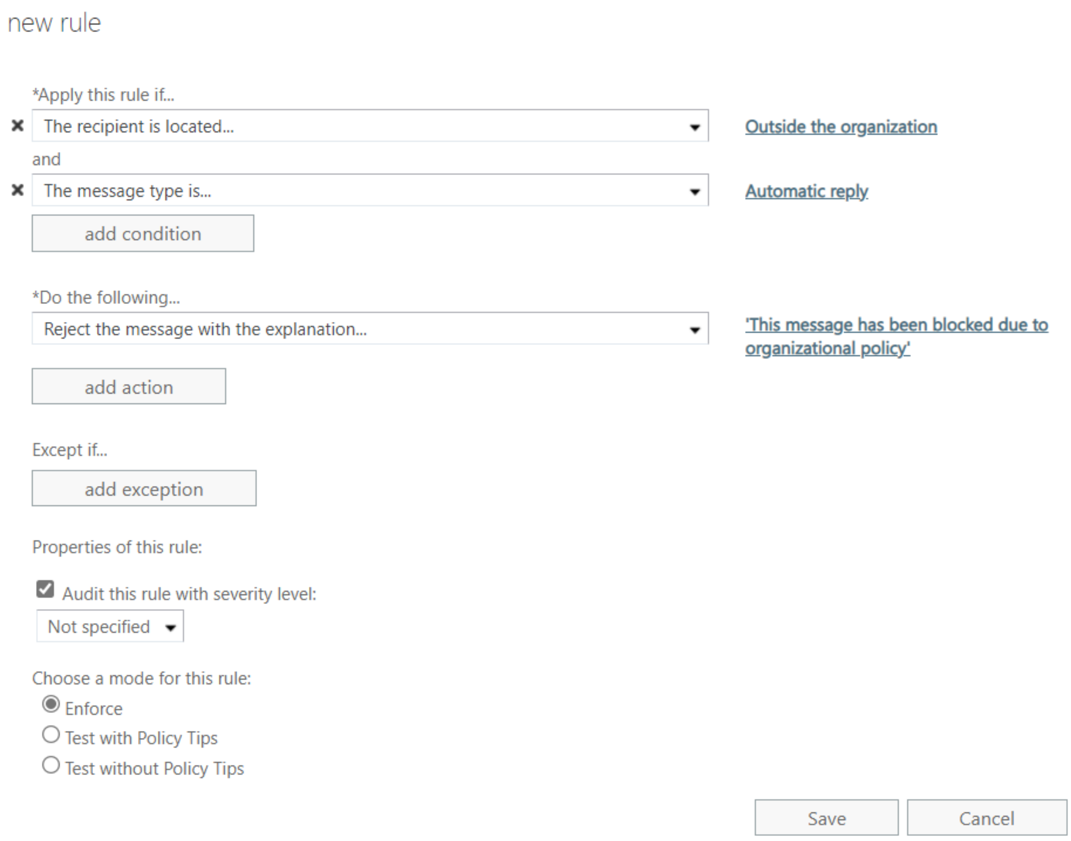
Safe links policy settings

Back on the Safe links page, explore the Global settings and make sure to enable it for Office 365 (desktop, mobile, web) -apps so that links in Word and Excel documents are also scanned there and again ensure that users can't click through to the original URL.

DISABLE FORWARDING TENANT WIDE

A common tactic for criminals once they have compromised a user's account is setting up email forwarding to an external mailbox to watch for sensitive information and email patterns, perhaps as a precursor to a Business Email Compromise (BEC) attack. Believe it or not, BEC is actually costing organizations more money than ransomware.

There are several ways to block forwarding, Microsoft offers a setting linked to outbound spam policies, I prefer a Mail Flow (formerly known as Transport) rule. Go to admin.exchange.microsoft.com (EAC), under Mail flow, click on Rules. Click the + sign to create a new rule, give it a descriptive name and in the drop down list for Apply this rule if.., select the recipient is located Outside the organization. Then click the add condition button, select The message properties. – include the message type – Auto-forward and under Do the following select Reject the message with the explanation and enter a text for your users to understand why you've blocked their auto forwarded messages. Make sure the mode is Enforce. Be prepared for some backlash as there might be legitimate uses for email forwarding which you have now broken but work with the business to ensure they understand it's for a very good reason.


new rule

*Apply this rule if...

✖ The recipient is located... ▾ Outside the organization

and

✖ The message type is... ▾ Automatic reply

*Do the following...

Reject the message with the explanation... ▾ 'This message has been blocked due to organizational policy'

Except if...

Properties of this rule:

☑ Audit this rule with severity level:

Not specified ▾

Choose a mode for this rule:

● Enforce

○ Test with Policy Tips

○ Test without Policy Tips

Block auto forwarding of emails tenant wide

BLOCK SIGN-IN FOR SHARED MAILBOX

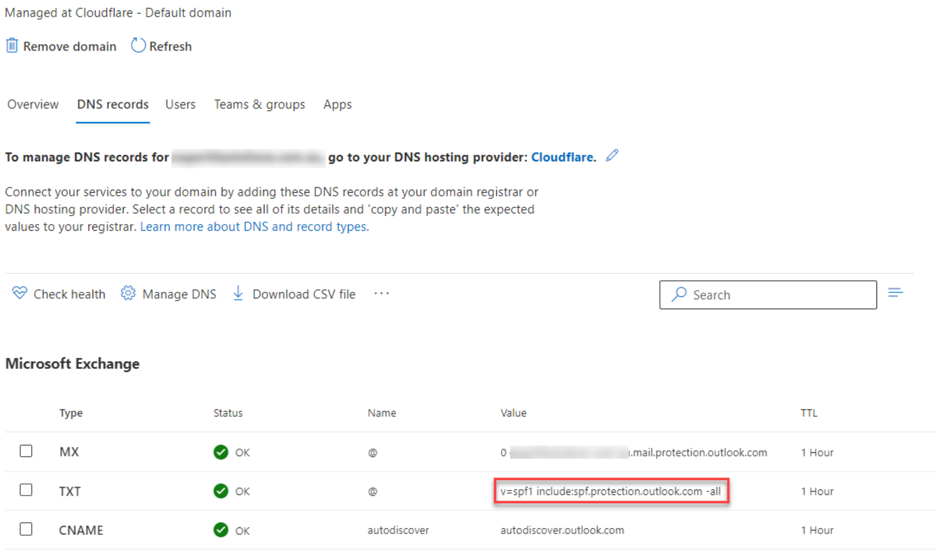
Most organizations use shared mailboxes, perhaps for aliases such as “support” or “sales” – especially since these types of mailboxes don’t consume an Exchange Online license. You then delegate permissions to a mailbox to staff that should have access to it, and they open it as a separate mailbox in Outlook. If you create a shared mailbox directly from EAC there’s no user account related to it, but if you converted an existing user mailbox to a shared mailbox – go back to the user account and block logins for it. There’s no reason to allow that user account to sign-in to Azure AD, staff can still access the shared mailbox, without knowing the password of the account.

SPF, DKIM AND DMARC

There are three main standards in use today in the email world to manage spam, email authentication and security: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC). An in-depth look is beyond the scope of this book but suffice to say you really should configure all three to be a good corporate citizen.

SENDER POLICY FRAMEWORK

This one is the easiest, you can't set up an Office 365 email domain without configuring SPF records in DNS. To see your current values, look under Settings – Domains in the M365 admin center. Click your vanity domain (the onmicrosoft.com default domain automatically has the correct SPF records configured) and go to DNS records, the second one in the list of type XT is generally your SPF record. If you have subdomains, you'll need to add SPF records for them as well.



To manage DNS records for [redacted] **go to your DNS hosting provider: Cloudflare.**

Connect your services to your domain by adding these DNS records at your domain registrar or DNS hosting provider. Select a record to see all of its details and 'copy and paste' the expected values to your registrar. Learn more about DNS and record types.

Microsoft Exchange

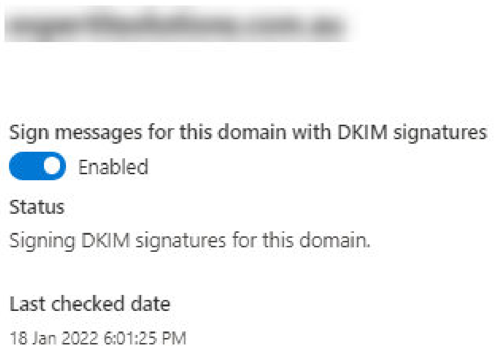
	Type	Status	Name	Value	TTL
□	MX	✓ OK	@	0 [redacted].mail.protection.outlook.com	1 Hour
□	TXT	✓ OK	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
□	CNAME	✓ OK	autodiscover	autodiscover.outlook.com	1 Hour

Sender Policy Framework DNS record in admin center

DOMAIN KEYS IDENTIFIED MAIL

Again, Microsoft manages keys for the onmicrosoft.com domain and will also create a private / public key pair and enable DKIM signing for your custom domain. However, if you have more than one custom domain, you're going to set up DMARC or you want more control you should configure this yourself.

Head back to the Defender 365 portal – Policies & Rules – Threat Policies and click on DKIM. In the list that appears, click on (one of) your vanity domains and turn DKIM on. You'll get an error that contains two CNAME DNS records that you need to enter where you host your DNS records. It can take some time (minutes to up to four days) but eventually you can click on DKIM and see that it's enabled.



[redacted]

Sign messages for this domain with DKIM signatures

● Enabled

Status

Signing DKIM signatures for this domain.

Last checked date

18 Jan 2022 6:01:25 PM

DKIM Configuration enabled

You test it by sending an email to a consumer email service for example and examining the header of the email.

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE

Before implementing DMARC you need know which IP addresses send messages from your domain, if it's just Exchange Online, or if you have other email servers (Exchange hybrid for instance). You also need to know whether the 5321.MailFrom and 5322.From domains matches for any third-party services that send email on your behalf. Unlike SPF and DKIM, there are three levels of DMARC settings: **none**, **quarantine** and **reject**. You start with **none** to identify legitimate and fraudulent messages sent from your domain and move on to **quarantine** once you're comfortable with your legitimate traffic being covered by SPF and DKIM. Finally **reject** tells any receiving mail server that if they get messages from your domain(s) that don't pass the DMARC checks (i.e., wasn't sent by you) they should reject them.

Create a TXT record at your DNS hoster that looks like this:

```
dmarc.domain  TTL  IN  TXT  "v=DMARC1; p=none;
pct=100"
```

Where domain is your email domain, and p can be set to none, quarantine and reject. You can also add a third-party provider to give you DMARC aggregated email reports, I'm hosting with Cloudflare and they have the service built in.

TROUBLESHOOTING HELP

If you've ever had to troubleshoot email issues you know that headers are your friend, including seeing DMARC, DKIM and SPF information. The free Message Header Analyzer shows all of this and more, go to the Home ribbon in Outlook and click on Get Add-ins and search for Message Header and install it. Pick an email and click MHA and it'll show you the headers and information for the selected email.

Email checklist >

Use the email checklist to protect this very common attack vector.

CHAPTER 3 - TEAMS

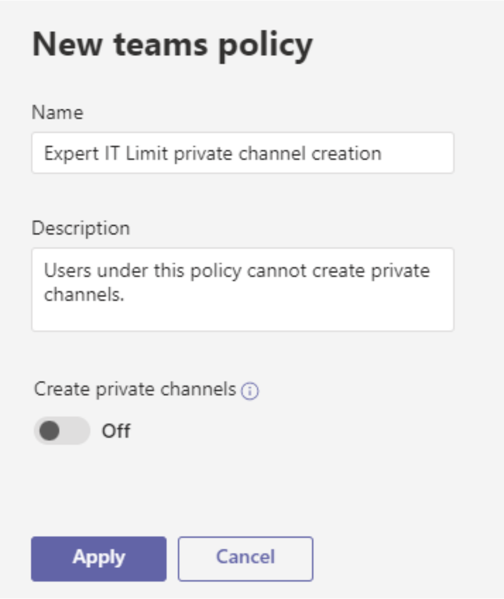
There are a few main themes around security for Teams, such as who can create Teams, who can create private Teams and Channels, sharing of files internally and externally and naming standards which can all be summed up by applying good governance. Depending on the size of your environment and the "looseness" of your current approach there might already be a mess for you to clean up.

One very important security feature that is not available in the M365 platform itself, is the backup of Teams data. 365 Total Backup, (available as either a standalone service or within the 365 Total Protection Enterprise Backup solution) offers a comprehensive SaaS service for backup and recovery of all Office 365 data, including Teams (user and group chats included!).

TEAMS AND CHANNEL CREATION PERMISSIONS

By default all users can create Teams (really create the underlying Microsoft 365 group). If you want to restrict to a set of users in a group, follow these instructions. Note that Global / Exchange / SharePoint / Teams and User Administrators can still create M365 groups irrespective of these settings.

A private channel in a Team is only visible to the people invited to it, so you could have a Team that spans your entire organization, with a channel that only users in the Sales department can see. If you want to limit who can create private channels (by default all Team members can, except Guests) use a Teams policy.



New teams policy

Name

Expert IT Limit private channel creation

Description

Users under this policy cannot create private channels.

Create private channels

Off

Teams policy to limit private channel creation

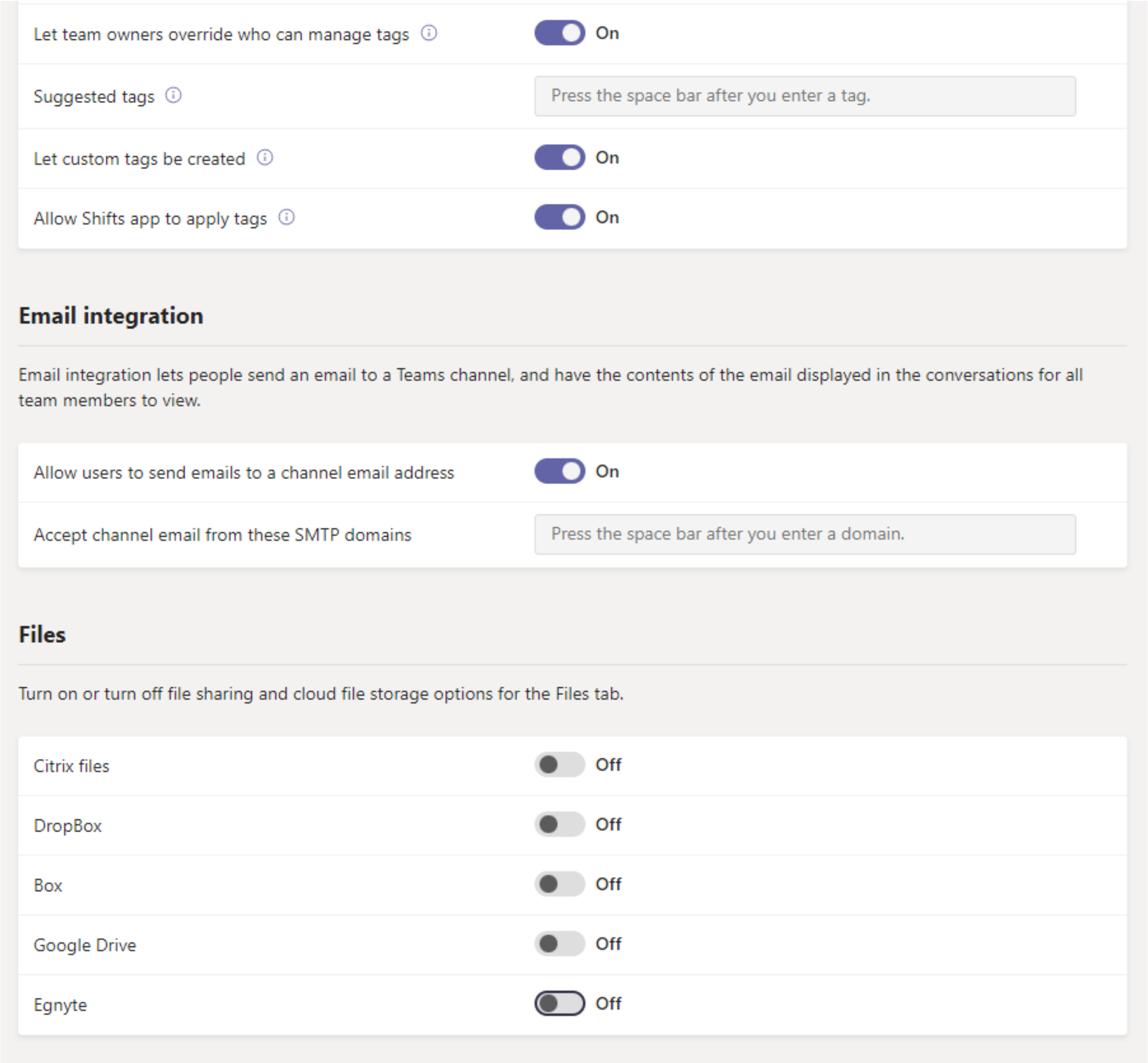
DELETE INACTIVE TEAMS

Whilst not a security risk per se, having unused Teams hanging around increases the mess of your environment and could expose you to potential data loss. Start by heading over to the Teams admin center – Analytics & reports – Usage reports and select Teams usage in the drop down for report type and say Last 90 days for date range. This will give you a list (that you can also export to csv for further analysis) and graph showing activity in each Team and when there last was activity.

If you have ones that clearly aren't being used, consider archiving them.

CONTROLLING FILE SHARING IN TEAMS

By default, Teams will use SharePoint to store files shared but you can use third-party cloud storage if you prefer. If, however, you want to ensure that company files are stored in SharePoint, consider disabling these other cloud storage locations. In the Teams admin center, go to Teams – Teams settings and scroll down to files and disable the ones you don't want.



Let team owners override who can manage tags ⓘ	On
Suggested tags ⓘ	Press the space bar after you enter a tag.
Let custom tags be created ⓘ	On
Allow Shifts app to apply tags ⓘ	On

Email integration

Email integration lets people send an email to a Teams channel, and have the contents of the email displayed in the conversations for all team members to view.

Allow users to send emails to a channel email address	On
Accept channel email from these SMTP domains	Press the space bar after you enter a domain.

Files

Turn on or turn off file sharing and cloud file storage options for the Files tab.

Citrix files	Off
DropBox	Off
Box	Off
Google Drive	Off
Egnyte	Off

Teams third-party file storage locations settings

EXTERNAL ACCESS

You should also make a choice about Teams interoperability with other systems – go to Users – External access and select if you allow your users to communicate in Teams with Skype for Business / Teams users in other tenants. You can select to allow all external domains, only specific ones, block specific ones (and therefore allow all others) or block all external domains. You can also control communications in and out of non-managed Teams (personal accounts) and Skype consumer users. Note that in all these situations there's no invitation of the external user into your Team(s), there's simply communication between them, for guest users – read on.

EXTERNAL USERS

The settings for who can be invited to be a member of a Team, called a guest, are organization wide (not specific to Teams), although you can control access to individual teams with sensitivity labels. By default, guest have quite a lot of freedom once they've received their invitation email and accepted it. Note that a guest can either be in another Azure AD tenant or a user in a consumer identity system (Google, Facebook). Most importantly, unless you've changed it, a guest can invite other guests to a Team (or SharePoint site etc.).

