

Office 365 / Microsoft 365

THE ESSENTIAL COMPANION GUIDE

SECOND EDITION BY PAUL SCHNACKENBURG

ALTARO
Part of **HORNETSECURITY** group

DOJO 



CONTENTS

INTRODUCTION	6
Drop your baggage.....	7
How to keep up	7
Be your own guinea pig	10
Adoption.....	11
CHAPTER 1 – WELCOME TO OFFICE 365 AND MICROSOFT 365.....	12
Office 365.....	12
Microsoft 365	14
CHAPTER 2 - MANAGING O365AND M365	16
Web Portals.....	16
PowerShell.....	17
CHAPTER 3 - MIGRATING TO O365	20
Migration.....	20
CHAPTER 4 - SUPPORTING M365.....	24
Test Connectivity.....	24
Client-side tools	25
Service Requests	27
Service Health	28
Network Connectivity	29
Microsoft 365 Desired State Configuration	29

CHAPTER 5 – AZURE ACTIVE DIRECTORY	30
Meet AAD & Hybrid Identity	30
AAD Connect – your umbilical cord	30
Azure MFA	32
Publishing Applications	34
Premium Features.....	35
Conditional Access Policies	36
Managing the Account lifecycle.....	37
CHAPTER 6 – CLIENTS	39
Desktop choices	39
Mobile choices.....	40
OneDrive.....	40
Teams.....	40
Apps Admin Center	40
CHAPTER 7 – EXCHANGE ONLINE	42
It’s a Hybrid World.....	42
Backup and Native Data Protection	42
Autodiscover	44
Managing Mailboxes.....	44
Mailbox Archive	45
Mail Forwarding.....	45
Shared Mailboxes	46
Mail Contacts and Users.....	46
Distribution Lists	46

CHAPTER 8 – ONEDRIVE FOR BUSINESS AND SHAREPOINT.....	47
OneDrive for Business.....	47
SharePoint.....	48
CHAPTER 9 OFFICE 365 GROUPS.....	52
Group Types.....	52
CHAPTER 10 – TEAMS.....	55
Meet Teams.....	55
Managing Teams.....	56
Using Teams.....	59
Viva.....	60
Extending Teams.....	60
CHAPTER 11 – OTHER OFFICE 365 APPLICATIONS.....	62
Planner.....	62
Stream.....	63
Kaizala.....	63
PowerBI.....	63
Power Automate.....	64
PowerApps.....	64
Yammer.....	65
CHAPTER 12 - SECURITY IN O365.....	66
Microsoft 365 Defender.....	67
Office 365 Sensitivity Labels.....	68
Microsoft Information Protection.....	68
Office 365 Message Encryption.....	69
Data Loss Prevention.....	69

Exchange Online Protection	70
Defender for Office 365	71
Auditing	71
Say Goodbye to passwords?	73
Block user access	74
CHAPTER 13 – SECURITY IN MICROSOFT 365	75
Microsoft Defender for Identity	75
Cloud App Security.....	75
Secure Score.....	76
Security is everyone’s responsibility.....	79
CHAPTER 14 – MICROSOFT ENDPOINT MANAGER	80
Mobile Device Management	81
Mobile Application Management	82
Microsoft Endpoint Configuration Manager	83
Defender for Endpoint	84
CHAPTER 15 – WINDOWS 10 ENTERPRISE	85
Windows 10 Enterprise	85
CONCLUSION.....	87
ABOUT THE AUTHOR	88
ABOUT ALTARO	91

INTRODUCTION

Welcome to this free eBook on Office 365 and Microsoft 365 from Altaro. We're going to show you how you can use these cloud services to improve your business.

The audience for this book is administrators and IT staff who are either preparing to migrate to Office / Microsoft 365 or who have already migrated and who need to get the lay of the land. If you're a developer looking to create applications and services on top of the Microsoft 365 platform, this book is not for you. If you're a business decision maker, rather than a technical implementer, this book will give you a good introduction to what you can expect when your organization has been migrated to the cloud and ways you can adopt various services in Microsoft 365 to improve the efficiency of your business. If you're a Microsoft Partner, [managing other companies' deployments](#) consider the forthcoming [Microsoft 365 Lighthouse](#) as a way to manage multiple tenants in one console.

We'll cover the differences more deeply later in the book but here's a good place to clarify that **Office 365** (from now on referred to as O365), is email collaboration and a host of other services provided as a Software as a Service (SaaS) whereas **Microsoft 365** (M365) is Office 365 plus Azure Active Directory Premium, Endpoint Manager (Intune) – cloud-based management of devices and security plus Windows 10 Enterprise. Both are per user-based subscription services that require none (or very little) infrastructure deployments on premises.

DROP YOUR BAGGAGE

One of the most important things you need to do if you have a background with Exchange Server or SharePoint Server on premises is to drop the idea that O365 is just a hosted Exchange or SharePoint. Some years ago, this was true and O365 was simply Microsoft hosting Exchange, SharePoint and Lync servers in their datacenters, but this is no longer true. O365 is now a cohesive platform, with Exchange Online and SharePoint online providing some foundational building blocks for that platform but there are many other services built on top that you'll miss (or misunderstand) if you're still thinking in terms of hosted mail servers. A case in point is Microsoft Teams, a collaboration product that uses Exchange Online to store retained data and chats, SharePoint to store documents, Planner for lightweight project management and Azure AD for identity. All that complexity is managed by Microsoft and you simply administer Teams as just another service. And that also means there'll never be a "Teams server" for on-premises, the required building blocks are just too complex for most businesses to deploy.