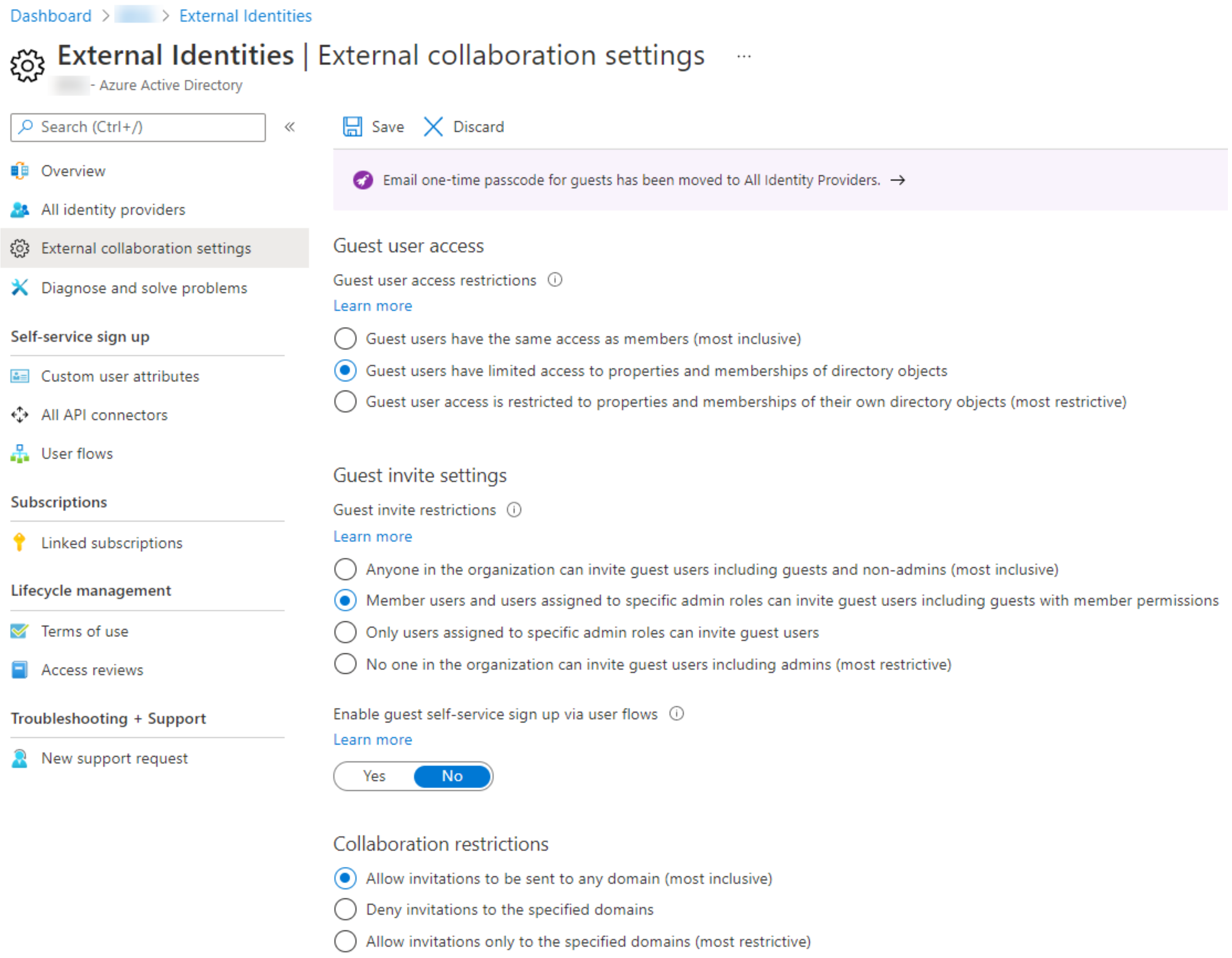
Head over to the Azure AD admin center, go to Azure Active Directory – External identities – External collaboration settings.

The first setting controls what permissions an invited Guest user has to user properties and group memberships of others in the directory, either the same as internal users, limited access or only having access to their own properties.

The second setting manages who can invite guests, either everyone (including guests), internal users in the tenant, only administrators or no one.

Thirdly you can control access to self-service sign up to applications in your directory via user flows and the final setting controls which domains invitations can be sent to, any domain, specific domains are denied, or only selected domains are allowed.

These four settings control a lot of collaboration and security in your tenant, across applications such as Exchange Online, Teams, SharePoint, and others but there's no hard and fast rule for how to set them. You should NOT just accept the defaults and instead work through with the business what the best balance is for your organization. Here are the settings for one of my clients:



Dashboard > [redacted] > External Identities

External Identities | External collaboration settings ...

[redacted] - Azure Active Directory

Email one-time passcode for guests has been moved to All Identity Providers. →

Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)

● Guest users have limited access to properties and memberships of directory objects

○ Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

○ Anyone in the organization can invite guest users including guests and non-admins (most inclusive)

● Member users and users assigned to specific admin roles can invite guest users including guests with member permissions

○ Only users assigned to specific admin roles can invite guest users

○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

Yes [✓ No]

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)

○ Deny invitations to the specified domains

○ Allow invitations only to the specified domains (most restrictive)

Azure AD external identity settings for guest

You should also configure the Teams specific Guest access settings, back in the Teams admin center, click Users – Guest access and go through the settings for calling, meetings and messaging for Teams users invited to your tenant.

If you invite external users to meetings using Teams, make sure you customize this branding, just like we did for Azure AD and for the same reason, instill trust that this is indeed a legitimate invitation. They're under Meetings - Meeting settings – Email invitation.

Teams checklist >

Use the Teams checklist to ensure you've applied good governance.

CHAPTER 4 – SHAREPOINT

The most important setting to control potential data leaks (apart from Data Loss Prevention, DLP itself, see Chapter 7) is the sharing setting controlling external sharing of files in SharePoint and OneDrive for Business, and by extension, Teams.

We've come to take external file sharing for granted. It's one of those features which users utilize day in and day out without much thought of the underlying implications. Many users won't think twice about configuring a file share with everyone allowed and just leaving it out there in perpetuity. It's not an if, but WHEN situation we're talking about here in terms of security issues and data leakage. By tightly controlling the sharing settings and permissions for data stored in M365, you'll be better prepared to prevent un-intended security issues as a result.

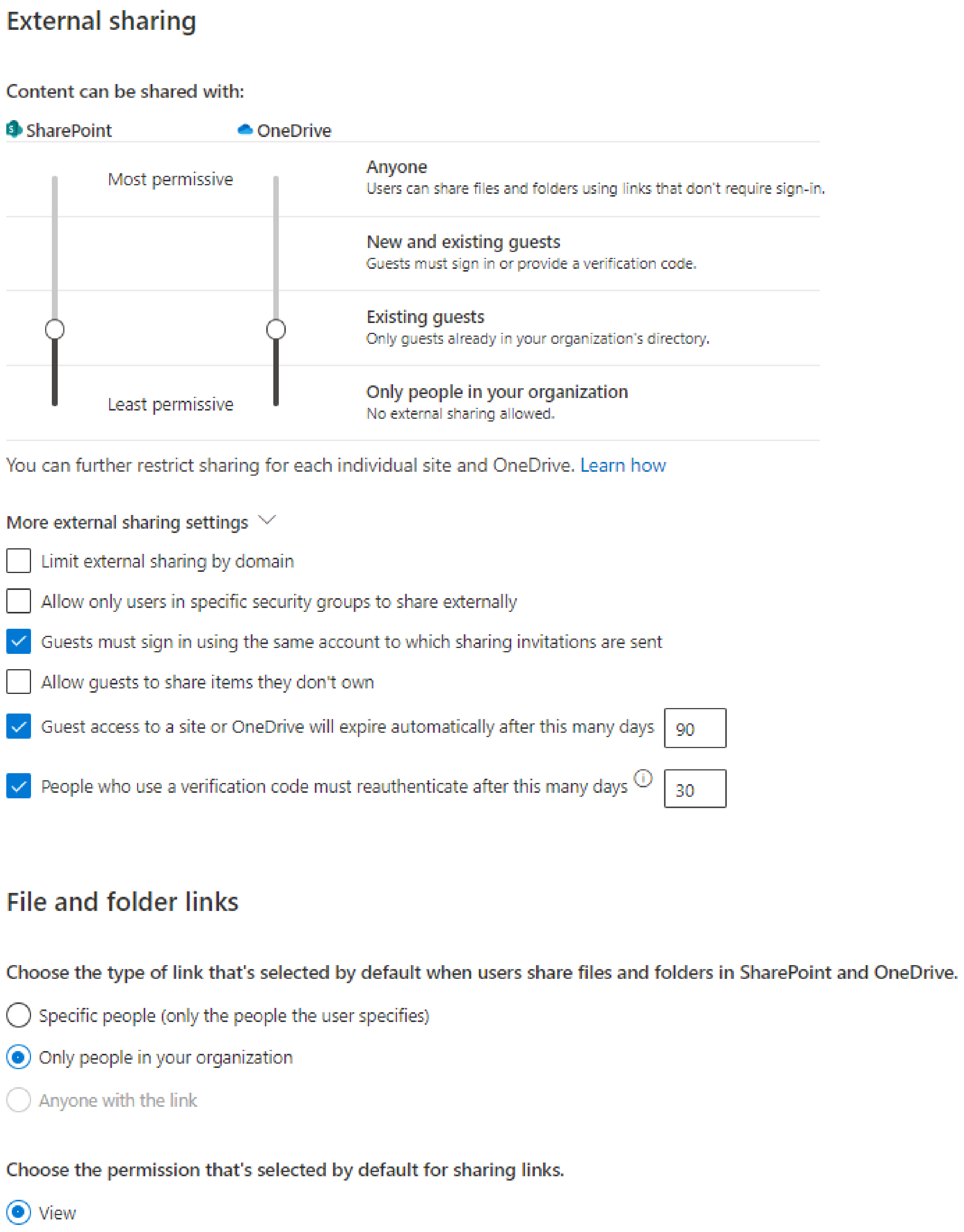
In this chapter, we'll look at how to handle sharing controls and mitigate potential data leaks.

EXTERNAL SHARING

Go to the SharePoint admin center and go to Policies – Sharing. Here you can move the slider for SharePoint and OneDrive for Business from sharing with anyone with no sign in required, new and existing guests (in other words, the act of sharing a file invites a guest into the tenant), existing guests (meaning, you can only share with guest who have already been invited by some other process) or no external sharing allowed at all. Apart from the obvious to not allow anonymous links, picking from the other three will require another round of interacting with the business. For most organizations, simply turning off external sharing probably isn't possible in today's world of teams made up of people from different businesses. I favor only allowing existing guests and having a process around the invitation of external users, but in smaller businesses New and Existing guests is OK. Note that the OneDrive settings can't be less restrictive than the SharePoint option.

Under More external sharing settings hides the ability to limit sharing to certain domains, allowing selected security groups to be able to share externally, forcing guests to use the same account as to where the invitation was sent, blocking guests from sharing items they don't own, expiring access after a set time, and forcing guests to reauthenticate after X number of days. You can also set the type of link that's suggested when a user shares a file (specific people or only internal users) and if the default is a View or an Edit link, if you set it to View, a user must decide to change it to an Edit sharing link.

Here are my recommended settings for each of these:



External sharing

Content can be shared with:

SharePoint		OneDrive	
	Most permissive		**Anyone** Users can share files and folders using links that don't require sign-in.
			New and existing guests Guests must sign in or provide a verification code.
○		○	**Existing guests** Only guests already in your organization's directory.
	Least permissive		**Only people in your organization** No external sharing allowed.

You can further restrict sharing for each individual site and OneDrive. Learn how

More external sharing settings

- □ Limit external sharing by domain
- □ Allow only users in specific security groups to share externally
- ☑ Guests must sign in using the same account to which sharing invitations are sent
- □ Allow guests to share items they don't own
- ☑ Guest access to a site or OneDrive will expire automatically after this many days 90
- ☑ People who use a verification code must reauthenticate after this many days ⓘ 30

File and folder links

Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.

- ○ Specific people (only the people the user specifies)
- ● Only people in your organization
- ○ Anyone with the link

Choose the permission that's selected by default for sharing links.

- ● View

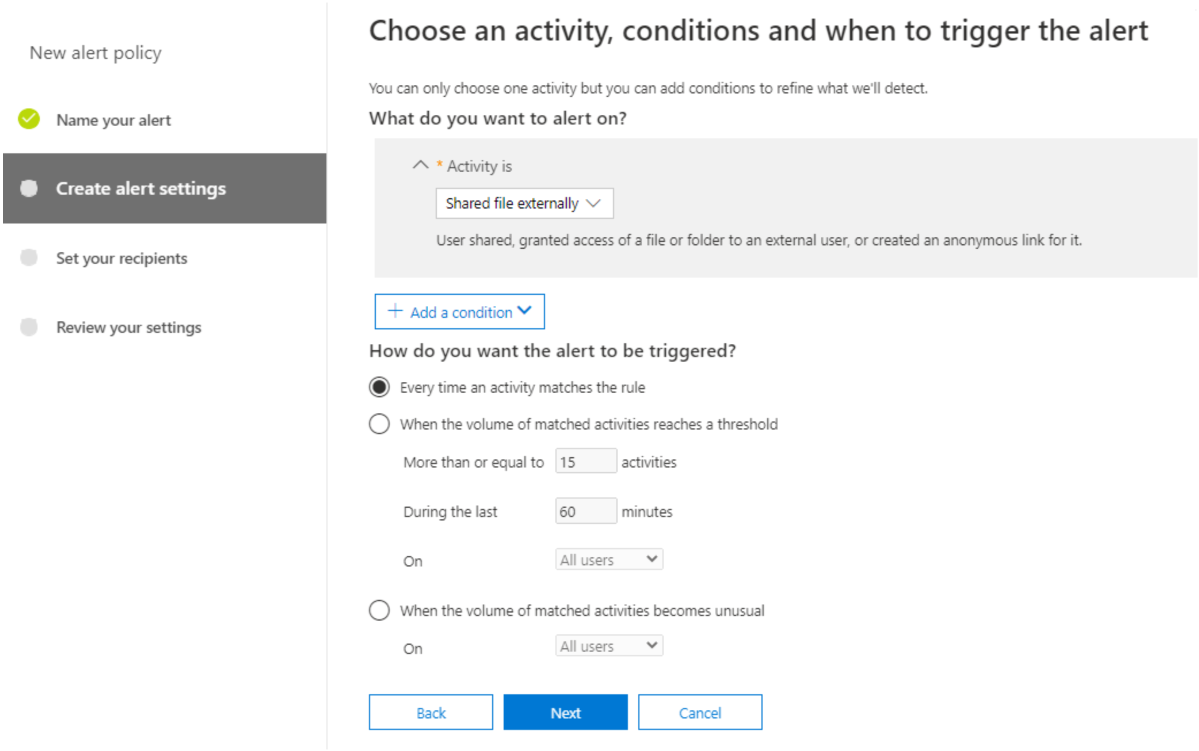
External file sharing settings for SharePoint and OneDrive for Business

There's another place where you can control a subset of these settings, the main Microsoft 365 Admin center, under Settings – Org settings – Security and Privacy. Click Sharing which lets you stop ordinary users inviting guests (see Teams above) and if you click the link called "change the external sharing settings for SharePoint" you can control the SharePoint part of file sharing. While you're here, configure your organization's privacy profile URL and a contact email.

Back in the SharePoint admin center, click on Access control under Policies. Unmanaged devices are a tenant wide restriction on the kind of devices that can access SharePoint and OneDrive, if you want more granular control over this, use a Conditional Access policy. Network location limits access to specific public IP addresses (only works if everyone is always working from the office), you can block access from older clients and you can limit who can use OneDrive for Business based on security group membership.

ALERTS TO NOTIFY YOU OF EXTERNAL FILE SHARING

Back in Chapter 2 we looked at Alert policies, there's one you might want to configure for SharePoint external file sharing. Go to security.microsoft.com - Email & collaboration – Policies & rules – Alert policy – New alert policy. Give it a name and description, select severity Low and Information governance as category, pick Shared file externally as activity and if you need to scope it down, click Add a condition and limit it to specific users, files, extension, or site collection URLs. If there's a lot of file sharing you can limit it based on the number of files shared over a specific time period.



Choose an activity, conditions and when to trigger the alert

You can only choose one activity but you can add conditions to refine what we'll detect.

What do you want to alert on?

* Activity is: Shared file externally

User shared, granted access of a file or folder to an external user, or created an anonymous link for it.

How do you want the alert to be triggered?

● Every time an activity matches the rule

○ When the volume of matched activities reaches a threshold

More than or equal to 15 activities

During the last 60 minutes

On: All users

○ When the volume of matched activities becomes unusual

On: All users

Alert policy for SharePoint and OneDrive external file sharing

SharePoint checklist >

Use the SharePoint checklist to control potential data leaks.

CHAPTER 5 - APPLICATIONS

The challenge around insecure applications in general is a big one – the first rule is to patch, patch and patch. Most IT Pros are onboard with monthly updates from Microsoft for Windows and Office but there are a lot more applications than that on most desktops. If you have E5 licensing / Business Premium, Defender for Endpoint offers full Threat and Vulnerability (TVM) management for Windows, MacOS with Linux coming (see Chapter 9 & 10).

If that's not an option, consider a third-party tool (or see Chapter 6 if you're using Endpoint Manager to deploy software) to keep track of what applications are installed on your desktops and which ones need to be updated.

In this chapter we'll focus on OAuth applications and how you should manage the workflow around these.

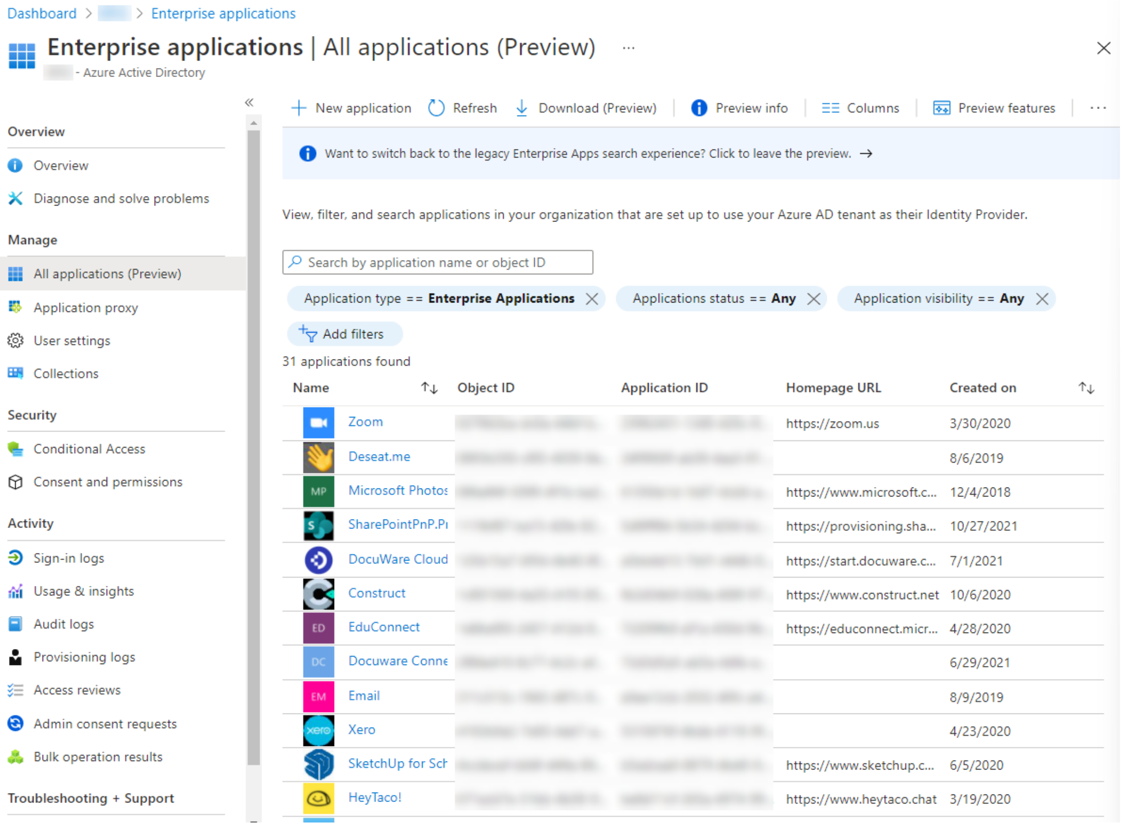
OAUTH APPS

There are add-ins for the Office applications, including Teams that rely on being registered with Azure AD using an OAuth flow. We covered this in-depth in an article and webinar, but the bottom line is that initially Microsoft didn't have a lot of guardrails around these apps and any user could grant any permissions to their own data, if the application asked for it. This was used in several successful attacks where a user is tricked into granting permissions to their mailbox and user profile by a legitimate looking application, which actually is malicious.

Once granted, the attackers have access to everything they were given permissions to, whether MFA or password resets are enacted.

In the last year or so, Microsoft has tightened this up a bit, so apps where the publisher hasn't been verified can only ask for very limited permissions and there are options for you to check existing apps and their access, as well as limit future app requests with administrator workflows. Again, if you have E5 licensing, and thus access to Defender for Cloud Apps, you have more powerful and easier to use options, here we'll focus on the options in Azure AD.

Go to the [AAD admin center]() and click on Azure AD – Enterprise applications. Start with All applications and you'll see a list of apps that are using your AAD tenant as their Identity Provider.



Want to switch back to the legacy Enterprise Apps search experience? Click to leave the preview. →

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Search by application name or object ID

Application type == **Enterprise Applications**

Applications status == **Any**

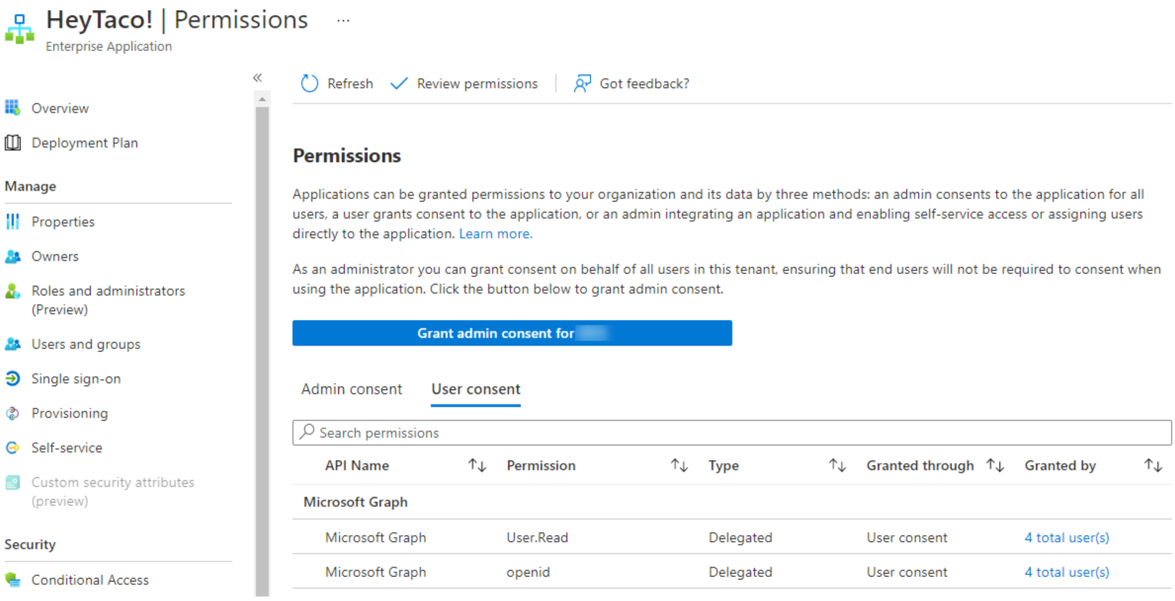
Application visibility == **Any**

31 applications found

Name	Object ID	Application ID	Homepage URL	Created on
Zoom	[redacted]	[redacted]	https://zoom.us	3/30/2020
Deseat.me	[redacted]	[redacted]		8/6/2019
Microsoft Photos	[redacted]	[redacted]	https://www.microsoft.c...	12/4/2018
SharePointPnP.Pı	[redacted]	[redacted]	https://provisioning.sha...	10/27/2021
DocuWare Cloud	[redacted]	[redacted]	https://start.docuware.c...	7/1/2021
Construct	[redacted]	[redacted]	https://www.construct.net	10/6/2020
EduConnect	[redacted]	[redacted]	https://educonnect.micr...	4/28/2020
Docuware Conne	[redacted]	[redacted]		6/29/2021
Email	[redacted]	[redacted]		8/9/2019
Xero	[redacted]	[redacted]		4/23/2020
SketchUp for Sch	[redacted]	[redacted]	https://www.sketchup.c...	6/5/2020
HeyTaco!	[redacted]	[redacted]	https://www.heytaco.chat	3/19/2020

Azure AD Enterprise Applications list

Let's say that one of these looks sketchy, click on it, and start by checking the Sign-in logs to see how popular it is amongst your users. Then click on Permissions, here you'll see if it's been granted only User consent and how many users have done so (and if you click on the number of users blue link it'll tell you who they are), or if it's been granted Admin consent by an administrator to your whole tenant.



Permissions

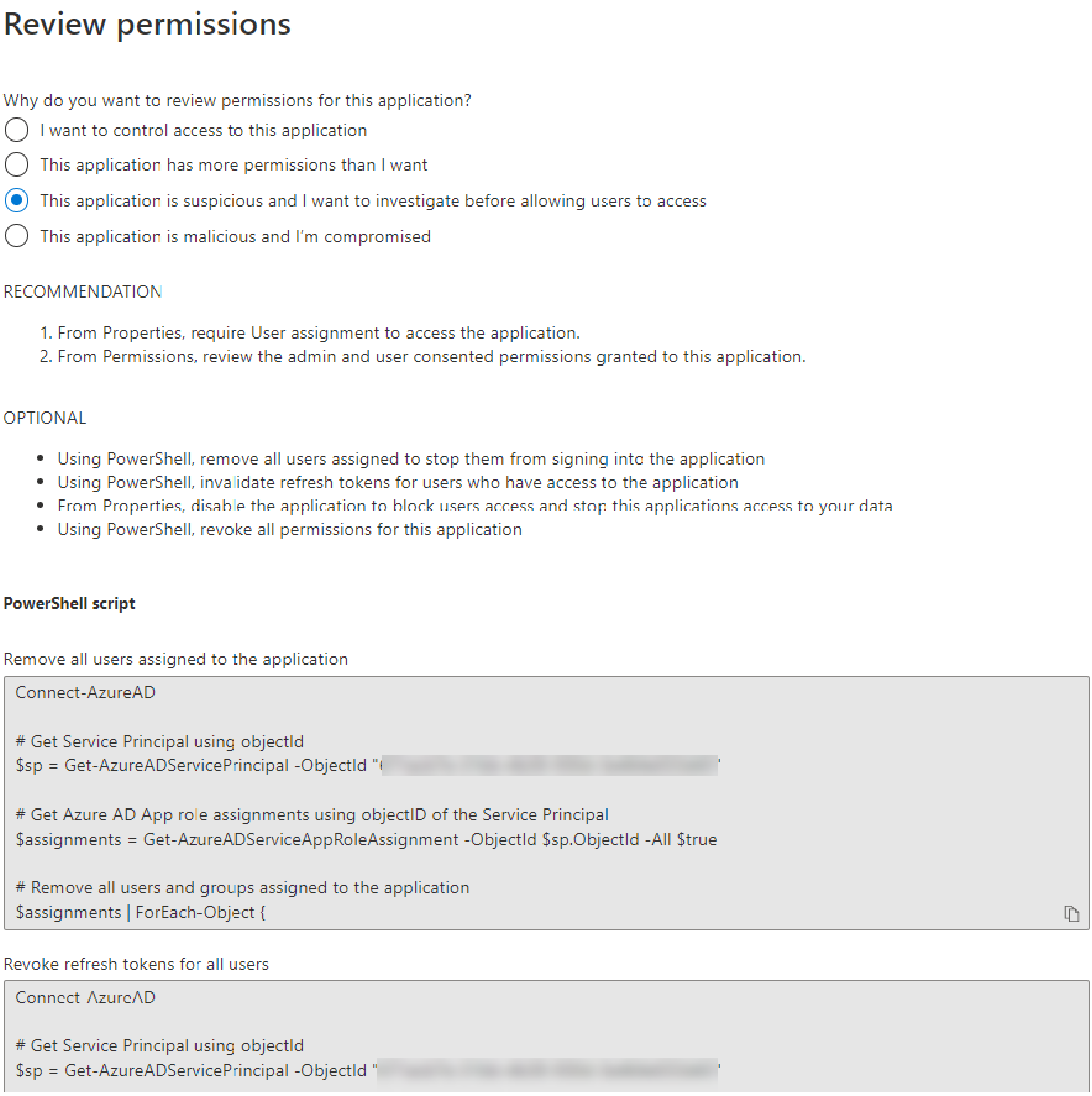
Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. Learn more.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

API Name ↑↓	Permission ↑↓	Type ↑↓	Granted through ↑↓	Granted by ↑↓
Microsoft Graph				
Microsoft Graph	User.Read	Delegated	User consent	4 total user(s)
Microsoft Graph	openid	Delegated	User consent	4 total user(s)

Azure AD checking existing permissions for suspicious application

If your investigation leads you to suspect that something is potentially malicious, click on Review permissions where you're given four options based on your level of concern, picking one will give you recommendations of steps to take and PowerShell scripts to run.



Review permissions

Why do you want to review permissions for this application?

○ I want to control access to this application

○ This application has more permissions than I want

● This application is suspicious and I want to investigate before allowing users to access

○ This application is malicious and I'm compromised

RECOMMENDATION

1. From Properties, require User assignment to access the application.
2. From Permissions, review the admin and user consented permissions granted to this application.

OPTIONAL

- Using PowerShell, remove all users assigned to stop them from signing into the application
- Using PowerShell, invalidate refresh tokens for users who have access to the application
- From Properties, disable the application to block users access and stop this applications access to your data
- Using PowerShell, revoke all permissions for this application

PowerShell script

Remove all users assigned to the application

```
Connect-AzureAD

# Get Service Principal using objectId
$sp = Get-AzureADServicePrincipal -ObjectId "[redacted]"

# Get Azure AD App role assignments using objectID of the Service Principal
$assignments = Get-AzureADServiceAppRoleAssignment -ObjectId $sp.ObjectId -All $true

# Remove all users and groups assigned to the application
$assignments | ForEach-Object {
```

Revoke refresh tokens for all users

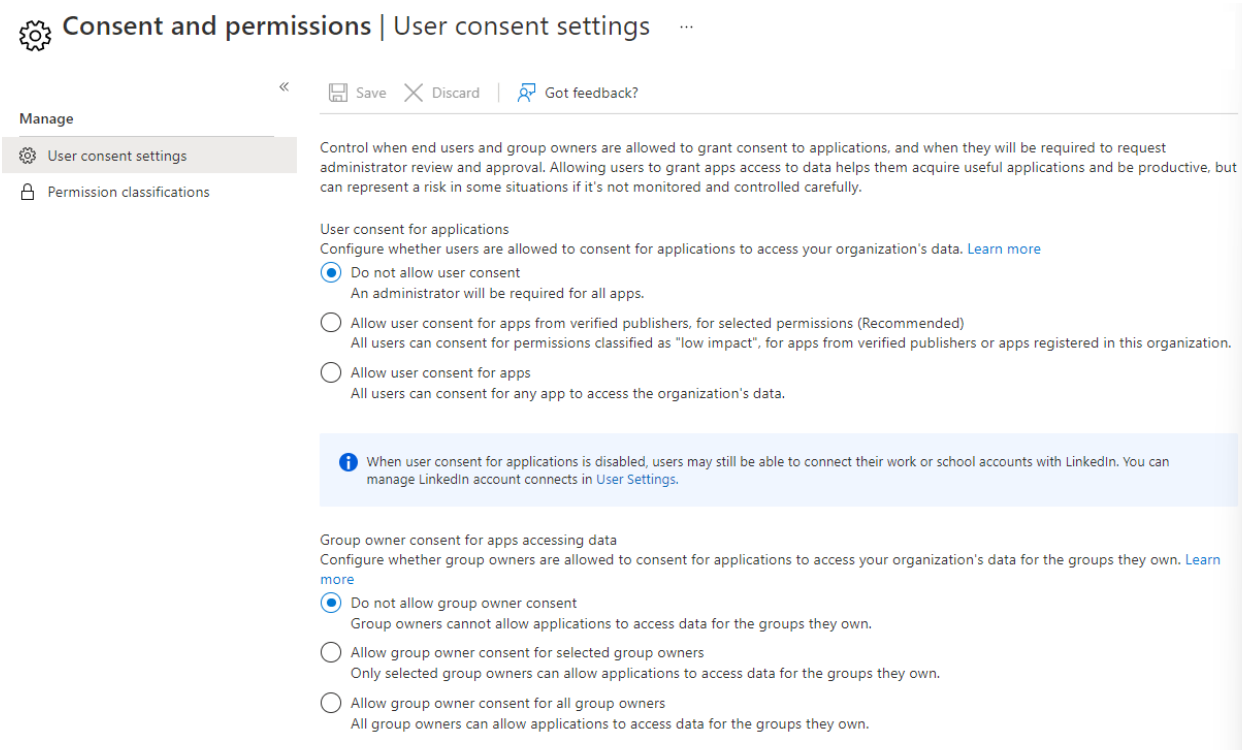
```
Connect-AzureAD

# Get Service Principal using objectId
$sp = Get-AzureADServicePrincipal -ObjectId "[redacted]"
```

Azure AD steps to take for suspicious application

To put more control in place for future application requests, go back to Enterprise applications and select Consent and permissions. Start with Permission classifications, here you can take Microsoft's suggested list of limited permissions that users can grant applications without compromising your business. You can also click, No, I'll add permissions and work through all the available APIs to customize a list of low security impact permissions that you can let your users grant by themselves. For most SMBs I'd suggest taking Microsoft's recommendation, or not allow users to install apps at all (see below).

Under User consent settings you can stop users installing apps by themselves altogether (be careful with the productivity implications), only allow them to consent to apps that come from verified publishers and only for the low impact permissions defined above or allow users to consent for any app (not recommended). Similar settings are available for group owners to grant access to apps (read Teams apps).

Here are the settings for one of my clients:



Consent and permissions | User consent settings ...
«
Save
Discard
Got feedback?
Manage
User consent settings
Permission classifications

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

● Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

When user consent for applications is disabled, users may still be able to connect their work or school accounts with LinkedIn. You can manage LinkedIn account connects in User Settings.

Group owner consent for apps accessing data
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

● Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

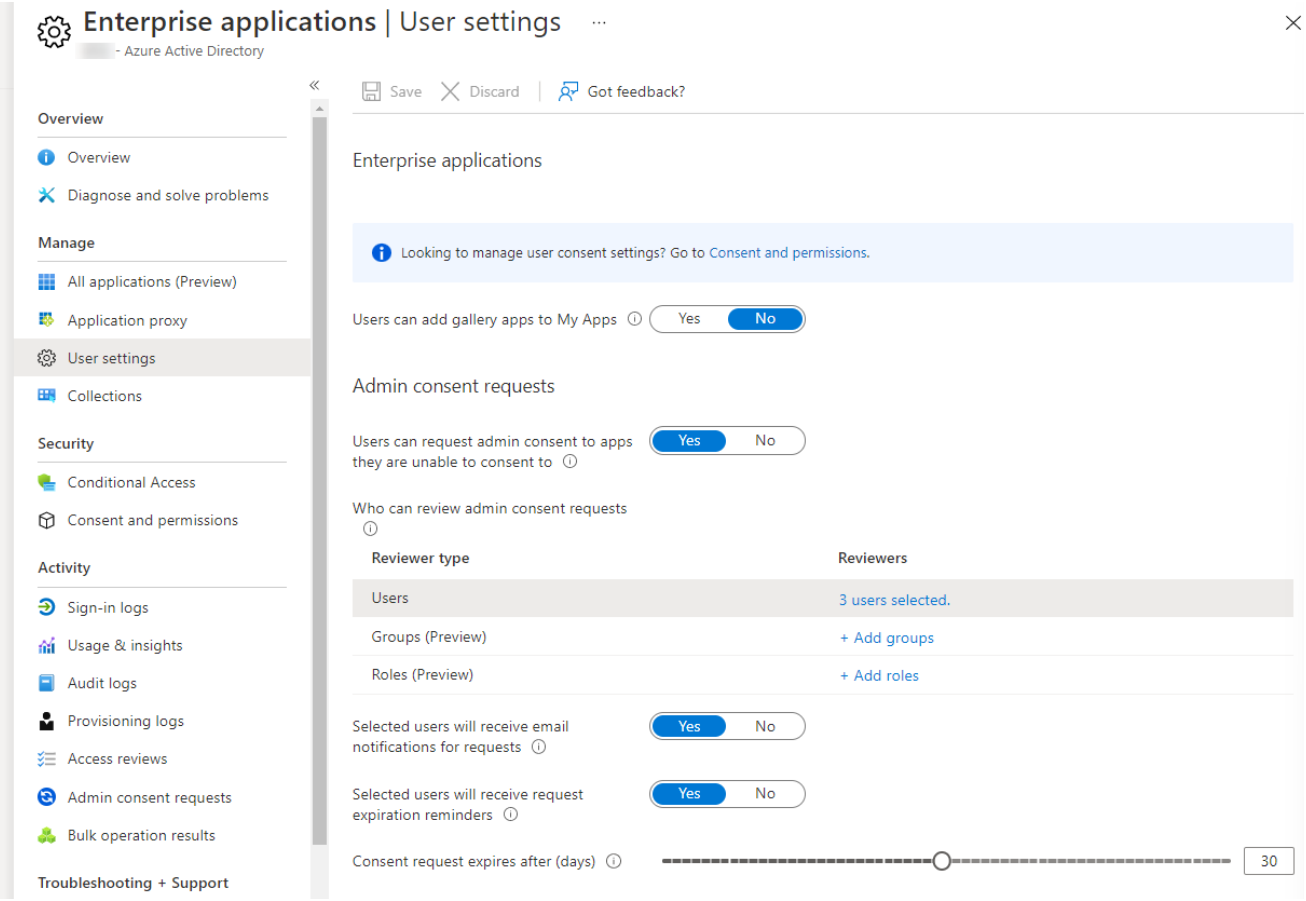
○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

Azure AD OAuth apps consent and permission settings

If you leave your settings like that, you also need to designate administrators that can approve user's grant requests, head back to Enterprise applications and go to User settings. Turn on "Users can request admin consent" and designate a security group or select users who will receive an email when a user tries to install an app and on the grant permissions screen request that an administrator review and allow the app.

Note that this request workflow also applies if you're allowing users to install low impact apps themselves, but an application is requesting more permissions than that.



Enterprise applications

Looking to manage user consent settings? Go to Consent and permissions.

Users can add gallery apps to My Apps: Yes [✓ No]

Admin consent requests

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

Who can review admin consent requests

Reviewer type	Reviewers
Users	3 users selected.
Groups (Preview)	+ Add groups
Roles (Preview)	+ Add roles

Selected users will receive email notifications for requests: [✓ Yes] No

Selected users will receive request expiration reminders: [✓ Yes] No

Consent request expires after (days): 30

Azure AD Enterprise applications Admin consent flow settings

Applications checklist >

Use the applications checklist to manage the workflow of OAuth applications.

CHAPTER 6 - ENDPOINT MANAGER

Once upon a time we could manage all (Windows) devices on a corporate network using Active Directory, Group Policy and maybe Configuration Manager. Today you must handle personal smartphones, organization issued smartphones (iOS and Android), along with MacOS, Windows and maybe even Linux PCs.

And those devices are seldom in the office, more likely they're in someone's home, making traditional tools next to useless. You need a better approach, using a cloud based Mobile Device Management (MDM) and Mobile Application Management (MAM) tool, such as Endpoint Manager / Intune.

In this chapter we'll cover a couple of basic settings in Microsoft Endpoint Manager (MEM), which will barely scratch the surface of what it's capable off, particularly outside of directly security related features.

STANDARDIZE

If you're an MSP it's a good idea to have the same set of device groups across all tenants. Some   suggestions are Company devices, Personal Devices, Phones but you'll need to customize this to suit your needs. If it's your own business, it's still a good idea to set up some groups with devices as nearly everything in MEM is managed through device groups.