The other thing to let go off if you're coming from an on-premises background is planning for software upgrades every few years. Upgrading Exchange Server, as an example, can be a large project (depending on the size of your environment), taking months to plan and execute. O365 is a different world with smaller updates coming every day or week and your job thus transforms into assessing these changes, how they'll impact users and manage change in the organization.

HOW TO KEEP UP

I have worked with Exchange Server since version 5.5 (1997) and I got used to the cadence of a new version every 2-3 years. I bought books and read up about all the new features and changes in preparation for the next iteration. That approach to software development is finished.

Nearly all software projects (and definitely O365/M365) are now aiming at frequent, incremental changes. This brings several benefits, first each update is minor and no big project plan for the “upgrade” is required, secondly the developers can adjust course and add new features based on user feedback much faster.

Filters

Showing 939 updates¹: [Download](#) [Share](#) [RSS](#)

In development	Rolling out	Launched
514	176	248

Description	Status	Products	Release
OneDrive: Full-fidelity shared libraries in OneDrive	Launched	All environments General Availability OneDrive	December CY2020
Microsoft Information Protection: Automatic sensitivity labeling in Office apps on Windows	Launched	Worldwide (Standard Multi-Tenant) Microsoft Information Protection General Availability Desktop	November CY2020
Microsoft Teams: New file sharing experience	Rolling out	Worldwide (Standard Multi-Tenant) Microsoft Teams General Availability Web	October CY2020

Products

- Access
- Azure Active Directory
- Azure Information Protection
- Bookings
- Cortana
- Excel
- Exchange
- Forms
- Microsoft 365 admin center
- Microsoft 365 compliance center
- Microsoft 365 Groups
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Edge
- Microsoft Graph
- Microsoft Information Protection
- Microsoft Intune
- Microsoft Search
- Microsoft Stream
- Microsoft Teams
- Microsoft To Do

The Microsoft 365 Roadmap

As an M365 administrator however this does bring a big challenge. Instead of being able to plan for and learn about a large set of new features coming in the next big release, new features are released daily, and you have to understand these and help your organization take advantage of them.

There are several ways to manage this – depending on your learning style. Some people learn by reading, other by listening, yet others by watching videos and some people only learn by doing tasks themselves (and most of us learn best with a blend of these).

Here are some resources to add to your toolbelt for keeping up with changes in M365:

The M365 roadmap lets you filter on many different components of M365.

<https://www.microsoft.com/en-au/microsoft-365/roadmap?rtc=2&filters=>

Office 365 Weekly is maintained by Thomas C. Finney at Microsoft.

<https://office365weekly.blog/>

Staying on top of Office 365 Updates is a new location with links to various resources for managing the flood of updates.

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/staying-on-top-of-office-365-updates/ba-p/1201118>

What's new in Microsoft Intune details the weekly updates in Microsoft Intune.

<https://docs.microsoft.com/en-us/intune/whats-new>

What's new in Azure Active Directory covers monthly updates to AAD (see [chapter 5](#)).

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/whats-new>

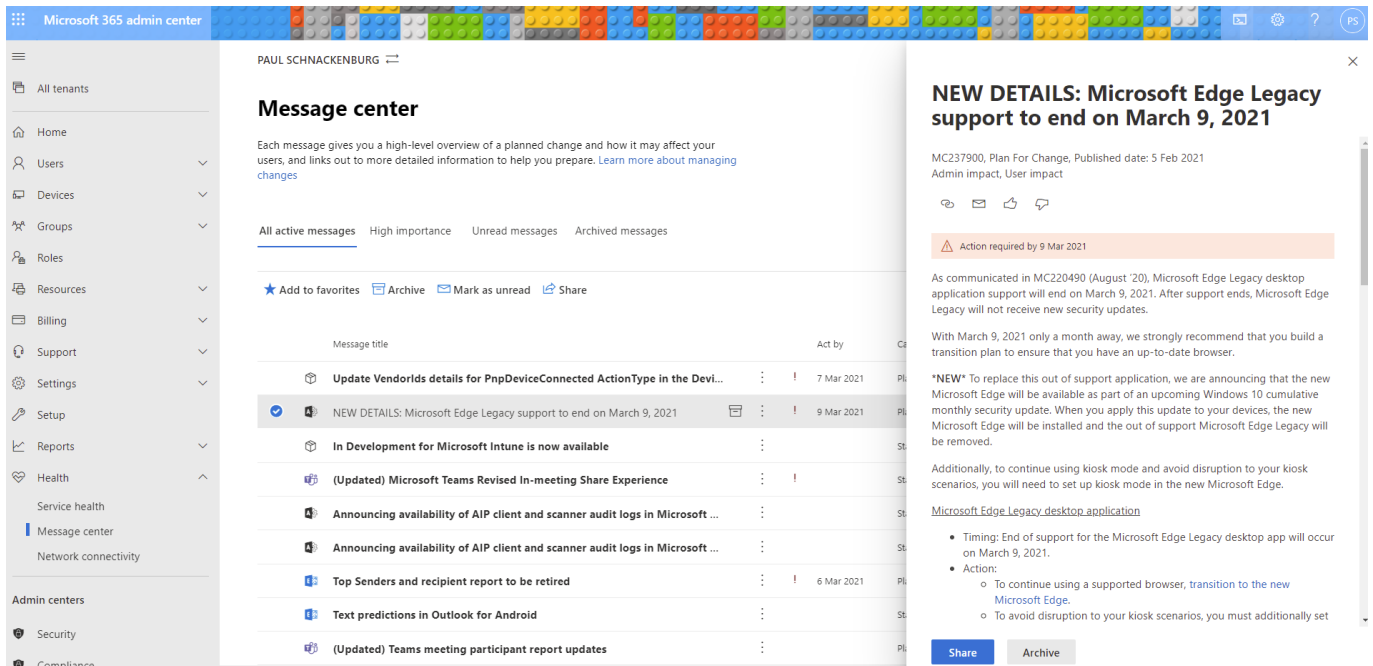
Azure AD Connect: Version release history covers updates to AAD Connect (see [chapter 5](#)).

<https://docs.microsoft.com/en-au/azure/active-directory/hybrid/reference-connect-version-history>

Microsoft Mechanics is a YouTube channel with interviews and demos on upcoming features along with Office and Azure playlists.

<https://www.youtube.com/channel/UCJ9905MRHxwLZ2jeNQGIWxA>

And finally, the **Message center** in the portal ([chapter 2](#)) shows a stream of what's changing and new features – click the Edit Message center preferences to customize which services you get updates for and who should get emailed the weekly digest – a best practice is to target an email distribution list so that staff who don't have access to Message center can receive weekly email updates.



Controlling notifications from the Message Center

BE YOUR OWN GUINEA PIG

It's important that as an administrator you are testing new features as they come out or ideally when they're in the preview phase. There are two tracks for updates released in O365, [Standard and Targeted](#). The former is the normal rollout cadence while the latter ensures that you get new features as soon as they're ready.

In the past the recommendation was to have a small, separate test tenant for this where the whole tenant was in **Targeted**, if you have the budget this can be useful. Today it's more common to define members of the IT team and power users in your business with **Targeted release for select users**. There's also [an option](#) to ensure that your local Office Apps for enterprise installation receives updates ahead of the rest of your users.

ADOPTION

If your challenge is helping others in your business to get on board the O365 train Microsoft has [a great community](#) and [resources](#) to help you, and if you need help to continue driving adoption across M365 workloads, join the free [Champions Program](#).

Another great resource is [Fasttrack](#) which provides migration guidance for every O / M365 tenant (and Dynamics 365 and Azure), if you're on O365 and have 150+ seats you can converse with a migration expert online and if you have over 500 seats you can have [an engineer assist you in the migration](#) (remotely) and also in subsequent adoption projects.

CHAPTER 1 – WELCOME TO OFFICE 365 AND MICROSOFT 365

In this chapter we're going to look at the different flavors of O365 and M365, how to pick between them and what value they provide to your business.

Correctly implemented O365 or M365 is an enabler for your business, making it easy for your staff to work in teams and collaborate both internally and with external people in a secure manner. They also enable secure work from home/anywhere for your employees. Apart from picking the right flavor of O365 or M365 the key to a successful adoption is planning, end user training and ensuring your IT staff understands their new role.

OFFICE 365

Some services mentioned in this chapter are explored more deeply in later chapters. We'll use the term SKU; it stands for Stock Keeping Unit and is a way to describe different licensing levels.

Your first waypoint here is between Business and Enterprise SKUs. The former tops out at 300 users so if you have a larger business (or is expecting to grow), stick with the Enterprise flavors.

To clarify – **Microsoft 365 Apps for enterprise** (what [used to be called Office ProPlus](#)) is the new name for the desktop applications such as Word, Excel etc. that are available for Windows and Mac – some SKUs include it, and some don't. On the other hand, all plans include Office Online (recently renamed to just "Office" – not confusing at all), so Word, PowerPoint etc. running in a browser. These online versions of Office are limited in functionality compared to their desktop brethren but are useful for quick edits.

There used to be both Office 365 and Microsoft 365 offerings for SMB, up to 300 users. Microsoft has however moved to a single set of SKUs for SMB – Microsoft 365 (see below), hopefully reducing confusion and choice paralysis.

On the Enterprise side (which is only a name, it doesn't have to be for a huge business, for example you could have five lawyers in an SMB using Enterprise E5) there's **Apps for enterprise** which only gives you Apps for enterprise and OneDrive file storage but no other cloud services. **E1** gives you Office (Online) and Exchange, OneDrive, SharePoint, Teams, Yammer and Stream, **E3** gives you Microsoft 365 Apps for enterprise in addition to E1's cloud services and **E5** adds PowerBI as a cloud service, along with several security features (see [chapter 12](#)).

Here's [the page](#) comparing these plans.

[This page](#) covers all the plans, including tailored versions for Education, Government and country specific flavors for China and Germany.

The most important point is that the different SKUs within each family aren't mutually exclusive. In a small manufacturing business, you may have the factory workers on Business Essentials, the office staff on Business and the executives on Business Premium and in a larger business, users could be spread across E1, E3 and E5 licenses.

[This page](#), called the Service Description, covers what the platform offers overall.

MICROSOFT 365

Building on top of the O365 plans above, M365 adds Windows 10 Enterprise, Endpoint Manager (Intune) and Azure Active Directory Premium.

For Business (up to 300 users) [there's are three options](#), **M365 Business Basic** which gives you Office (online only), email, file sharing, Teams and security features. **M365 Business Standard** adds the desktop version of Office “Microsoft 365 Apps for Business”, whereas **M365 Business Premium** adds iOS, Android and Windows 10 device management and policy enforcement from Intune plus many advanced security features. See more here <https://www.microsoft.com/en-us/microsoft-365/business#coreui-heading-hiatrep>.

On the [Enterprise](#) side there's **F3** (for “Frontline” workers, used to be called F1) which gives you Office (Online), Windows 10 Enterprise, Active Directory Premium P1, Azure Information Protection P1 and Intune on top of O365 E1. **E3** adds Active Directory Premium P1, Advanced Threat Analytics (ATA), Azure Information Protection P1, Windows 10 Enterprise and Intune on top of O365 E3. Finally, **E5** adds Active Directory Premium P2, Microsoft 365 Defender, Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Identity and Azure Information Protection P2, Windows 10 Enterprise, a host of security features and Intune on top of O365 E5.