One decision is around joined, hybrid-joined and registered devices in AAD. MacOS/iOS and Android are always registered, they can't be joined whereas

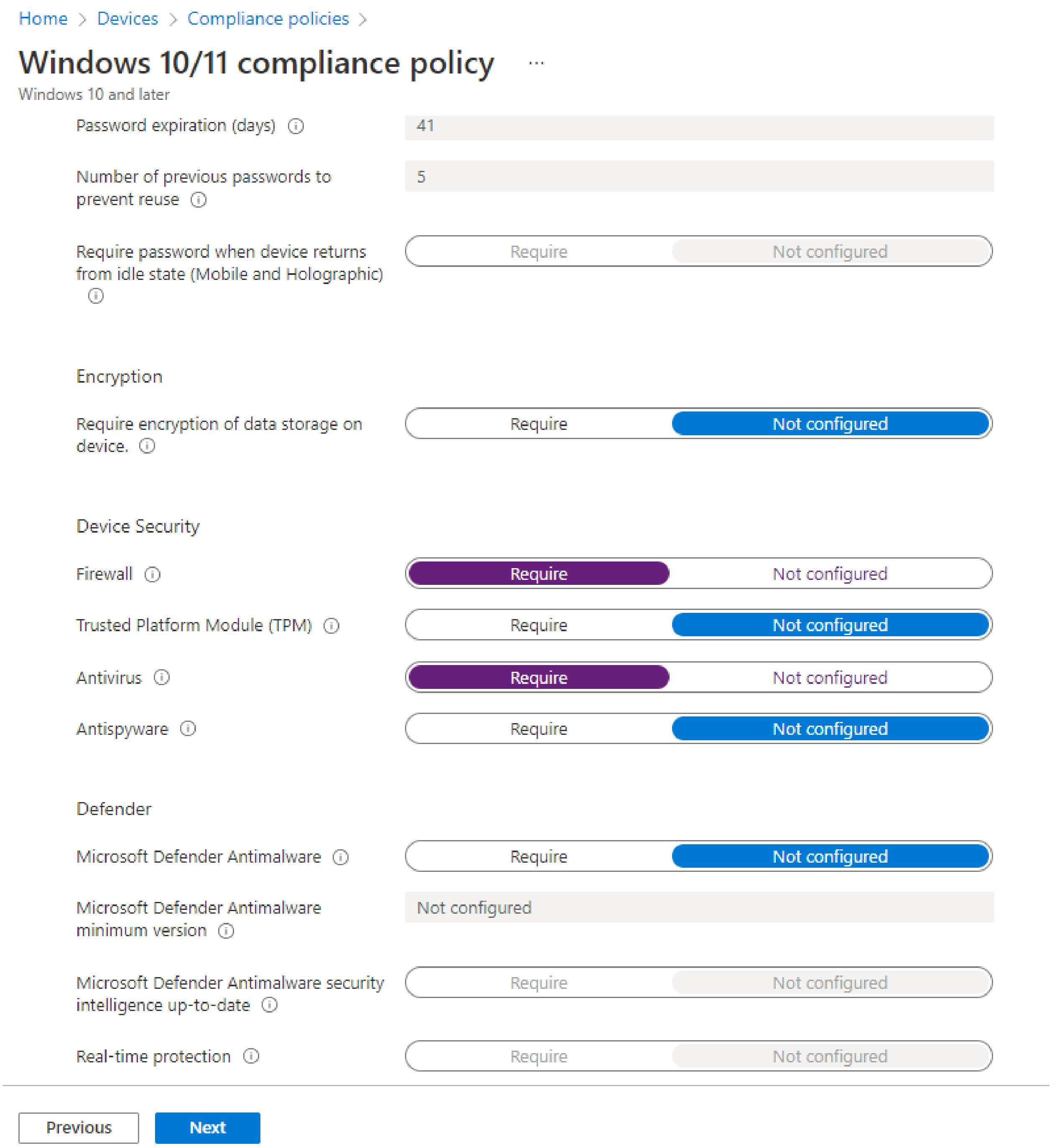
Windows devices (apart from Windows 10 Home) can be all three. Registered is generally a personal device that AAD knows about and is tied to a user account and mainly used to manage corporate data on it, without actually touching anything else. A joined device is part of AAD, and this gives you single sign on to apps in the cloud, SSPR from the lock screen and access can be controlled through Conditional Access. Finally, a hybrid-joined device is also joined to Active Directory on-premises, on top of being joined to AAD.

Another decision is around enrollment, all the device types already mentioned can be enrolled in MEM which lets you apply policies and easily deploy applications to them. However, for personal devices, particularly smartphones, this can be seen as too invasive and just managing access to corporate data through applications using MAM might have to suffice.

A full decision tree for these options is beyond the scope of this book but it's important that you define a policy for your business as to what devices (of any type) can access business resources and how that access should be controlled.

POLICIES

MEM comes with many different policy types, here we'll look at a couple of sample ones. Go to the MEM admin center, click on Devices – Compliance policies and pick Windows 10 and later as the platform. Give your policy a descriptive name and under Compliance settings, explore the options you have. You can require that devices are protected with Bitlocker, Secure Boot, that the firewall/antivirus/antispyware is on, a minimum OS version plus many others.



Home > Devices > Compliance policies >

Windows 10/11 compliance policy ···

Windows 10 and later

Password expiration (days) ⓘ: 41

Number of previous passwords to prevent reuse ⓘ: 5

Require password when device returns from idle state (Mobile and Holographic) ⓘ: Require | Not configured

Encryption

Require encryption of data storage on device. ⓘ: Require [✓ Not configured]

Device Security

Firewall ⓘ: [✓ Require] Not configured

Trusted Platform Module (TPM) ⓘ: Require [✓ Not configured]

Antivirus ⓘ: [✓ Require] Not configured

Antispyware ⓘ: Require [✓ Not configured]

Defender

Microsoft Defender Antimalware ⓘ: Require [✓ Not configured]

Microsoft Defender Antimalware minimum version ⓘ: Not configured

Microsoft Defender Antimalware security intelligence up-to-date ⓘ: Require | Not configured

Real-time protection ⓘ: Require | Not configured

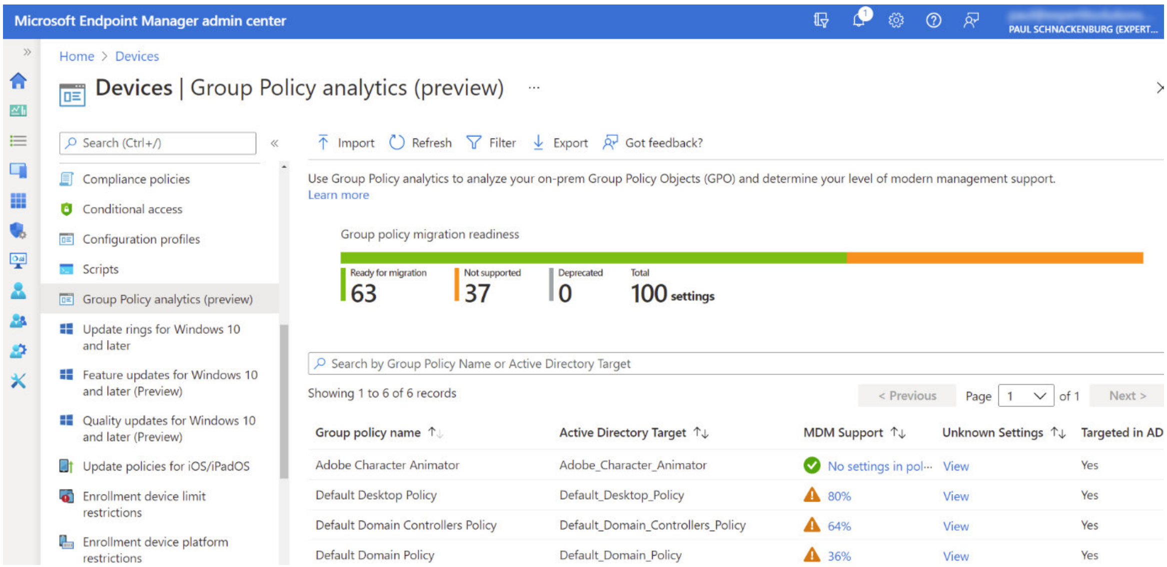
Configuring a Windows 10 Compliance policy in MEM

Under actions for noncompliance, pick what actions should be taken if a device isn't compliant with your settings, and then under Assignments, link the policy to a device group. Be patient, evaluation in MEM can take hours (or even days).

The beauty is that you can now use Conditional Access and control access to applications based on if the device that's connecting is compliant with your policies.

Another option is Configuration profiles that can be applied to various types of Android management types, iOS/iPadOS, MacOS and Windows. In Devices – Configuration profiles, click +Create profile, select Windows 10 and later – Templates to see all the available options. There are many options such as Email to auto configure email settings, Endpoint protection for Bitlocker and several other security controls, VPN and Wi-Fi settings etc.

There are many variables here but if you're familiar with using Group Policy to manage endpoints, migrating to MDM policies should be straightforward. There's even an option to pick Administrative templates as a Configuration policy template which gives you access to a set of computer and user administrative policies GPO settings to use. And if you have complex GPOs that you want to bring into Intune, go down to Group Policy analytics (preview) under Devices. Here you can import backed up GPOs from your on-premises AD environment and it'll analyze each setting to show you which ones can be directly migrated to MDM settings, which ones aren't available in MDM etc.



Microsoft Endpoint Manager admin center

PAUL SCHNACKENBURG (EXPERT...

Home > Devices

Devices | Group Policy analytics (preview) ...

Search (Ctrl+/)

- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Group Policy analytics (preview)
- Update rings for Windows 10 and later
- Feature updates for Windows 10 and later (Preview)
- Quality updates for Windows 10 and later (Preview)
- Update policies for iOS/iPadOS
- Enrollment device limit restrictions
- Enrollment device platform restrictions

Use Group Policy analytics to analyze your on-prem Group Policy Objects (GPO) and determine your level of modern management support.
Learn more

Group policy migration readiness

Ready for migration	Not supported	Deprecated	Total
63	37	0	100 settings

Search by Group Policy Name or Active Directory Target

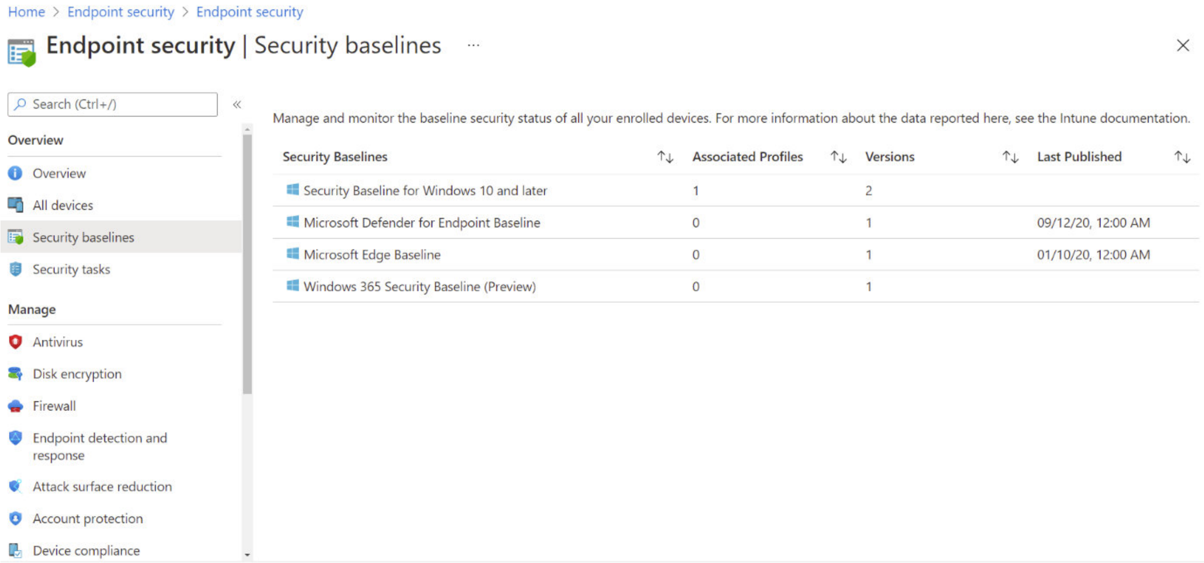
Showing 1 to 6 of 6 records

< Previous Page 1 of 1 Next >

Group policy name	Active Directory Target	MDM Support	Unknown Settings	Targeted in AD
Adobe Character Animator	Adobe_Character_Animator	✓ No settings in pol···	View	Yes
Default Desktop Policy	Default_Desktop_Policy	⚠ 80%	View	Yes
Default Domain Controllers Policy	Default_Domain_Controllers_Policy	⚠ 64%	View	Yes
Default Domain Policy	Default_Domain_Policy	⚠ 36%	View	Yes

Endpoint Manager Group Policy Analytics

There are many permutations of different policies in Intune that you can use to improve your device security, Microsoft has a few guided scenarios to get you started and don't miss the new Endpoint security blade in MEM which gathers all endpoint security settings in one place. This is also where you'll find the Security Baselines that Microsoft recommends, I recommend investigating each of these.



Home > Endpoint security > Endpoint security

Endpoint security | Security baselines ...

Search (Ctrl+/)

Overview

- Overview
- All devices
- Security baselines
- Security tasks

Manage

- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance

Manage and monitor the baseline security status of all your enrolled devices. For more information about the data reported here, see the Intune documentation.

Security Baselines	Associated Profiles	Versions	Last Published
Security Baseline for Windows 10 and later	1	2	
Microsoft Defender for Endpoint Baseline	0	1	09/12/20, 12:00 AM
Microsoft Edge Baseline	0	1	01/10/20, 12:00 AM
Windows 365 Security Baseline (Preview)	0	1	

Endpoint Manager Security Baselines

Endpoint Manager checklist >

Use the Endpoint Manager checklist to help manage the security of all (Windows) devices on a corporate network.

CHAPTER 7 - INFORMATION PROTECTION

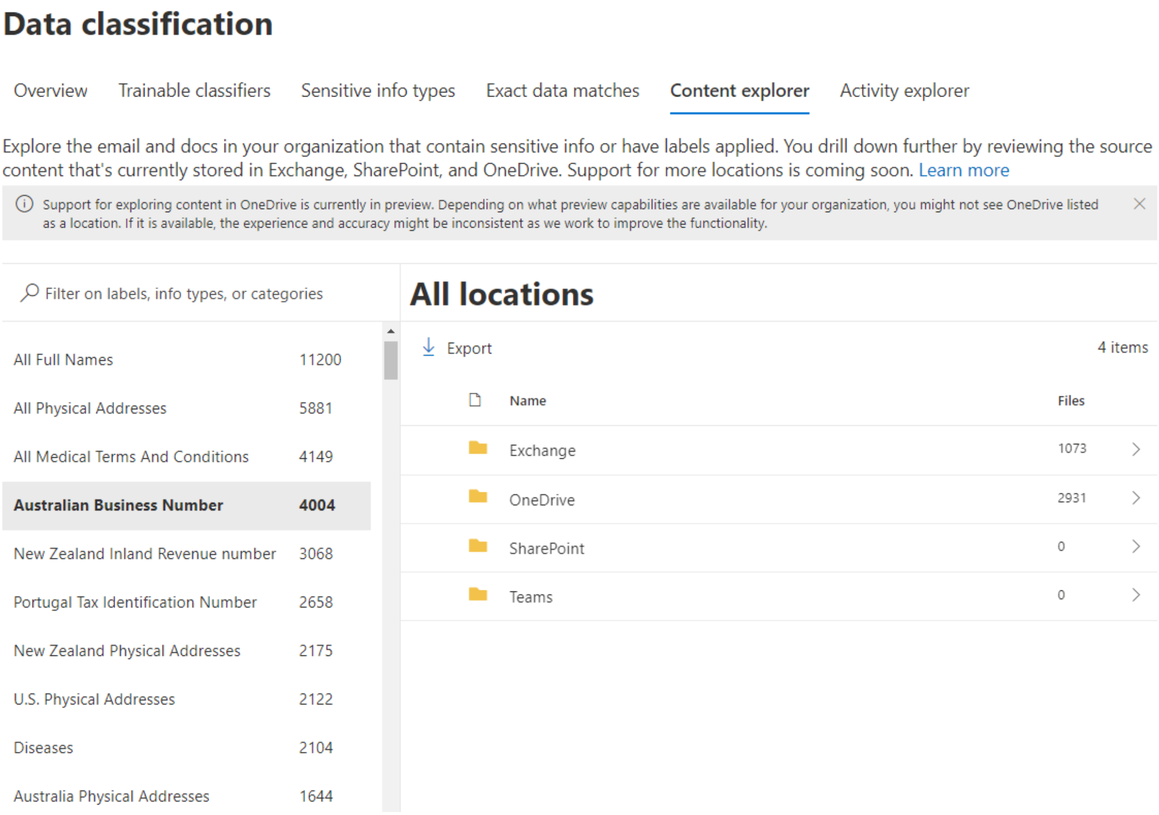
In the old world, we stored documents on file servers and controlled access via share and NTFS permissions. This worked well when everyone was in the office, never used a laptop, personal email accounts or USB sticks...

In other words, it was never a secure way of controlling access to sensitive data.

There are better ways, known as Microsoft Information Protection (MIP) although you may see older names such as Azure Information Protection (AIP) and Azure Rights Management Services (RMS). Again, a thorough exploration of MIP is a whole eBook in itself, so here we're merely going to introduce the concepts and get you started – automatic labelling of documents based on their content is an E5 feature, covered in Chapter 10.

INFORMATION PROTECTION BUILDING BLOCKS

The first step is finding out what kind of sensitive data is stored in your environment, assign a trusted administrator in your organization Content Explorer list viewer and Content Explorer content viewer (these are highly sensitive roles that not even a Global Administrator has by default) and direct them to the M365 compliance portal – Data classification – Content explorer. Before you have created any policies or anything (unified auditing must be turned on, which is the default) you'll find out what you've got stored in SharePoint / OneDrive for Business and Exchange Online in the way of sensitive data.



Data classification

Overview | Trainable classifiers | Sensitive info types | Exact data matches | Content explorer | Activity explorer

Explore the email and docs in your organization that contain sensitive info or have labels applied. You drill down further by reviewing the source content that's currently stored in Exchange, SharePoint, and OneDrive. Support for more locations is coming soon. Learn more

Support for exploring content in OneDrive is currently in preview. Depending on what preview capabilities are available for your organization, you might not see OneDrive listed as a location. If it is available, the experience and accuracy might be inconsistent as we work to improve the functionality.

Filter on labels, info types, or categories

All Full Names	11200
All Physical Addresses	5881
All Medical Terms And Conditions	4149
Australian Business Number	**4004**
New Zealand Inland Revenue number	3068
Portugal Tax Identification Number	2658
New Zealand Physical Addresses	2175
U.S. Physical Addresses	2122
Diseases	2104
Australia Physical Addresses	1644

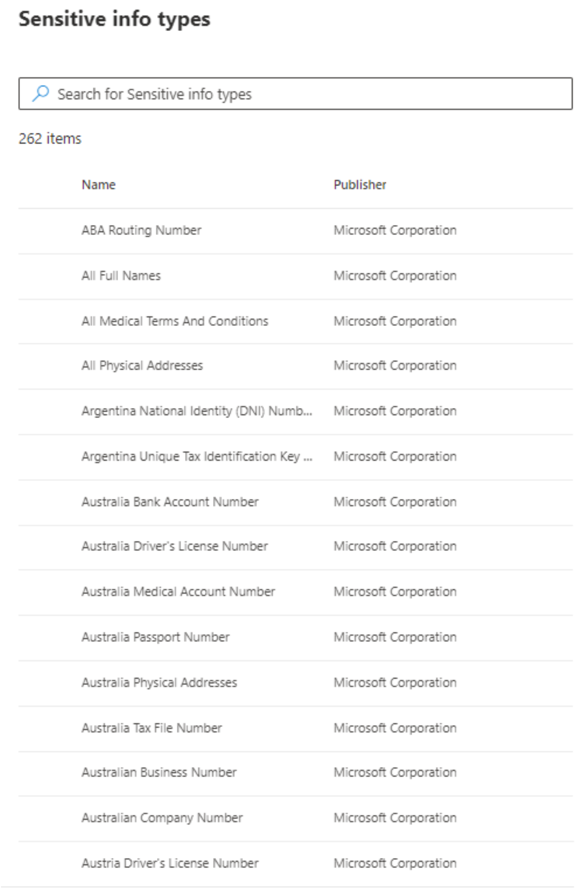
All locations

Export — 4 items

Name	Files
Exchange	1073
OneDrive	2931
SharePoint	0
Teams	0

Content explorer in the compliance portal

Your work starts with labeling; you can't protect every single document in your organization. The highly sensitive contract for your big acquisition is very different to the lunch cafeteria menu for next week. There are 262 (and constantly growing) built in Sensitive Information Types (SITs), identifying types of data from all over the world and you can create your own, based on specific patterns in your organization (project identifiers, staff IDs etc.).