It's tempting to think that “I'm a small business so I can save a few dollars with the Business SKUs” but you need to be aware of some limitations. Once you opt for the M365 Business plans you can't add phone system (PSTN) calling or Data Loss Prevention (DLP), eDiscovery and retention policies. Your OneDrive for Business is also limited to 1TB per user in Business, whereas in Enterprise you can increase this with a support call. Microsoft has made substantial changes to the Business Premium plan in 2020, and now includes all of the features of [Azure AD Premium Plan 1](#), so in addition to the security features already included (Conditional Access, self-service password reset and MFA),

this added cloud app discovery, Azure AD Application Proxy, dynamic groups and passwordless authentication, see [chapter 12](#).

Be aware that you can move licenses between different SKUs (both upgrade and downgrade) and that you can upgrade Business SKUs to Enterprise SKUs. This discussion has been around the full SKUs and what features they contain but it's also possible to purchase individual features such as just Azure Active Directory Premium P1 as a stand-alone feature for instance. Depending on the needs of (some) of the users in your business you can tailor an exact package with just the features they need.

A great way to understand all the different parts of O365, how they fit together, and a quick description of each service is [the periodic table of Office 365](#).

The take-away from this chapter is to not assume that if you're a small business you should automatically opt for the Business SKUs, investigate exactly what features will serve your business needs and don't be afraid to mix different SKUs for different worker roles.

CHAPTER 2 - MANAGING O365 AND M365

Once you have your tenant set up in M365 you'll need to manage it, in this chapter we'll show the different interfaces you can use.

If you don't have an O365 / M365 tenant please sign up for a trial tenant at <https://www.microsoft.com/en-us/microsoft-365/business/compare-more-office-365-for-business-plans> - simply click Try for free under E3 or E5. These trial tenants last for 30 days, although you can extend the trial for another 30 days by contacting support.

WEB PORTALS

For both O365 and M365 the main portal is admin.microsoft.com, which you can also reach from www.office.com, by clicking on the Admin tile. On the left-hand side are links to manage Users, Groups, Billing and Settings etc. and further down under Admin centers are links to the individual portals for Exchange, Teams, SharePoint, OneDrive and others. Depending on your SKU you will have slightly different links show up.

Highlights for day-to-day work include the ability to multi select users (Users - Active users) and change their licensing for instance. You can manage invited external users, that have had documents shared to them from OneDrive or SharePoint for instance under Users – Guest users. You can also restore a recently (30 days or less) deleted user.

You can manage Groups and Shared mailboxes, like “sales@mycompany.com” that is accessed by several different people and Resources such as Rooms and Equipment (booking conference rooms or company cars). Billing is the area where you can purchase additional licenses, manage your Subscriptions and Payment methods and Support is where you lodge service requests. Under Settings is an area where you can configure different Services and add-ins whereas Setup lets you manage your email Domains. Reports has both Usage and Security reports while Health has two important areas; Service health shows you if there are any problems in the cloud with your resources and Message center has a list of updates and changes that are coming.

Each individual Admin center lets you manage an individual service such as Azure Active Directory or Flow. [This site](#) has updated links for most of the different portals that you can access directly without going through the main portal.

POWERSHELL

For small tenants you’ll probably never have to venture beyond the web portal but if you have large amounts of users, you’re going to want to automate common tasks in PowerShell.

True to form, Microsoft had two ways of doing this, the now retired “MSol” or [MSOnline module](#) and the newer [Azure AD module](#).

To install the new module, in an elevated PowerShell window simply run:

```
Install-Module -Name AzureAD
```

To connect (and optionally authenticate with MFA) use:

```
Connect-AzureAD
```

To check that everything is working use:

Get-AzureADUser

Which will give you a list of the users in your tenant. Full instructions are [here](#), including if you need to connect to government or Chinese / German tenants.

```
Administrator: Windows PowerShell
PS C:\> connect-AzureAD

Account          Environment TenantId          TenantDomain      AccountType
-----          -
[redacted]        AzureCloud [redacted]        [redacted]        User

PS C:\> get-azureaduser

ObjectId          DisplayName          UserPrincipalName  UserType
-----          -
[redacted]        DE JONG, Frans      [redacted]          Guest
[redacted]        Kelvar Garth        [redacted]          Member
[redacted]        Marion Dresdner     [redacted]          Member
[redacted]        Paul Schnackenburg [redacted]          Guest
[redacted]        Paul1                [redacted]          Guest
[redacted]        DAMETTO, Piero     [redacted]          Guest
[redacted]        Ranjana Jain        [redacted]          Guest
[redacted]        Veeam Backup        [redacted]          Member
```

Connecting with PowerShell

Once you're connected there are many tasks that you may want to do and perhaps automate such and [managing user accounts and licensing](#), [creating SharePoint sites and managing users and groups](#), [configuring Exchange settings](#), [managing email migrations](#) (Chapter 3) and setting [Skype for Business information](#). Note that several of these require additional modules to be installed.

Microsoft has [finally documented](#) an official, scripted way to run a single PowerShell session connected to all the different services, whether you're using MFA ([Chapter 5](#)) or not.

For SharePoint (both Online and On-premises 2013/2016/2019) there's an open source alternative / complement to the official SharePoint module by the Patterns and Practices (PnP) team, you can find it [here](#). The official SharePoint online cmdlets are focused on creating / managing sites and users whereas the PnP cmdlets are useful for working with artifacts inside sites that have already been created.

If you need to manage M365 tenant settings or SharePoint Framework (SPFX) extensions, have a look at [CLI for Microsoft 365](#), also by the PnP team, which [runs on Windows, macOS, Linux](#). And if you can't be bothered installing CLI on your box you can now [run it directly in Azure Cloud Shell](#).