Sensitive info types

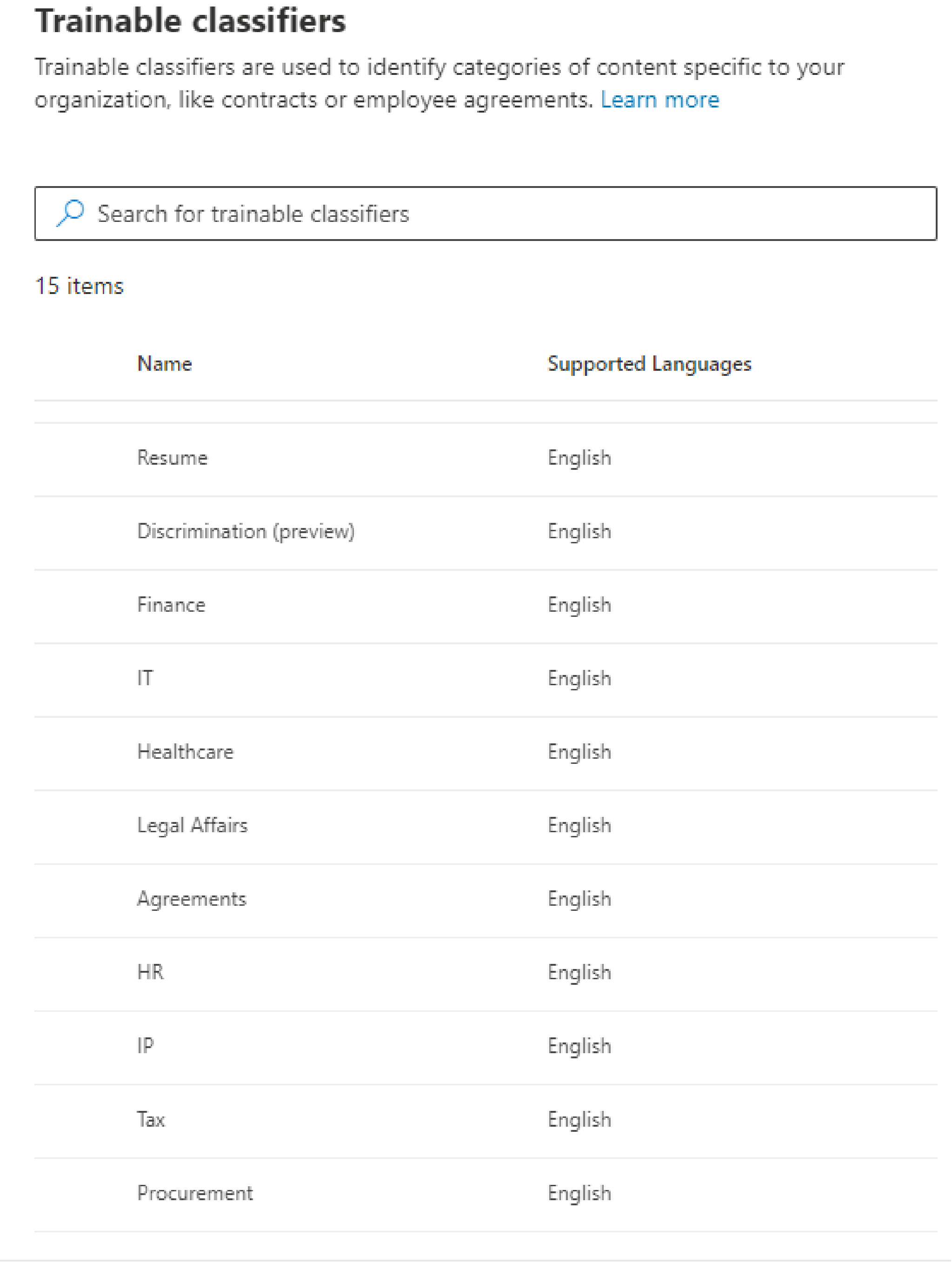
Search for Sensitive info types

262 items

Name	Publisher
ABA Routing Number	Microsoft Corporation
All Full Names	Microsoft Corporation
All Medical Terms And Conditions	Microsoft Corporation
All Physical Addresses	Microsoft Corporation
Argentina National Identity (DNI) Numb...	Microsoft Corporation
Argentina Unique Tax Identification Key ...	Microsoft Corporation
Australia Bank Account Number	Microsoft Corporation
Australia Driver's License Number	Microsoft Corporation
Australia Medical Account Number	Microsoft Corporation
Australia Passport Number	Microsoft Corporation
Australia Physical Addresses	Microsoft Corporation
Australia Tax File Number	Microsoft Corporation
Australian Business Number	Microsoft Corporation
Australian Company Number	Microsoft Corporation
Austria Driver's License Number	Microsoft Corporation

Information Protection list of Sensitive Information Types

There are also built-in trainable classifiers that uses Machine Learning models to identify data that's not just a Credit card number and accompanying evidence but more complex such as Resumes, Legal Affairs, Healthcare, Targeted Harassment, Profanity and more.



Trainable classifiers

Trainable classifiers are used to identify categories of content specific to your organization, like contracts or employee agreements. Learn more

15 items

Name	Supported Languages
Resume	English
Discrimination (preview)	English
Finance	English
IT	English
Healthcare	English
Legal Affairs	English
Agreements	English
HR	English
IP	English
Tax	English
Procurement	English

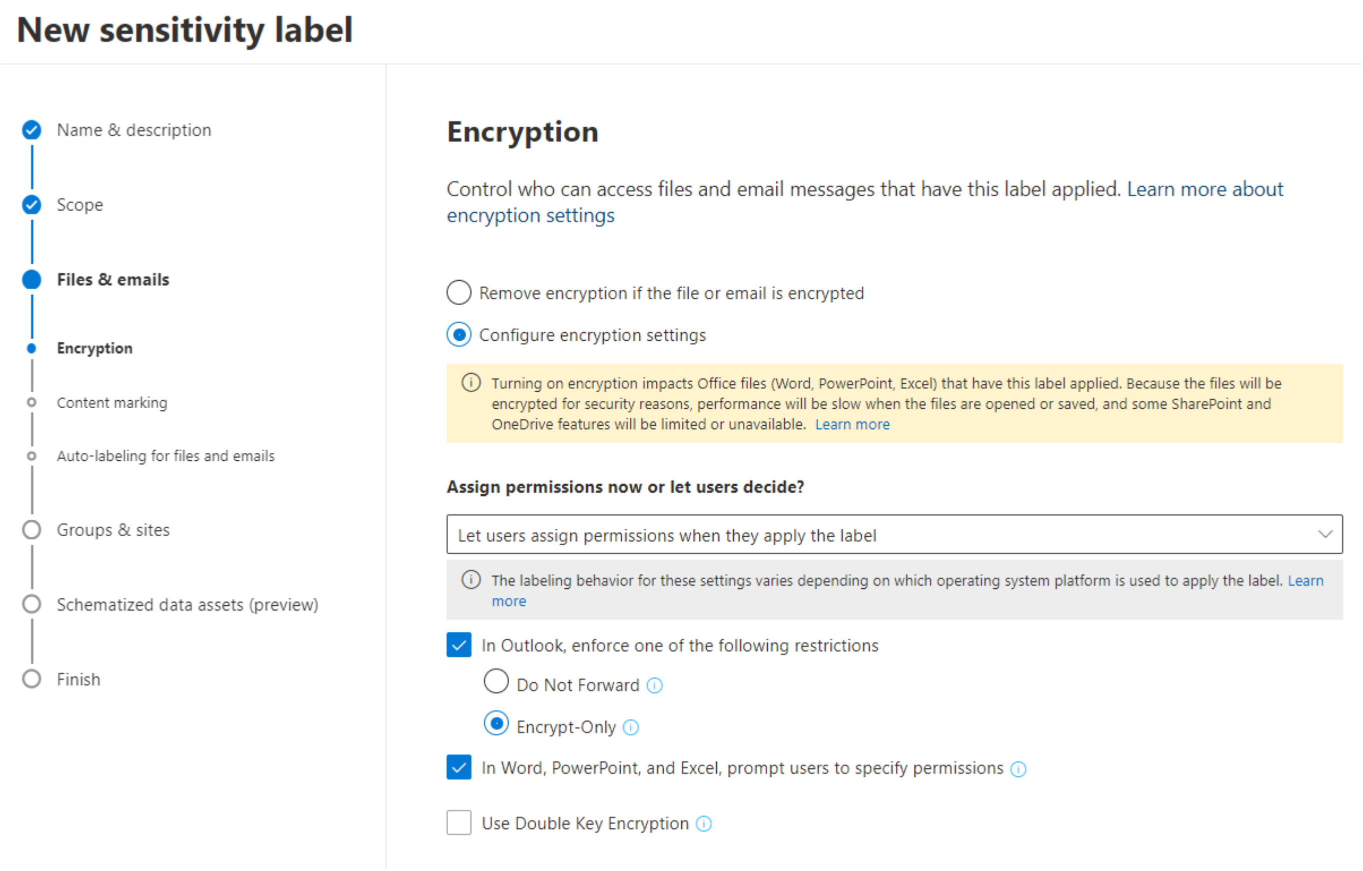
Information Protection list of Trainable Classifiers

Rather than matching random numbers, if you have a database of student ID numbers for instance, you can use Exact Data Match to label documents when those patterns show up.

The power of these labels, when you apply them to Office documents and PDFs (plus many other third-party file types) is that the protection follows the document, irrespective of where it's stored. You can now send an email and an attached Word document to a specific person and be sure that this person can only open the email and document once they're authenticated and only have the access you've given them (no printing or forwarding of the email for example) and only for the time you've given them. Of course, this isn't science fiction, if they really want to take pictures of the screen with their smartphone or write down the information you can't stop them (if they're authorized to see the information) BUT it's hard to argue that this was done by mistake if they're caught.

CREATE A SENSITIVITY LABEL AND POLICY

In the compliance portal, head down to Information protection and select the Labels tab and click Create a label. Enter a short name ("Sensitive – Internal use only") and a good description ("Use this label to mark documents that shouldn't be shared outside of our organization") to help your users understand what kind of data the label should apply to. Select Files & emails, pick both Encrypt and Mark and for encryption select Let uses assign permissions when they apply the label, enforce Encrypt-only in Outlook and prompt users in Word, PowerPoint, and Excel for permissions.



New sensitivity label

- ✓ Name & description
- ✓ Scope
- ● **Files & emails**
  - ● **Encryption**
  - ○ Content marking
  - ○ Auto-labeling for files and emails
- ○ Groups & sites
- ○ Schematized data assets (preview)
- ○ Finish

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted

● Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

ⓘ The labeling behavior for these settings varies depending on which operating system platform is used to apply the label. Learn more

☑ In Outlook, enforce one of the following restrictions

○ Do Not Forward ⓘ

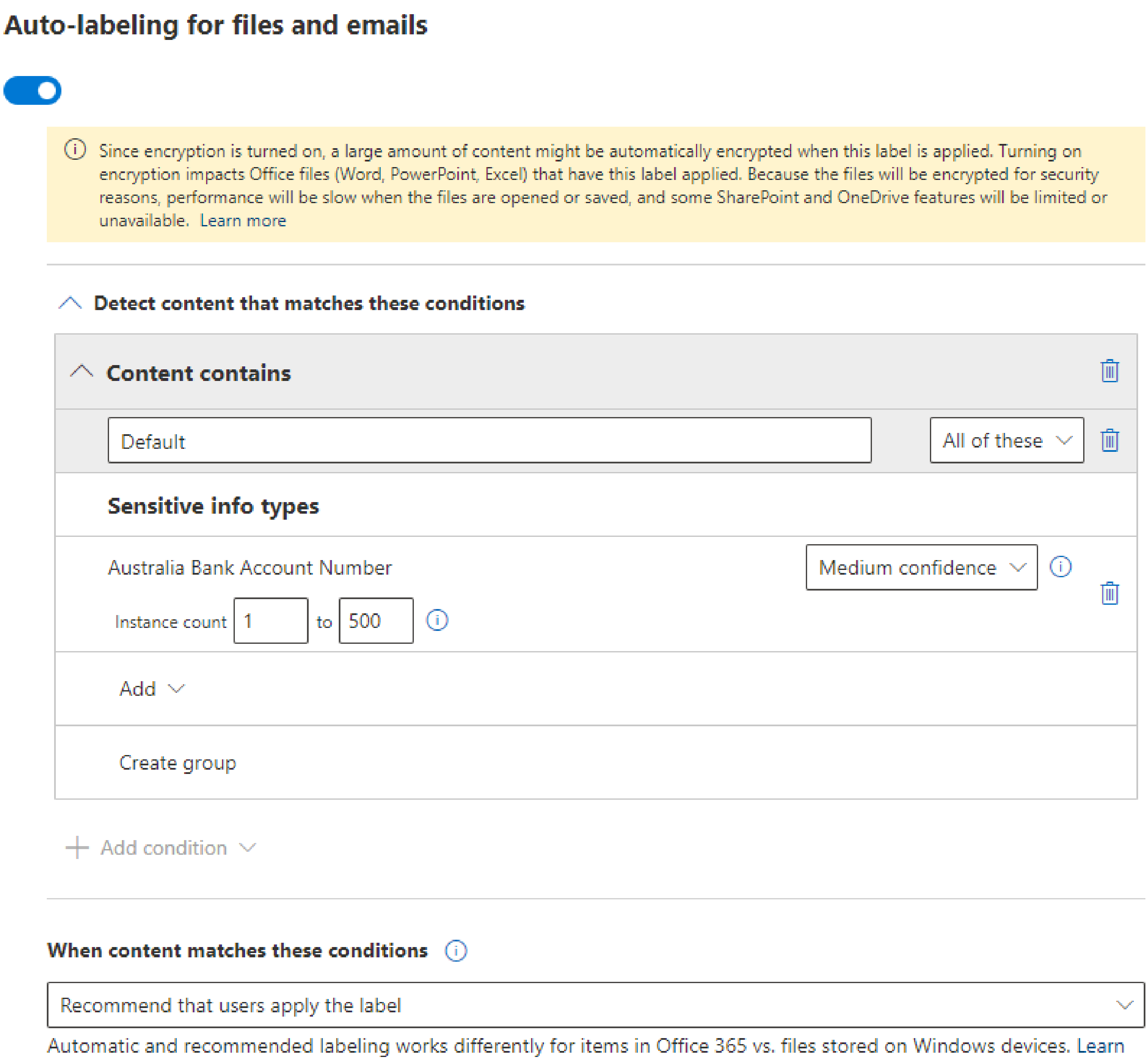
● Encrypt-Only ⓘ

☑ In Word, PowerPoint, and Excel, prompt users to specify permissions ⓘ

□ Use Double Key Encryption ⓘ

Information Protection Encryption settings for a new sensitivity label

Explore Content marking on your own, you can add headers, footers, and watermarks to documents and on the Auto-labeling page, click +Add condition and select Add – Sensitive info types and pick the applicable one(s) for your label so that if you're creating a new document and it contains this type of sensitive information, it can either be automatically applied or a banner can appear and recommend that users apply the label.



Auto-labeling for files and emails

Since encryption is turned on, a large amount of content might be automatically encrypted when this label is applied. Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Detect content that matches these conditions

Content contains

Default | All of these

Sensitive info types

Australia Bank Account Number | Medium confidence

Instance count 1 to 500

When content matches these conditions

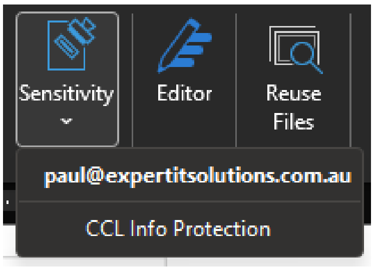
Recommend that users apply the label

Automatic and recommended labeling works differently for items in Office 365 vs. files stored on Windows devices. Learn

Information Protection configure labeling based on Sensitive Information Types

Click Next past the following two pages and create your new label. Under Next steps, click Publish this label, pick your new label, which users and groups is should apply to, pick Users must provide a justification to remove…. on the Settings page, don't apply the label by default to documents, emails and Power BI workspaces and give your new policy a clear name and description and publish it.

Users who are in scope for your new label and policy can now apply it manually to documents and emails with the Sensitivity button in the different Office applications.



Sensitivity button to apply a label manually to a document

As you can tell there's a lot more to explore around Information Protection, including the ability to label SharePoint sites and Teams to control external sharing options and adaptive scopes to target policies to the right people. For more, read:

- M365 Records Management Guide,
- Microsoft Information Protection in Microsoft 365;
- Deploy a Microsoft Information Protection solution.

Chapter 10 will cover how you can automatically label existing data at rest.

Also, ensure you assign Super User permissions to a few trusted administrators so that documents that were protected by someone who's no longer at the company can be opened and the permissions changed.

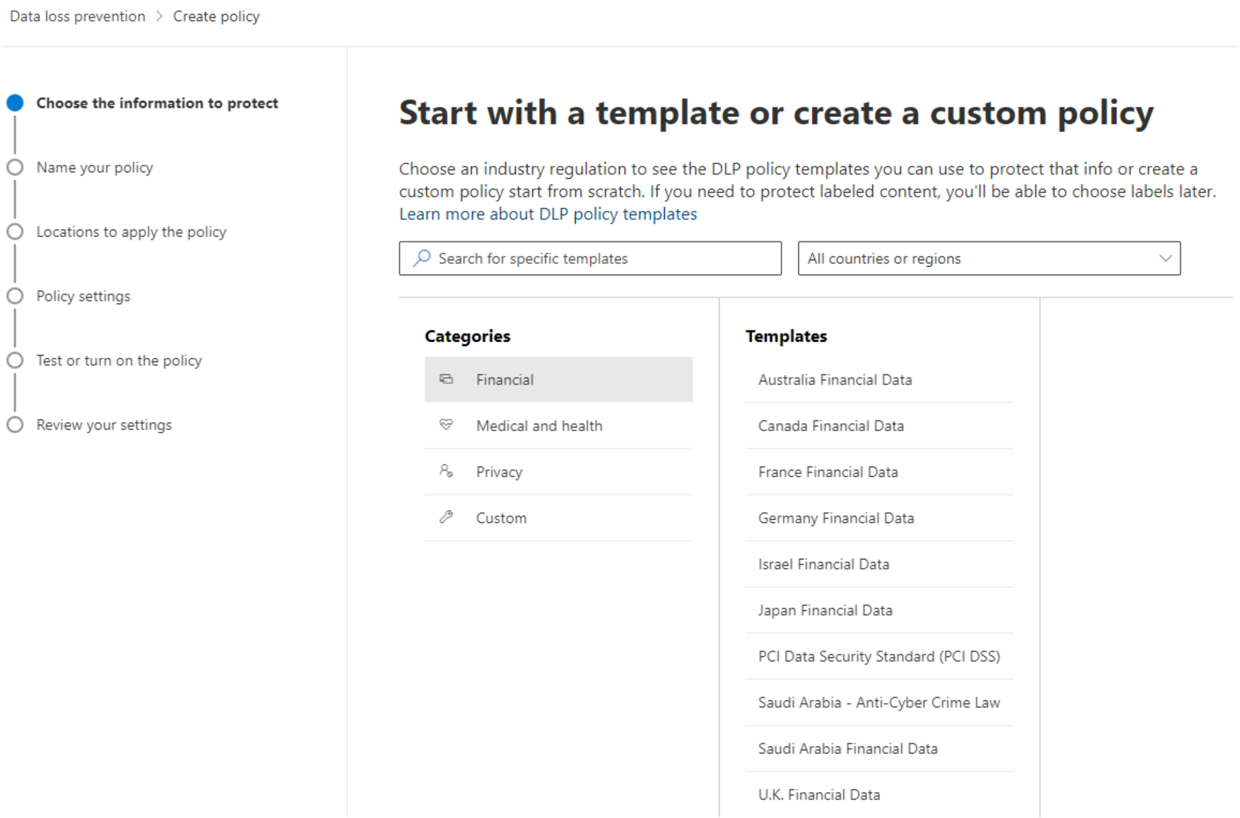
DATA LOSS PREVENTION

The other side of the coin is Data Loss Prevention (DLP). Here it's less about labeling sensitive data and marking it (so that users are aware of it and encrypting it to protect it as it's being shared), and more about warning users when they're about to share data in the wrong context.

Microsoft has done a lot of work in this area and now have a solution not only for the cloud and on-premises, but you can also control data sharing on endpoints (MacOS and Windows).

Again, there's a lot to dig into here, but my recommendation to get your feet wet with DLP is to simply create a policy that's report only, with no end user interaction. Just like Content Explorer above gives you an insight into what sensitive data types you have stored and where they're housed, using a DLP report only policy gives you a feel for what kind of data sharing is happening across your tenant. You can then build a business case for enforcing warnings and even block policies to stop accidental over sharing.

Back in the Compliance portal, head over to Data loss prevention – Policies and click +Create policy. You can use the built-in template categories (Financial, Medical and health, Privacy) or pick your region / country to see what's on offer. For this report only one, pick Custom and click Next.



Data loss prevention > Create policy

- ● Choose the information to protect
- ○ Name your policy
- ○ Locations to apply the policy
- ○ Policy settings
- ○ Test or turn on the policy
- ○ Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.
Learn more about DLP policy templates

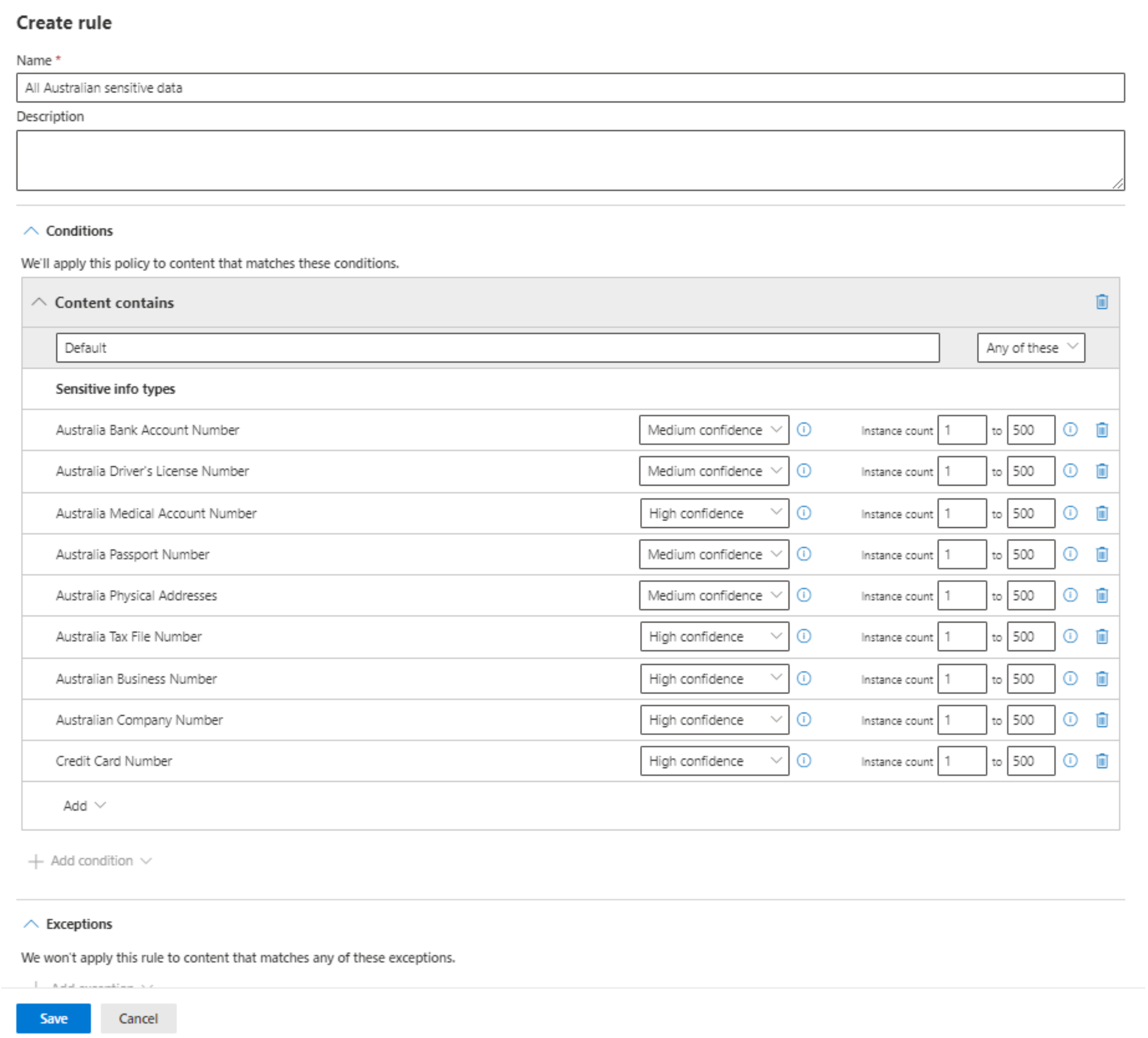
Search for specific templates

All countries or regions

Categories	Templates
Financial	Australia Financial Data
Medical and health	Canada Financial Data
Privacy	France Financial Data
Custom	Germany Financial Data
	Israel Financial Data
	Japan Financial Data
	PCI Data Security Standard (PCI DSS)
	Saudi Arabia - Anti-Cyber Crime Law
	Saudi Arabia Financial Data
	U.K. Financial Data

Data Loss Prevention Financial templates

Give it a name and a description and leave all available locations selected, then click Create rule, give it a name, and click +Add condition – Add and then search across the SITs for data that you wouldn't want to be shared externally by mistake. Examples include credit card numbers, plus region / country specific data. Leave Exceptions, Actions and User notifications / overrides blank for now, pick Low for severity level and add one or more administrators to be notified when an activity matches the rule, plus throttle the amounts of notifications if you're expecting a lot of emails. Leave the rest of the settings blank as well and Save the rule.



Create rule

Name *

All Australian sensitive data

Description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Default — Any of these

Sensitive info types

Sensitive info types	Confidence	Instance count	to
Australia Bank Account Number	Medium confidence	1	500
Australia Driver's License Number	Medium confidence	1	500
Australia Medical Account Number	High confidence	1	500
Australia Passport Number	Medium confidence	1	500
Australia Physical Addresses	Medium confidence	1	500
Australia Tax File Number	High confidence	1	500
Australian Business Number	High confidence	1	500
Australian Company Number	High confidence	1	500
Credit Card Number	High confidence	1	500

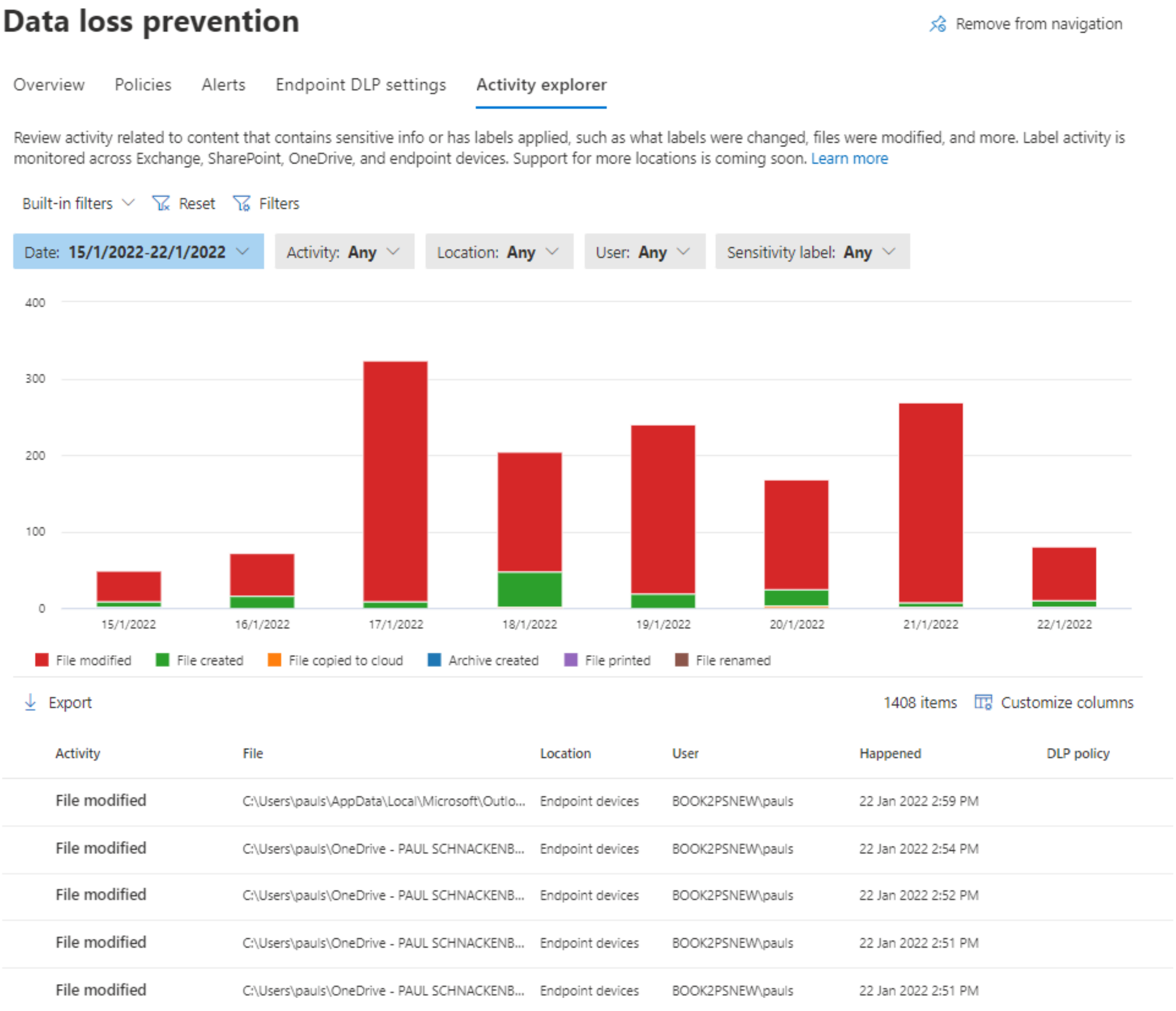
Exceptions

We won't apply this rule to content that matches any of these exceptions.

Data Loss Prevention Create rule

Since you haven't configured any action for policy violations you can safely turn on the policy right away. You'll now get an email whenever sensitive data matching your selected SITs is shared in any of the locations you picked.

The Activity explorer tab in Data loss prevention gives you a filterable view of actions taken by your users and in which location it took place.



Data loss prevention

Review activity related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and more. Label activity is monitored across Exchange, SharePoint, OneDrive, and endpoint devices. Support for more locations is coming soon. Learn more

Activity	File	Location	User	Happened	DLP policy
File modified	C:\Users\pauls\AppData\Local\Microsoft\Outlo...	Endpoint devices	BOOK2PSNEW\pauls	22 Jan 2022 2:59 PM	
File modified	C:\Users\pauls\OneDrive - PAUL SCHNACKENB...	Endpoint devices	BOOK2PSNEW\pauls	22 Jan 2022 2:54 PM	
File modified	C:\Users\pauls\OneDrive - PAUL SCHNACKENB...	Endpoint devices	BOOK2PSNEW\pauls	22 Jan 2022 2:52 PM	
File modified	C:\Users\pauls\OneDrive - PAUL SCHNACKENB...	Endpoint devices	BOOK2PSNEW\pauls	22 Jan 2022 2:51 PM	
File modified	C:\Users\pauls\OneDrive - PAUL SCHNACKENB...	Endpoint devices	BOOK2PSNEW\pauls	22 Jan 2022 2:51 PM	

Data Loss Prevention Activity Explorer

You can also to go Reports in the compliance portal, scroll down, and see reports on DLP Policy Matches, Incidents and false positives & overrides (for when you start enforcing your DLP policies).

WINDOWS INFORMATION PROTECTION

You can use Windows Information Protection (WIP), a pre-cursor to Endpoint DLP (Chapter 10) to separate business data from personal data. If you have personal Windows 10/11 devices you can use a Mobile Application Management (MAM) policy and if you have corporate owned, enrolled devices you can use a Mobile Device Management (MDM) policy. "Enlightened applications" i.e., ones that understand WIP policies will now block copy and paste from a corporate (stored in OneDrive for Business) to a personal (saved anywhere else) Word document for instance. Follow the instructions here to create WIP policy.

The number of regulations that (even small) businesses must comply with is increasing worldwide and they are increasingly focusing on keeping PII and other sensitive data secure – using Information Protection and DLP is going to be very important, make sure you're doing the right thing now, even if you don't have a specific regulation enforcing it yet.

Information Protection checklist >

Use the Information Protection checklist to controlling access to sensitive data.

CHAPTER 8 - SECURE SCORE

After reading this far you might ask yourself, doesn't Microsoft have a list of all the security settings? They do (sort of), for Business Premium there's this Tech Community article from mid-2020 and this docs page. The blog article isn't maintained (although all the recommendations in there are still valid) and both articles are missing a lot of suggested actions.

The second place to check is Secure Score, which has been in M365 for a long time – I wrote about it for the first time back in 2017.

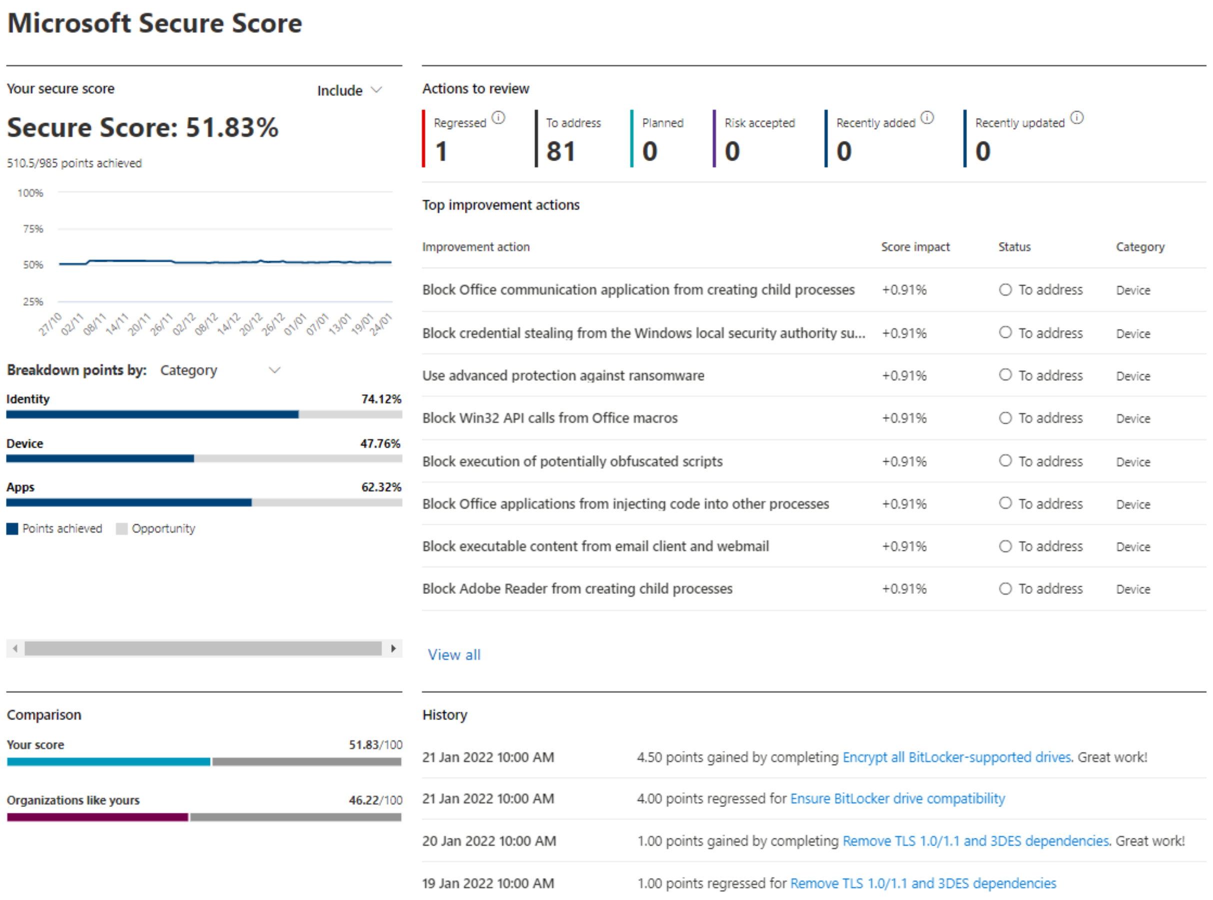
The concept is simple, gather a list of security "improvement actions" in a single pane, give each of them a score based on how important they are to a company's overall security posture and automatically track a score for the tenant as each action is taken. Let administrators compare their score to other businesses of their size, and in their industry to "gamify" security gains, plus track improvement over time.

Over time the single overall Secure score has been broken out into Identity, Device and Apps scores contributing to the overall score, it's changed to a percentage-based system (0% no actions taken, 100% all possible configurations implemented). Also, you'll find Secure Score in Azure (nothing to do with Microsoft 365) and Compliance Score both in Azure and in Microsoft 365, plus Productivity score as part of Endpoint Analytics in Intune which tracks your organization's digital transformation journey.

Note that improvements in the score can take some time to happen after you implement a control, Microsoft mentions 24-48 hours for the engine to pick up the change and award you the points, in my experience it can sometimes take longer than that.

CHECK YOUR SCORE

In the M365 Defender portal click on Secure score to see your current score and list of Top improvement actions. Scroll down a bit to compare your score with other organizations and see the history of settings applied.



Microsoft Secure Score

Your secure score

Secure Score: 51.83%

510.5/985 points achieved

Breakdown points by: Category

Identity	74.12%
Device	47.76%
Apps	62.32%

■ Points achieved □ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
1	81	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Block Office communication application from creating child processes	+0.91%	○ To address	Device
Block credential stealing from the Windows local security authority su...	+0.91%	○ To address	Device
Use advanced protection against ransomware	+0.91%	○ To address	Device
Block Win32 API calls from Office macros	+0.91%	○ To address	Device
Block execution of potentially obfuscated scripts	+0.91%	○ To address	Device
Block Office applications from injecting code into other processes	+0.91%	○ To address	Device
Block executable content from email client and webmail	+0.91%	○ To address	Device
Block Adobe Reader from creating child processes	+0.91%	○ To address	Device

Comparison

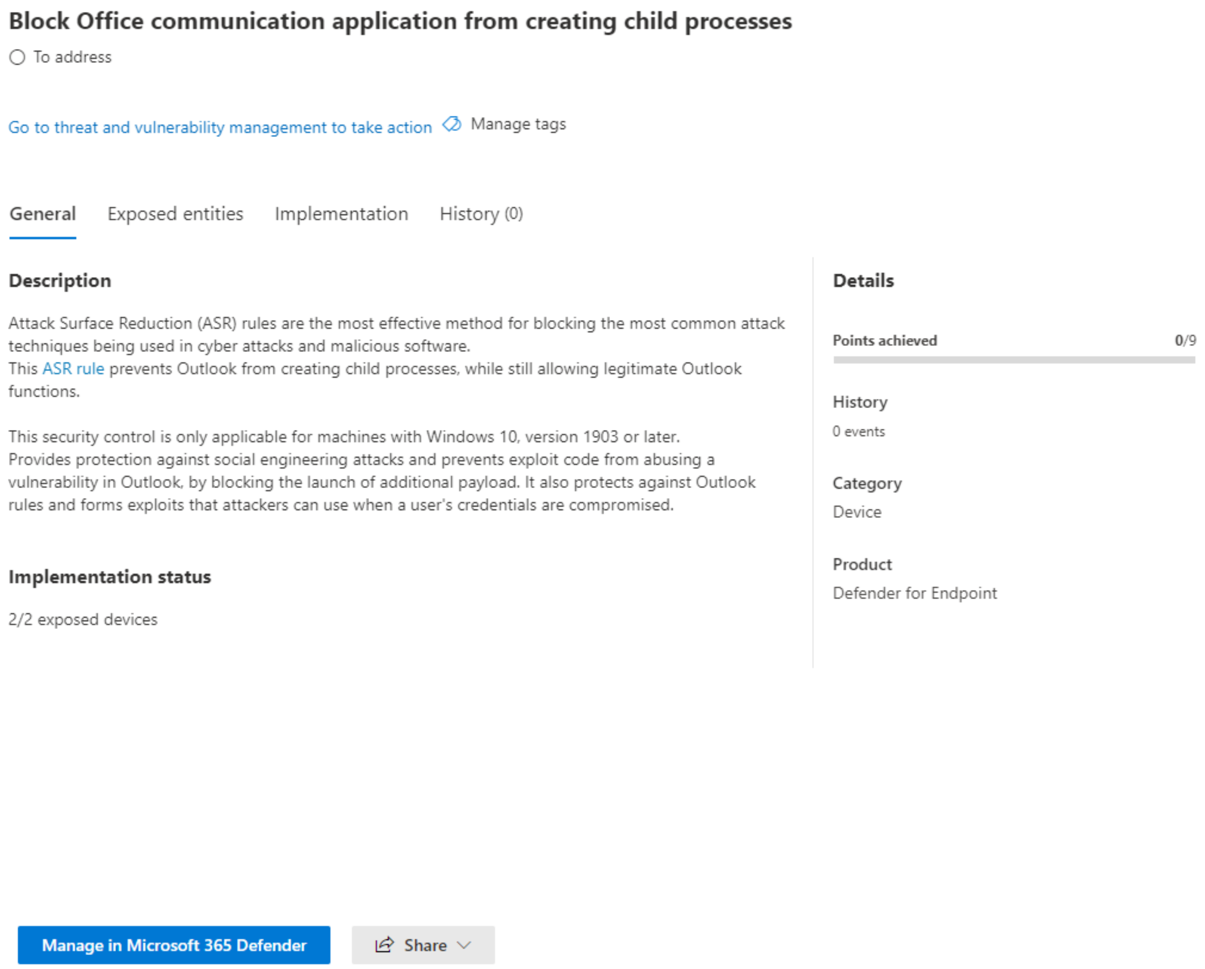
Your score	51.83/100
Organizations like yours	46.22/100

History

21 Jan 2022 10:00 AM	4.50 points gained by completing Encrypt all BitLocker-supported drives. Great work!
21 Jan 2022 10:00 AM	4.00 points regressed for Ensure BitLocker drive compatibility
20 Jan 2022 10:00 AM	1.00 points gained by completing Remove TLS 1.0/1.1 and 3DES dependencies. Great work!
19 Jan 2022 10:00 AM	1.00 points regressed for Remove TLS 1.0/1.1 and 3DES dependencies

Secure Score dashboard

When you click on an action you get a summary of what the control would do, points you'd gain, which devices or user accounts are vulnerable unless you take the action, the implementation steps, and any history for this particular action. You can also Share the action with someone if there's a team working on the actions.