CHAPTER 3 - MIGRATING TO O365

If you're a new business this chapter doesn't apply to you – simply create user accounts in the cloud, join your Windows 10 devices to AAD and manage your iOS and Android devices with Endpoint Manager and you're good to go.

MIGRATION

Most businesses however have investments in existing technology on-premises and need to [migrate to O365](#). This chapter will cover your different options:

- Cutover migration
- Staged migration
- Express hybrid migration
- Minimal hybrid migration
- Hybrid migration
- PST-based migration
- IMAP migration
- Third party tools

If you don't have Exchange on-premises, i.e. you're using [Lotus Notes](#) / Domino, another email system, [Google Workspace](#) or another cloud email solution you're looking at either an IMAP migration or third-party migration services.

Most of the other migration methods rely on directory synchronization where your on-premises AD accounts are synched to Azure AD, which we'll cover in [chapter 4](#).

If you're still on Exchange 2003, 2007 or 2010 (which are no longer supported releases) a **Staged** setup allows you [to migrate mailboxes in batches](#), once you've configured directory synchronization. Be aware that you'll need to manually reconfigure each user's Outlook profile to point to O365 when their mailbox has been migrated.

For smaller environments the **Cutover** approach is the easiest. Microsoft talks about [this method](#) for less than 2000 mailboxes (Exchange 2003+) but in the real world it's probably appropriate for 100-150 mailboxes or so, depending on internet bandwidth. The idea is that you move everyone's mailbox from on-premises to the cloud over a weekend or other appropriate downtime.

If you're on Exchange 2010+ and your plan is to move all mailboxes to the cloud over a few weeks, consider the **Express hybrid** option. If you're larger and are looking at a few months of migration time, look at the **Minimal hybrid** alternative. If you have a larger environment (Exchange 2010+) and you expect to be in a hybrid state for an extended period of time and you need the ability to move mailboxes from the cloud back to on-premises (offboarding) consider **Full Hybrid**. For a full breakdown of the different flavors of hybrid see [here](#). The various types of hybrid [provide rich co-existence](#) with a unified Global Address list, sharing of Free/busy calendaring information and mailbox moves that are seamless for end-users, when their mailbox has been moved, they're just prompted to restart Outlook.

On-premises Exchange Server Organization

Office 365 Worldwide
BOOK2PS - BOOK2PS\pauls
17.0.5785.0

- Detect the optimal Exchange server
- Specify a server running Exchange 2010, 2013 or 2016

Exchange Hybrid setup requires a connection to an Exchange 2010, 2013 or 2016 server in your environment to perform management tasks. On Exchange 2010 or 2013 this must be a server running the Client Access Server role.

Client Access server:

Office 365 Exchange Online

My Office 365 organization is hosted by:

Office 365 Worldwide

- Office 365 Worldwide
- Office 365 Worldwide (Legacy Login)
- Office 365 China
- Office 365 Germany
- Office 365 Germany (Legacy Login)
- Office 365 U.S. Government GCC High
- Office 365 U.S. Government DoD
- Office 365 Airgap

Hybrid Configuration Wizard

[Microsoft's documentation](#) will point you to the [mail migration advisor](#), which may lead you on to the Hybrid Configuration Wizard (HCW), depending on your choices in the advisor. HCW will step you through the individual steps you must take, depending on the route you're taking, including the hybrid flavors as well as Staged and Cutover.

[IMAP migrations](#) lets you move from non-Exchange systems that support IMAP with a limit of 500,000 objects per mailbox and a maximum email size of 35 MB.

If you have PST files with email on premises you [can migrate them to Office 365](#), there's even a PST Collection tool to track them down on your network and collect them. If you have lots of them you can even [ship them on disks to Microsoft](#).

Once you have completed your migration, you'll need to consider your [Mail Exchanger \(MX\) DNS record](#) which will have been pointing to your on-premises mail server and now needs to be changed to point to Exchange Online instead. You also need to revisit your [Autodiscover DNS records](#) which is how Outlook and other email clients find the right Exchange server automatically.