Block Office communication application from creating child processes

○ To address

Go to threat and vulnerability management to take action   Manage tags

General   Exposed entities   Implementation   History (0)

Description

Attack Surface Reduction (ASR) rules are the most effective method for blocking the most common attack techniques being used in cyber attacks and malicious software.
This ASR rule prevents Outlook from creating child processes, while still allowing legitimate Outlook functions.

This security control is only applicable for machines with Windows 10, version 1903 or later.
Provides protection against social engineering attacks and prevents exploit code from abusing a vulnerability in Outlook, by blocking the launch of additional payload. It also protects against Outlook rules and forms exploits that attackers can use when a user's credentials are compromised.

Implementation status

2/2 exposed devices

Details

Points achieved 0/9

History
0 events

Category
Device

Product
Defender for Endpoint

Manage in Microsoft 365 Defender   Share

Secure Score sample action steps

The specific steps to take will vary from control to control but the instructions are pretty clear, as is any expected impact to end users. Note that Secure Score knows about your licensing level so a tenant with access to more potential security controls will have a longer list of actions.

Take some time to explore each action and make sure to implement all that have a low end-user impact and give a good score boost – "low hanging fruit". Also, Microsoft frequently adds more controls, so the list isn't static. Set yourself a reminder in your calendar to revisit Secure Score once a month and keep implementing controls to get as close to 100% as possible.

If you're an MSP that's managing multiple tenants, consider implementing a centralized dashboard to keep an eye on all your tenants scores and improvements using the API.

Information Protection checklist >

Use the Information Protection checklist to keep on top of scores and improvements to make.

CHAPTER 9 - BUSINESS PREMIUM

There are two sides of Microsoft 365, Business (up to 300 users) and Enterprise (E3, E5, F3, F5), this is ignoring government and education (A3, A5 – follows E3/E5 closely).

A few years ago, a lot of security features were missing from the Business side but that's improved markedly. Perhaps someone at Microsoft realized that SMBs need as good security as the larger end of town but don't have the skills and manpower to configure complex solutions.

MEET THE BUSINESS FAMILY

So, if you're an SMB and you're not expecting to grow beyond 300 users, just pick the least costly Business plan and you're done? Not so fast, first, if you're a small business but you manage sensitive data (lawyers, doctors, financial institutions) go for Microsoft 365 E5. You'll get the best security services Microsoft offers, they're very good and getting better, plus they're tightly integrated, unlike "best of breed" point solutions.

If that's not your situation however and you want to stay in the business family (Business Basic, Apps for business, Business Standard, Business Premium) there's only one option; Business Premium. The others don't offer any of the security features, whereas Business Premium comes with Azure AD Premium Plan 1 AND (very soon) Defender for Business, the new flavor of Microsoft's excellent Endpoint protection tool designed specifically for SMBs.

If you find that the cost jump is too steep, there are third-party alternatives such as Hornetsecurity's 365 Total Protection Business that stops spam, malware, adds email signatures etc.

BUSINESS PREMIUM

Azure AD Premium P1 gives you Cloud app discovery which is a scaled down version of Defender for Cloud Apps, formerly known as Microsoft Cloud App Discovery (MCAS), which will discover office like applications in use across your business. It won't give you policies or the full catalog of 27,000+ cloud apps for discovery and management that the E5 version offers. It does give you Azure AD Application proxy to publish on-premises web applications securely, Conditional Access (this is key), SharePoint limited access if you're on a personal device, Password Protection for both AD and AAD and Self-Service Password Reset from the cloud back to AD on-premises and more.

Business Premium itself gives you Bitlocker (local SSD on devices encrypted) and Bitlocker To Go (encrypt USB sticks), Windows Information Protection, Defender for Office Plan 1 (Chapter 2), Intune / Endpoint Manager (Chapter 6) and Information Protection & DLP (Chapter 7).

Defender for Business will be a powerful addition when it comes out of public preview, offering Threat & vulnerability Management (TVM), inventorying all installed software on all endpoints, and comparing with all CVEs to give you a prioritized list of applications to upgrade, based on the risk of the discovered vulnerability plus the number of endpoints in your business that has it installed, and how frequently it's used. It also brings Attack surface reduction rules, Next generation protection against attacks and malware with both local and cloud-based ML models, full Endpoint Detection and Response (EDR) so every process and action on every endpoint is visible. Most importantly in an SMB context it comes with Automated Investigation and Response (AIR), meaning it'll fix most issues itself without you having to intervene. And it does this across Windows, macOS, iOS and Android.

Business Premium checklist >

Use the Business Premium checklist to get your security settings configured.

CHAPTER 10 - MICROSOFT 365 E5

In the previous nine chapters we've looked at the security features available to most administrators in Microsoft 365 – E3, F3/F5 and Business Premium. Here we look at what the additional SKUs such as Microsoft 365 E5 Security and Microsoft 365 E5 Compliance (these are add-ons to M365 E3 and offer a subset of the full E5) offers. We'll also look at the security features in the full Microsoft 365 E5.

If you're on Office 365, adding Enterprise Mobility + Security (EMS) E3 or E5 is the equivalent of Microsoft 365 E3 and E5 respectively.

Both E5 and E5 Security includes Defender for Endpoint Plan 2, Defender for Identity, Defender for Office 365 Plan 2, Application Guard for Office 365 and Safe Documents, Defender for Cloud Apps, Azure AD Premium Plan 2, rule-based automatic retention policies and Machine Learning based retention.

Only the full E5 offers Information Protection Plan 2, DLP for Teams chat, Endpoint DLP, Advanced Office Encryption, Advanced Audit, Insider Risk Management, Communication Compliance, Information Barriers, and Privileged Access Management.

That's a long list and this excellent article contains a description of many advanced security features and the licensing required for each.

The point of course of bundling so many of these features together in this plan is that it can replace many existing point solutions and their associated monthly licensing cost. Defender for Cloud Apps can replace a current CASB, Defender for Endpoint can replace your current EDR and anti-malware solution as well as your current TVM service and so forth.

However, it's worth nothing here that Microsoft is not liable for data loss, so if you don't want to put all your security eggs in Microsoft's basket, you should consider a third-party service to manage email security, including full Exchange Online, Teams, OneDrive and SharePoint backup through Hornetsecurity's 365 Total Protection Enterprise Backup.

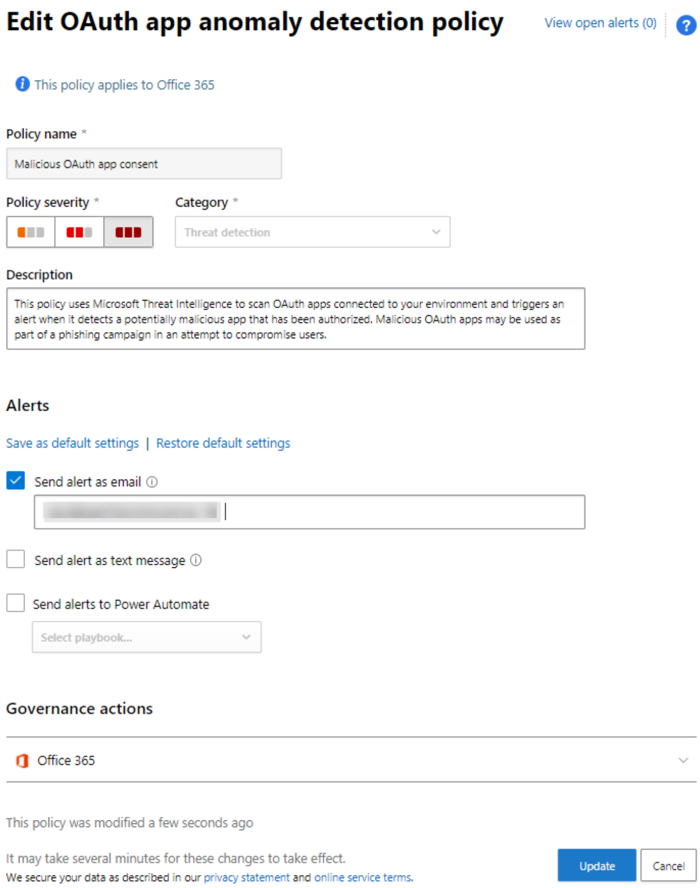
MICROSOFT 365 E5 AND E5 SECURITY

Let's start with Defender for Endpoint P2 (which used to be just Defender for Endpoint until P1 came along, part of M365 E3). On top of the features mentioned in Chapter 9 for Defender for Business, P2 adds Microsoft Threat Experts and Threat hunting. This is a two-pronged feature, once you're enabled for it (apply in the console) they'll let you know if they detect a threat in your environment and on a pay for service basis you can also use Microsoft's SOC analysts to extend your team when required. Plan 2 also adds support for Linux servers, on top of the other OS platforms.

Defender for Identity (formerly Azure ATP) is a cloud-based service for your Active Directory Domain. Agents on AD Federation Services servers and Domain Controllers forward relevant network traffic captures and event log information to the cloud to be analyzed and intrusions into your network will be quickly spotted.

Defender for Application Guard brings virtualization isolation technology to Edge and Office (Word, Excel and PowerPoint on Windows) and when suspicious sites / documents are opened they're in a separate area, so malicious actions can't spread to the rest of the OS.

Defender for Cloud Apps is worthy of its own eBook but suffice to say – if you have the licensing, make sure you explore what it can do and how powerful it is. Most importantly, back in Chapter 5 we looked at the risks around malicious OAuth apps and illicit consent grants. Defender for Cloud Apps has very strong ways of discovering these in your environment as well as policies available to manage this risk and controlling access.



Edit OAuth app anomaly detection policy

This policy applies to Office 365

Policy name *

Malicious OAuth app consent

Policy severity *

Category *

Threat detection

Description

This policy uses Microsoft Threat Intelligence to scan OAuth apps connected to your environment and triggers an alert when it detects a potentially malicious app that has been authorized. Malicious OAuth apps may be used as part of a phishing campaign in an attempt to compromise users.

Alerts

☑ Send alert as email

[redacted]

☐ Send alert as text message

☐ Send alerts to Power Automate

Select playbook...

Governance actions

Office 365

This policy was modified a few seconds ago

It may take several minutes for these changes to take effect.

We secure your data as described in our privacy statement and online service terms.

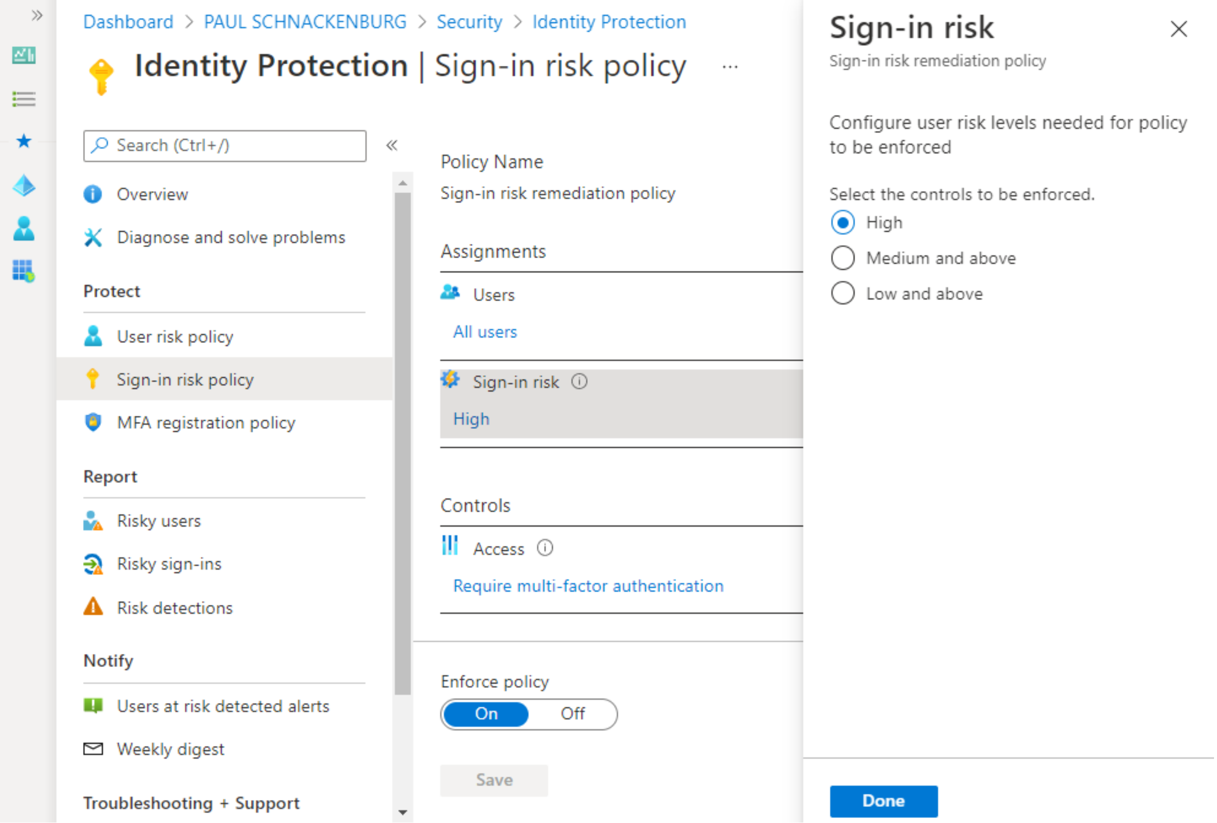
Defender for Cloud Apps detection policy

Apart from Safe Attachments and Safe Links that's available in Defender for Office Plan 1, Plan 2 in E5/E5 Security adds Threat Trackers (information about current cybersecurity issues that may impact your organization), Threat Explorer (to keep tabs on current threats impacting your organization and help with Hunting), Automated Investigation and Response (AIR), Attack Simulation Training (send phishing simulation to your users and follow up with automated training videos for those who fail) and Campaign Views (shows current phishing campaigns against your business and the impact). Explore each of these features and make sure you use the attack simulations frequently; both the lures and the training videos are much better quality than they used to be.

AZURE AD PREMIUM P2

While this is just single line in what's included in E5/E5 Security it deserves its own section as it gives you Privileged Identity Management (PIM), Identity Protection and Access reviews. PIM allows you to turn permanent Global Administrator / Exchange Administrator etc. accounts into eligible accounts. These user accounts are now ordinary user accounts and if they're compromised, the blast radius is much smaller. When these users need to perform administrative actions, they login to the Azure AD portal and go through a workflow to elevate their privileges for a set amount of a few hours. This workflow can include entering a service ticket number, performing MFA, and being approved by another administrator / manager.

An impactful feature is Identity Protection which comes in the form of two policies, Risky Sign-ins, and Risky Users. Risky user accounts are identified using ML and other means, if an account is likely compromised, for example when Microsoft finds credentials in dumped breach data, it automatically enforces a Self-Service Password Reset. Each sign-in is also analyzed and based on risk signals (and how you've configured the policy sensitivity), if a particular access is "iffy", the user will automatically be prompted for MFA.


Dashboard > PAUL SCHNACKENBURG > Security > Identity Protection
Identity Protection | Sign-in risk policy
Search (Ctrl+/)
Overview
Diagnose and solve problems
Protect
User risk policy
Sign-in risk policy
MFA registration policy
Report
Risky users
Risky sign-ins
Risk detections
Notify
Users at risk detected alerts
Weekly digest
Troubleshooting + Support

Policy Name
Sign-in risk remediation policy

Assignments

Users
All users

Sign-in risk
High

Controls

Access
Require multi-factor authentication

Enforce policy
[✓ On] Off

Save

Sign-in risk

Sign-in risk remediation policy

Configure user risk levels needed for policy to be enforced

Select the controls to be enforced.

● High
○ Medium and above
○ Low and above

Done

Azure AD Identity Protection Sign-in risk policy

Access Reviews solves the age-old problem where access is never removed from users, only added. You can always tell if a particular user has worked at a company for a long time, based on the number of security groups they're members in. Access Reviews can be used to identify and minimize the number of users with privileged access, catch excessive permissions granted as users move between departments, control access given to guest users, and can even be extended to reviewing access by applications in Azure AD.

MICROSOFT 365 E5

The full license of Microsoft 365 E5 provides Information Protection Plan 2 which adds automation, in addition to users labeling documents manually this will identify sensitive content automatically, including scanning your SharePoint, Exchange Online and OneDrive for Business repositories for sensitive data and label it. Not only that, but you can also use the Information Protection scanner on-premises to scan file shares and SharePoint servers and identify, label and optionally protect / encrypt documents.

Plan 2 also comes with DLP for Teams chat and most importantly, Endpoint DLP. This is now available for Windows 10/11 (client built in, no agent required) and MacOS. It comes with powerful features to control printing, saving to USB storage, copy files via Bluetooth and different cloud storage locations based on the sensitivity of the data in the documents.

Advanced Message Encryption lets you control encryption of messages with policies that identifies the content automatically, and applies different branding based on it plus lets you revoke access to email and expire them after a set time.

Advanced Audit adds the ability to keep your unified audit log data for one year, with the option to extend to 10 years with an add-on license. You also get additional events logged and high-bandwidth access to logs based on the number of seats in the organization.

The risk to your business isn't just external, disgruntled staff who want revenge on their boss, or the long-term sales star who wants to take the customer database that he's built up when he leaves are all part of Insider Risk, particularly now when many people are working from home. Insider Risk Management is a full featured, HR integrated solution that anonymizes any identified users during the investigation phase (to eliminate bias by the investigator) and turns the case into an eDiscovery case when there's enough evidence to warrant further action.

When you want to ensure that your staff isn't using harassing or bullying language in Teams and other communications channels, use Communication Compliance. Blocking electronic communication between staff in different departments can be achieved with Information Barriers if you require that to adhere to a specific regulation.

Privileged Access Management is the cousin of PIM and it allows you to configure policies to limit the capabilities of an administrator, enabling just-enough-access in addition to the just-in-time access that PIM provides.

Microsoft 365 Enterprise E5 checklist >

Use the Microsoft 365 Enterprise E5 checklist to make better use of the additional SKUs this license offers.