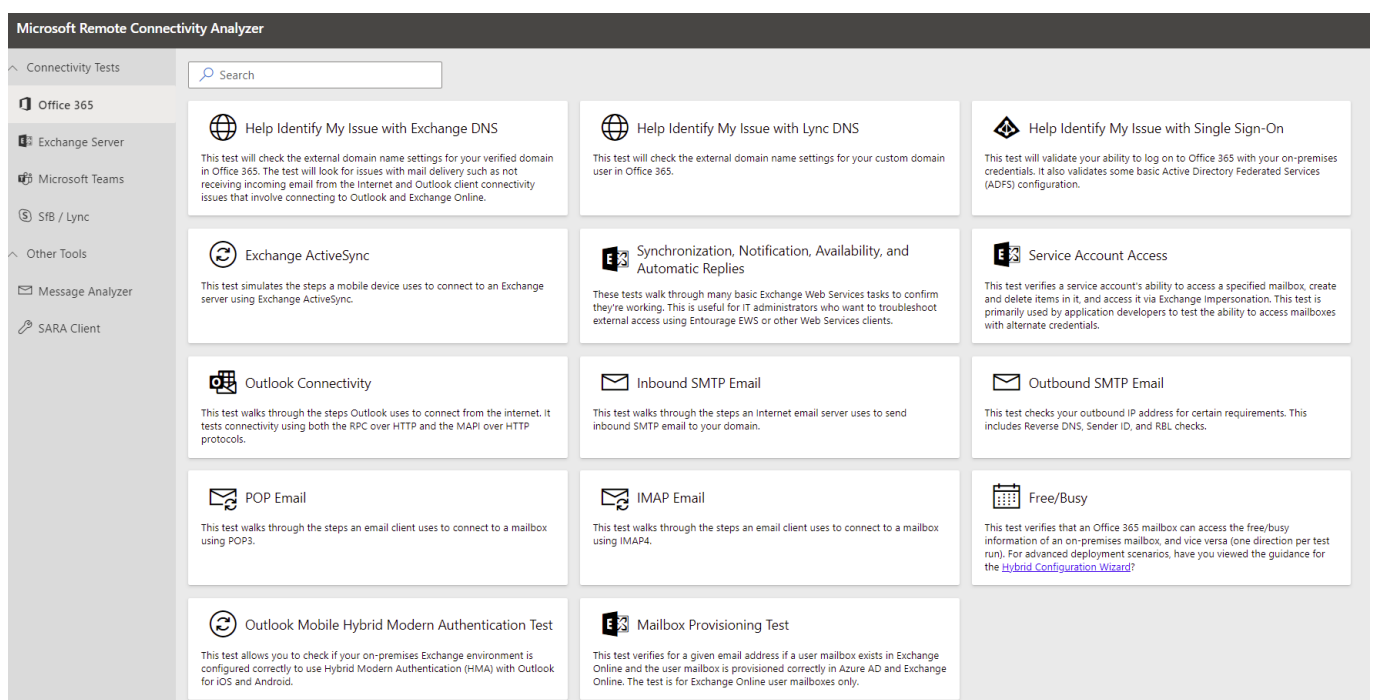
CHAPTER 4 - SUPPORTING M365

A big challenge for us in IT is the loss of control that the cloud brings. If you have a problem on-premises with email delivery you can check every part of the chain to see where the problem lies. Once you have migrated to M365 it's now a shared responsibility between you and Microsoft. In this chapter we'll look at two self-help tools that I use when there's trouble and then look at how you open and work a support case with Microsoft.

TEST CONNECTIVITY

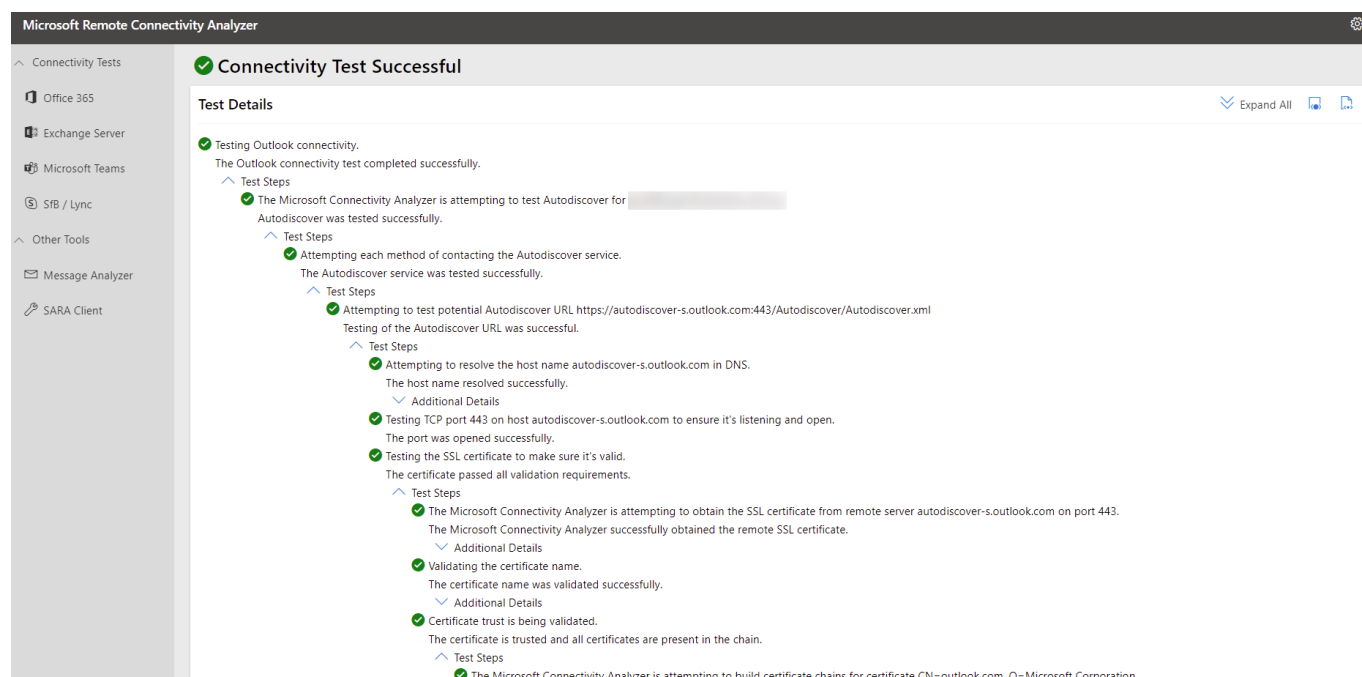
For email and Teams connectivity is a common cause of issues. Microsoft offers a useful tool;

Microsoft Remote Connectivity Analyzer (MRCA or RCA) at <https://testconnectivity.microsoft.com/>.



Remote Connectivity Analyzer

Here you can test several things: DNS entries, ActiveSync connectivity to Exchange, Outlook and Outlook Autodiscover functionality and both inbound and outbound SMTP email etc. Pick the test you need to perform and enter the required information. Depending on the test you may need to enter a valid username and password – I suggest resetting the password of this account after you've completed the troubleshooting. The Captcha verification lasts for 30 minutes so if you're doing several runs as you change values you don't have to verify that you're a human every time.

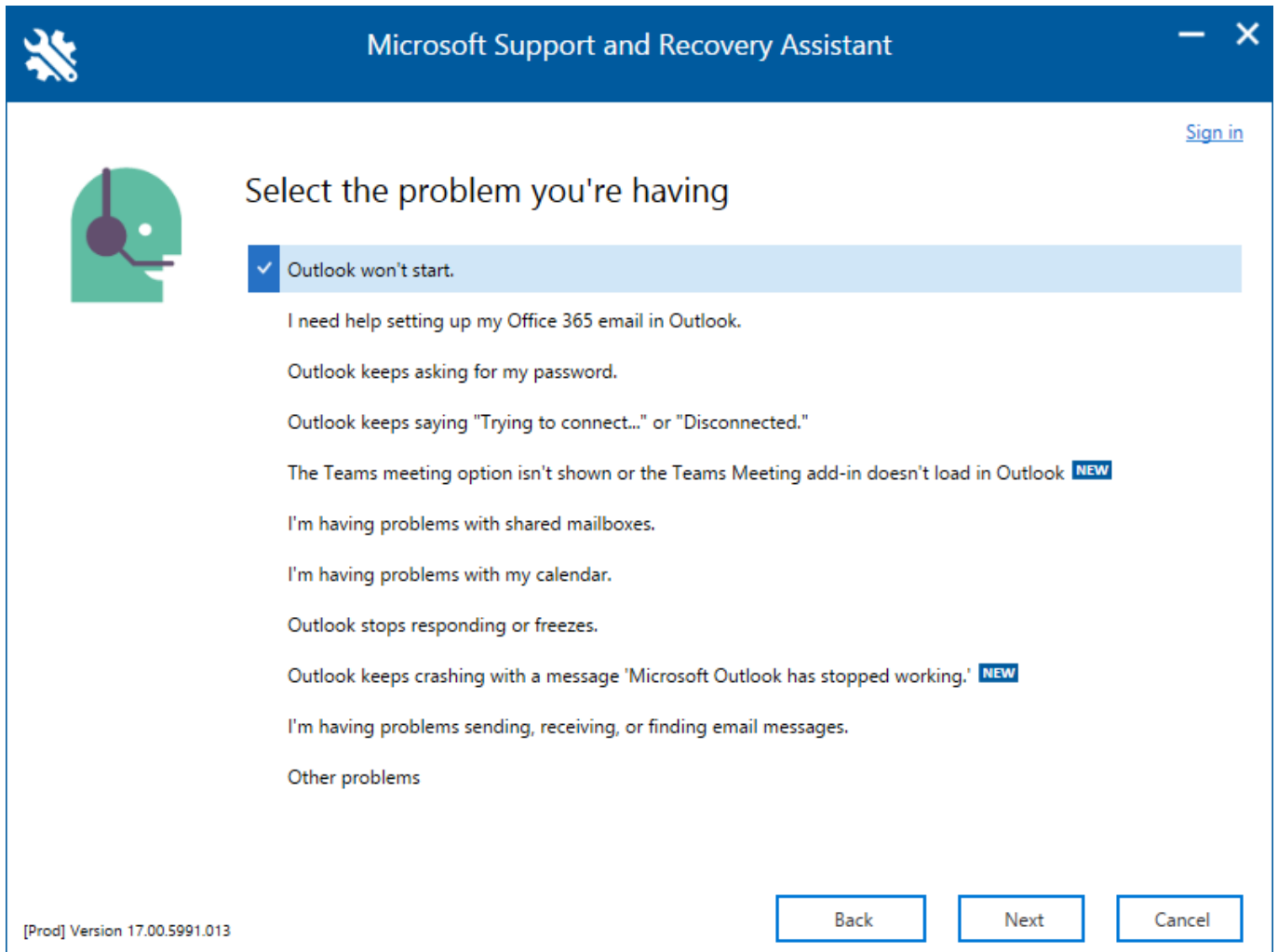


Connectivity test report

The test output is comprehensive and should help you pinpoint the issue quite quickly.

CLIENT-SIDE TOOLS

If the issue isn't connectivity related and instead you suspect an issue on a particular client device you should use [the Support and Recovery Assistant for Office 365 \(SARA\)](#) which will help identify Outlook, Dynamics 365 and OneDrive for Business issues as well as Apps for enterprise problems. It's a simple download which you run on the affected device; it steps you through a few questions to track down the problem.



Support and Recovery Assistant

In my experience when you're struggling with profile or intermittent connection issues (that aren't due to a service side misconfiguration – see RCA) SARA is pretty good at tracking down the cause.

Another recent addition to help end users help themselves are the [My Sign-ins](#), [My groups](#) and [My Access](#) sites, which along with [My Applications](#) gives users a good way to manage their access of M365 services. My Sign-ins is also an excellent education tool as it lists both successful logins and failed ones from attackers, here's a list of what my account looks like on a typical day (MFA is enabled on this account):

Time	Location	App	Status
Today at 10:08:08 AM AEST	Oklahoma, US	Office 365 Exchange Online	Unsuccessful sign-in
Today at 7:55:02 AM AEST	Lima Province, PE	Office 365 Exchange Online	Unsuccessful sign-in
Today at 5:37:42 AM AEST	Rio Grande Do Sul, BR	Office 365 Exchange Online	Unsuccessful sign-in
Today at 5:36:22 AM AEST	Wisconsin, US	Office 365 Exchange Online	Unsuccessful sign-in
Today at 5:32:13 AM AEST	Rio De Janeiro, BR	Office 365 Exchange Online	Unsuccessful sign-in
Today at 4:29:59 AM AEST	Antioquia, CO	Office 365 Exchange Online	Unsuccessful sign-in
Today at 2:39:42 AM AEST	Bahia, BR	Office 365 Exchange Online	Unsuccessful sign-in
Today at 12:08:29 AM AEST	Kyiv Misto, UA	Office 365 Exchange Online	Unsuccessful sign-in

My Sign-Ins with attackers' login attempts

SERVICE REQUESTS

When you have exhausted the self-service options, click on the “Need help?” button in the lower right-hand corner of the portal. Start by entering a description of your issue which might give you some results for common issues and their solution. Once you hit enter the Contact support option at the bottom lights up. Enter your contact information and preference between phone and email. You can also attach screenshots or log files (up to five, each less than 25 MB), pick a time-zone and a language for the communication.