CHAPTER 11 – THE CHECKLIST

There are three columns, one for settings available for most licensing options, one for Business Premium specific controls and finally one for the advanced security settings in M365 E5. Dark grey boxes indicate controls not available in that licensing SKU. Share and use this with your team/s to secure your M365 environment.

Chapter 1 - Identity	**M365 General**	**Business Premium**	**M365 E5**
Enable MFA for administrators			
Enable MFA for users			
Create cloud only administrator accounts for privileged users / occasional administrators			
Disable app passwords			
(Configure trusted IPs)			
Disable text message MFA			
Disable phone call MFA			
Remember MFA trusted devices 90 days			
Train staff in using MFA correctly			
Use Windows Hello where possible			
Use FIDO2 / 2FA keys where possible			
Investigate legacy authentication protocol usage in AAD Sign-in logs			
Block legacy authentication with CA Policy			
Block legacy authentication in M365 Admin Center			
Create two Break glass accounts and exempt from MFA, CA Policies etc.			
Configure alerting if a Break glass account is used			
Enable Security Defaults in AAD (consider the limitations)			
Enable PIM (AAD Premium P2) for all admin users			
Add organization specific words to Password protection			
Deploy Password protection in AD on-premises			

Enable PIM (AAD Premium P2) for all admin users			
Add organization specific words to Password protection			
Deploy Password protection in AD on-premises			
CA Policy Require MFA for admins			
CA Policy Require MFA for users			
CA Policy Require MFA for Azure management			
CA Policy Block legacy authentication			
CA Policy Require compliant or Hybrid AAD joined device for admins			
CA Policy Require compliant or Hybrid AAD joined device for users			
CA Policy Block access to M365 from outside your country			
Require MFA for risky sign-ins	▨	▨	
Require password change for high-risk users	▨	▨	
Create custom branding logos and text in Azure AD			
Enable and configure Self Service Password Reset, including password writeback			
Check that Unified Auditing is enabled			
Define audit retention policies (90 or 365 days)			
Integrate applications into Azure AD			
AAD Connect - Ensure only relevant OUs are replicated to Azure AD			

Chapter 2 - Email	**M365 General**	**Business Premium**	**M365 E5**
Check that mailbox auditing is on for all mailboxes, if not, enable it			
Edit the default anti-phishing policy			
Include domains you own			
Enable mailbox intelligence including impersonation protection			
Enable spoof intelligence			
Threat policies - configure Anti-phishing, enable mailbox intelligence, safety tips on			
Threat policies - configure Anti-spam, enable ZAP, outbound spam notification			
Threat policies - configure Anti-malware, add all file extensions			
Configure Outlook Report Message add-in for all users + tenant mailbox to get reported messages			
Configure Alert policies to match business needs			
Train users to use Office Message Encryption			
Configure Office Message Encryption with Mail flow rules			
Warn and Block emails with dangerous attachments			
Configure Safe Attachments policy			
Configure Safe Attachments Global settings			
Configure Safe Links policy			
Configure Safe Links Global settings			
Block auto forwarding of emails with a Mail flow rule			
Check user accounts linked to shared mailboxes and block login for them			
Check SPF record for each vanity domain			
Configure DKIM CNAME records in DNS and ensure they're picked up in DKIM in the security portal			
Configure DMARC TXT record in DNS			
Configure DMARC to reject policy once you know the domain is covered			
Install Message Header Analyzer add-in on your device			

Chapter 3 - Teams	**M365 General**	**Business Premium**	**M365 E5**
Limit Teams creation to a set of users			
Limit private channel creation to a set of users			
Delete inactive Teams			
Disable third-party Teams file storage locations			
Configure interoperability with Teams in other tenants and Skype consumer			
Configure guest user settings in Azure AD - directory permissions			
Configure guest user settings in Azure AD - who can invite			
Configure guest user settings in Azure AD - user flows for application access			
Configure guest user settings in Azure AD - which domains can users be invited from			
Configure Guest access settings in Teams			
Customize meeting invitation branding			

Chapter 4 - SharePoint	**M365 General**	**Business Premium**	**M365 E5**
Configure External file sharing for SharePoint			
Configure External file sharing for OneDrive for Business			
Configure other external file sharing settings			
Configure Access control			
Configure an alert when files are shared externally			

Chapter 5 - Applications	**M365 General**	**Business Premium**	**M365 E5**
Investigate existing OAuth applications and their granted permissions			
Restrict or remove suspicious / malicious OAuth applications			
Configure User and Group settings for granting permissions to OAuth apps, None or limited permissions			
If using limited permissions, define those			
Configure Admin consent requests and accounts who are going to review requests			

Chapter 6 - Endpoint Manager	M365 General	Business Premium	M365 E5
Define device groups in Endpoint Manager			
Define enrollment / application management policies Endpoint Manager			
Create a device compliance policy for Windows devices			
Optional - create policies for other device types			
Optional - create Configuration policies			
Optional - import existing Group Policy settings			
Configure Security baselines			

Chapter 7 - Information Protection	M365 General	Business Premium	M365 E5
Create a label			
Create a label policy and test it			
Work with the business to identify data labels to use			
Create a group of Super User accounts for data recovery			
Create a report only DLP policy with email notifications			

Chapter 8 - Secure Score	M365 General	Business Premium	M365 E5
Check current secure score			
Implement all low user impact actions			
Implement all high score improvement actions			
Plan to implement the rest of the possible actions to take			

Chapter 9 - Secure Score	M365 General	Business Premium	M365 E5
Go through the list of security features available in Business Premium and ensure they're configured			
Deploy Defender for Business to all endpoints (when it's available)			

Chapter 10 - Microsoft 365 Enterprise E5	**M365 General**	**Business Premium**	**M365 E5**
Deploy Defender for Endpoint plan 2	▨	▨	
Deploy Defender for Identity	▨	▨	
Enable Defender for Application Guard	▨	▨	
Enable Safe Documents	▨	▨	
Create an OAuth app policy in Defender for Cloud Apps	▨	▨	
Explore Threat Trackers	▨	▨	
Use Threat Explorer	▨	▨	
Configure Automated Investigation and Response in Defender for Office 365	▨	▨	
Use Attack Simulation Training to train end users	▨	▨	
Explore Campaign Views	▨	▨	
Enforce PIM for ALL administrative accounts, apart from your break glass accounts	▨	▨	
Configure Sign-in risk policy	▨	▨	
Configure User risk policy	▨	▨	
Configure Access Reviews for Teams / groups, guests, administrative accounts and AAD applications	▨	▨	
Automate Information Protection labelling across your cloud estate	▨	▨	
Use the Information Protection scanner to find, label and protect sensitive data on premises	▨	▨	
Enable DLP for Teams chat	▨	▨	
Configure Endpoint DLP with business input	▨	▨	
Configure Advanced Message Encryption	▨	▨	
Configure Advanced Audit retention policies to 1 year for all users	▨	▨	
Configure Insider Risk Management policies	▨	▨	
Configure Communication Compliance policies and reviewers	▨	▨	
Configure Information Barriers	▨	▨	
Configure Privileged Access Management	▨	▨	

THE PATH AHEAD

Possibly the most important approach to IT security is to adopt the "assume breach" mindset. In other words, put all the controls in place, train your users and have the right processes in place BUT also plan for what happens when you do have a breach. How do you spot the intrusion early (Defender for Identity/ Endpoint + Sentinel – see below)? How do you contain the attackers before they fully compromise your entire network?

MAKE THE TIME.

You might be feeling overwhelmed after reading this eBook and feeling that there's a mountain of stuff to do to implement all these controls. Maybe you're the IT person in your company and you've got to convince your boss to let you set aside time and effort to do this. Or you're an MSP / IT Service provider and you've realized that you have a lot of work to do to get your clients security posture up to scratch. If so, here are a couple of pointers that can help as you sit down with a client. You could draw a real-world analogy and point out that while they're living in a house that works, it's not finished and the exposed wires in the ceiling and unfinished plumbing are security risks. Or you could talk about the relatively minor cost upfront to implement these security controls, compared to the major cost and interruption of a breach. As someone who's been in exactly that situation many times, I wish you good luck.

ADD THESE TO YOUR TOOLKIT.

Another important step is to become familiar with the ATT&CK Matrix and to see if the controls that you've configured cover all the different techniques attackers use to infiltrate your business. Keep an eye on the Microsoft Security Intelligence page to learn about recent campaigns and attacks.

We haven't talked about Microsoft Sentinel as it's not a part of Microsoft 365 but it's an invaluable addition if you don't have Security, Information, and Event Management (SIEM) in place today. As you've seen throughout this eBook, most security settings and investigations are converging in the Microsoft 365 Defender portal, but this only covers Microsoft 365 workloads. What about all the other applications and SaaS services your business relies on? This is where Sentinel comes into the picture, taking all the logs and incidents / alerts raised in 365 Defender and combining them with all those other data sources for a true 360 view of your entire business. Learn more about Sentinel here.

FINAL THOUGHT.

IT security is a journey without a final destination, and it's never finished. However, if you implement the steps outlined in this eBook, your Microsoft 365 tenant will be more secure than it was before.

But did we miss anything? Is there a setting you think we should have included or a recommended configuration that you disagree with? Let us know at dojo@altaro.com and we'll include it in the next version.

APPENDIX – ACRONYMS

There are many IT acronyms used in this eBook and while they're spelt out the first time they're used, here's a handy list of all of them, along with a short explanation of what each means.

AAD – Azure Active Directory. The underlying directory of Microsoft 365 that maintains information about user and device accounts, authenticates and authorizes access to resources, and can optionally be synchronized with on-premises Active Directory using Azure AD Connect.

CA/CAP - Conditional Access Policies. A feature of Azure AD Premium P1+ that lets you craft policies to control who can access what resource, from where and under what conditions.

CAE – Continuous Access Evaluation. A feature of Azure AD that evaluates a change in a user's state (disabled, moved to a different Wi-Fi network etc.) much faster than the legacy 1 hour delay.

CASB – Cloud Access Security Broker. A "Firewall as a Service" that runs in the cloud and controls access to SaaS applications and identifies malicious files and actions.

CVE – Common Vulnerabilities and Exposures. An identified vulnerability in a system (software or hardware), used in TVM to identify vulnerable software in your environment.

DC – Domain Controller. A server in your on-premises Active Directory that authenticates and authorizes user and device account access to resources. Can be synchronized with Azure Active Directory.

DLP - Data Loss Prevention. A technology in Microsoft 365 to identify sensitive data and report on, recommend against or block accidental sharing of this data in the wrong context.

DKIM - Domain Keys Identified Mail. An email security feature that enables recipients of emails that purport to be coming from your organization to check the validity of that claim.

DMARC - Domain-based Message Authentication, Reporting and Conformance. An email security feature that lets recipients of emails from your domain know what to do if they're identified as spoofed.

EDR - Endpoint Detection and Response. A modern endpoint protection approach that keeps track of every single action, by every process, taken in the OS, to identify malicious code or attacker's actions.

MAM - Mobile Application Management. Managing applications on iOS, Android and to some degree, Windows, and these application's access on personally owned devices.

MDCA – Microsoft Defender for Cloud Apps. Microsoft's CASB, part of M365 E5 licensing.

MDE – Microsoft Defender for Endpoint. A full EDR and endpoint protection solution for Windows, MacOS, iOS, Android, and Linux. Comes in P1, P2 and Business versions.

MDM - Mobile Device Management. Enrolling all types of devices into full management through a cloud-based service for device control.

MDI – Microsoft Defender for Identity. A cloud service that gathers information from your Domain Controllers on premises to quickly identify malicious activity by attackers.

MDO – Microsoft Defender for Office 365. A set of security features to enhance the security of email and collaboration tools and protect against malicious emails, attachments, messages, and links.

MEM – Microsoft Endpoint Manager. The umbrella name for Intune, the cloud service for MAM and MDM plus Configuration Manager Endpoint Manager for larger businesses' on-premises device management.

MFA – Multi Factor Authentication. Using a second factor beyond username and password to identify a user when they log in to a system.

MIP - Microsoft Information Protection. The umbrella term for different technologies, all designed to identify sensitive data in your business and safeguard it with policies, visual cues, and encryption.

MSP – Managed Service Provider. An outsourced IT service provider that manages your IT systems on a contracted, preventative maintenance basis.

MSSP - Managed Security Service Provider. An outsourced IT Security provider who focuses on protecting your systems against cyber threats and identify / block them when they do occur.

OAuth – Open Authentication. A standard for authentication of applications and how they can be integrated into Azure AD.

OME - Office Message Encryption. The ability to encrypt and / or set Do not Forward on emails sent from Exchange Online to any email address, either manually or automatically.

PII – Personally Identifiable Information. Data about a person that could be used to identify them or reveal sensitive information about them.

PIM - Privileged Identity Management. A feature of Azure AD Premium P2 that turns permanent administrator accounts into eligible accounts so that they must elevate their accounts to privileged permissions (for a short time) when they need to perform admin activity.

SIEM - Security, Information, and Event Management. A group of services and tools that give real-time analysis of information security in an organization.

SIT - Sensitive Information Type. A component of MIP with predefined identifiers for sensitive data such as credit card numbers, passport IDs etc. from all over the world.

SPF – Sender Policy Framework. A way to use DNS records to identify potentially malicious or spam email.

SSPR – Self Service Password Reset. The ability for users to reset their own password when they've forgotten it, using alternate email address, MFA and / or security questions to lower the load on your help desk.

TVM - Threat & vulnerability Management. A feature of Defender for Endpoint that identifies all software installed on each endpoint, what known vulnerabilities exists (CVEs) and gives you a list of what needs to be upgraded to minimize the attack surface.

WHFB – Windows Hello for Business. A collection of biometric (fingerprint and face scan) technologies and other features to improve the sign in security on Windows devices.

WIP - Windows Information Protection. The ability to separate business and personal data on a Windows device in applications that support the blocking of copy and paste, saving etc. to the wrong location.

ZAP - Zero-hour auto purge. The ability of Exchange Online to "reach into" users' mailboxes and to delete an already delivered email that's been subsequently identified as malicious.

SECURE YOUR DATA

TRY OUR TOOLS

365 TOTAL PROTECTION

Security and compliance management for Microsoft 365

We offer you two comprehensive packages for your company security management developed for Microsoft 365: With 365 Total Protection Business, you get a comprehensive security solution with a wide range of features that ensure your email and data security in Microsoft 365. The Enterprise version covers legally compliant email archiving with advanced features and offers intelligent protection against advanced persistent threats by using AI-based analysis mechanisms.

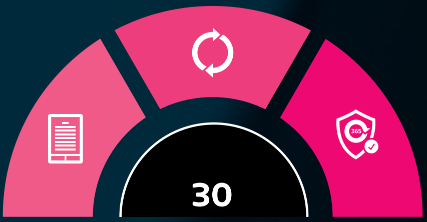
Protection from:

Targeted attacks on Microsoft 365 accounts

SPECIALLY DEVELOPED FOR MICROSOFT 365 AND SEAMLESSLY INTEGRATED

It couldn't be easier – onboarding within 30 seconds.
In just 3 clicks, the intuitive onboarding process is complete and your Microsoft 365 merges with 365 Total Protection.
365 Total Protection makes sure you get the most out of your Microsoft cloud services.

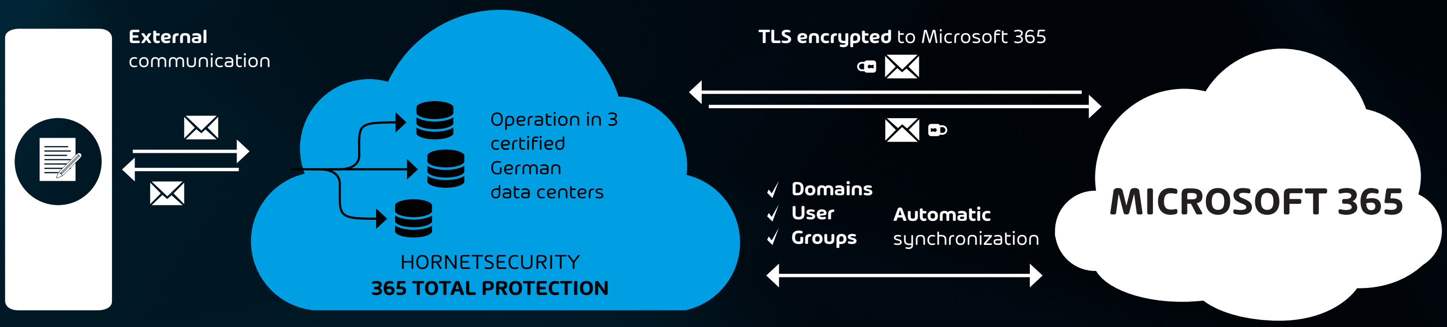
Fig.: Simple onboarding process in three steps



1. REGISTER **COMPANY DATA**
2. CONNECT **WITH MICROSOFT**
3. SET UP **COMPLETED!**

INTEGRATION OF 365 TOTAL PROTECTION IN THE EMAIL MANAGEMENT SYSTEM

All aspects of security administration are easy to manage with 365 Total Protection – without the need for maintenance or updates. Existing user profiles can be managed or created in mere seconds.


External communication
Operation in 3 certified German data centers
HORNETSECURITY
365 TOTAL PROTECTION
TLS encrypted to Microsoft 365
✓ Domains
✓ User
✓ Groups
Automatic synchronization
MICROSOFT 365

www.hornetsecurity.com | info@hornetsecurity.com

START YOUR 30-DAY TRIAL

FOUND THIS EBOOK HELPFUL?

LEARN MORE ABOUT MICROSOFT 365

On-demand Webinar:

Critical Security Features in Office/Microsoft 365 Admins Simply Can't Ignore

Simply enter your name and email, then sit back and enjoy!

Critical Security Features in Office/Microsoft 365 Admins Simply Can't Ignore

On-demand webinar

Watch >

The Real Cost of Microsoft 365 Revealed

Blog article

Read >

Office 365 vs Office 2019: Pros and Cons for IT Admins

Blog article

Read >

R.I.P. Office 365, Long Live Microsoft 365

Blog article

Read >

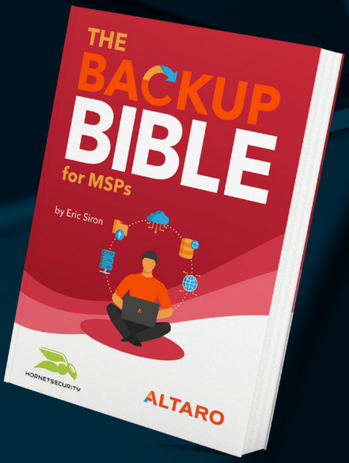
EXPLORE OTHER EBOOKS AND PUBLICATIONS

Office 365 / Microsoft 365
THE ESSENTIAL COMPANION GUIDE
SECOND EDITION BY PAUL SCHNACKENBURG
HORNETSECURITY
ALTARO
OFFICE 365
MICROSOFT 365
DOJO

Office 365 / Microsoft 365 - The Essential Companion Guide

Office 365 and Microsoft 365 contain truly powerful applications that can significantly boost productivity in the workplace. However, there's a lot on offer. Use this guide to ensure you get the most out of your investment!

Download now >



The Backup Bible

Everything you need to know about planning, deploying and maintaining a secure and reliable backup and disaster recovery strategy.

Download now >

Cyber Threat Report – Edition 2021/2022

Email is still the most popular way of communicating for companies. However, not all emails that land in employee inboxes, are wanted. Learn everything about current email security threats in Hornetsecurity's brand new Cyber Threat Report.

Download now >

Join the Altaro DOJO for eBooks, webinars and more, on everything from automation to security.

HOW CAN WE MAKE OUR EBOOKS BETTER?

LET US KNOW

As we're always looking to ensure our content helps you, we'd like to check in and see what you thought of this eBook and how we can make it better.

It should only take a couple of minutes and will be super helpful to us as we shape future eBooks!

Or complete the feedback form using this link

SHARE THIS EBOOK

FOLLLOW HORNETSECURITY

THIS EBOOK WAS PUBLISHED BY HORNETSECURITY

www.hornetsecurity.com/en

Production: Dunya Spiric

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

If you have any feedback about this book, its content, questions for the author, or any other feedback, please write to info@hornetsecurity.com.

.

HORNETSECURITY