In my experience the support for O365 is very good and generally tracks down the problem a lot faster than I would on my own searching forums and trying different solutions.

Behind the scenes – in the rare case that the support engineer needs access to a server that hosts your data, they use a “lockbox system” where they apply for access and a supervisor approves the request for a limited time. If you’re on O365 / M365 E5 you may have turned on [Customer Lockbox](#), which will involve you in that process and you have to approve the request as well.

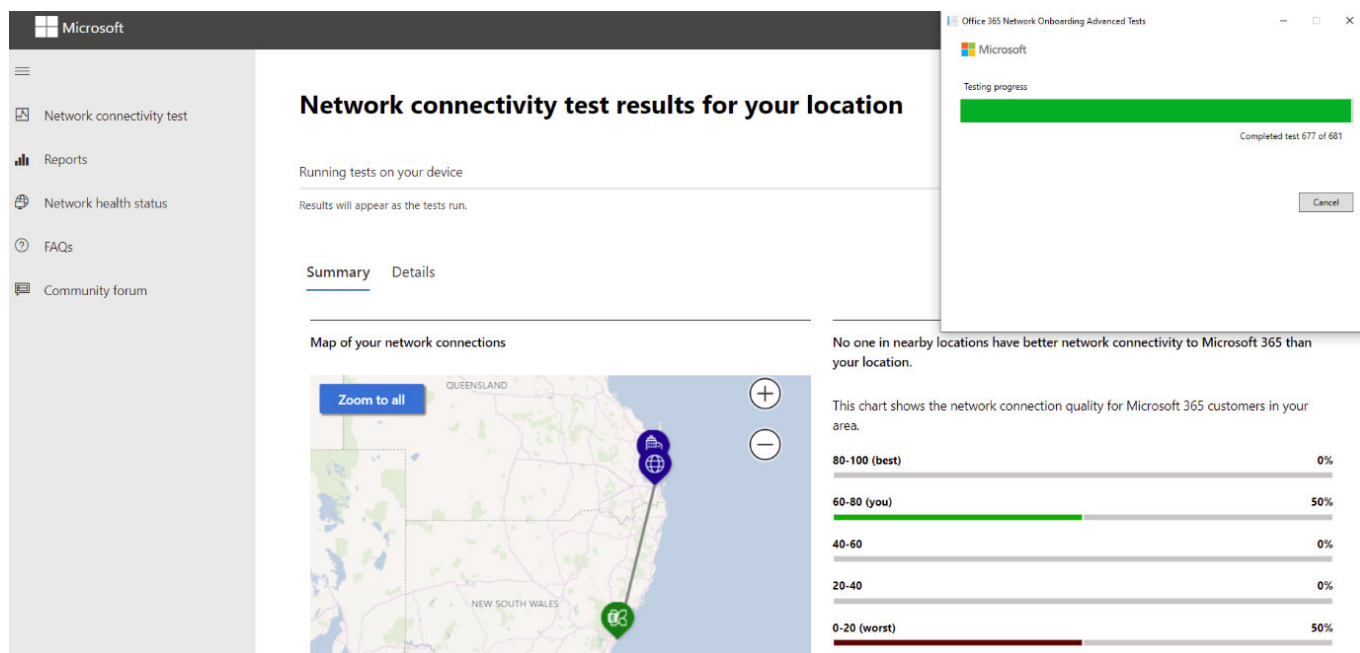
If on the other hand the problem is located on your end the support engineers can use a remote desktop client (that you install) to connect to your server or client PC in a view only mode and work through the issue with you.

SERVICE HEALTH

The Health section of the admin center provides overall health of the different services in M365 and if there are any outages / incidents affecting your tenant, provided you can access the portal.

If the outage is affecting the portal or the health portion of it, try <https://status.office365.com/> and follow [@Office365Health](#) and [@MSFT365Status](#) on Twitter.

The Health section also offers an interesting new tool called [Network connectivity](#) which uses the OD4B client, together with the Windows Location Service and optional manual data gathering tests to identify each client's [connectivity quality to Office 365](#). It's even got its [own portal](#).



Manual Network Connectivity test to Office 365

NETWORK CONNECTIVITY

Many businesses provide a substandard experience for their users by forcing them to use VPN connections back to the office and then onwards to Office 365 (overall a slower experience but a killer for Team's voice and video calls) or even proxying all outgoing traffic for "security". This last one is based in the erroneous assumption that all webservices / internet sites are "bad", and all traffic must be inspected, rather than differentiating between business services provided by Microsoft and others that can be trusted and dodgy websites and handling the traffic accordingly. Here's [an excellent article](#) outlining required and optional optimization techniques for M365. Microsoft has also partnered with many ISPs, internet exchange partners (IXPs), and software-defined cloud interconnect (SDCI) providers for optimal connectivity to M365, Dynamics 365 and Azure using [the Azure Peering service](#).

If your business is using a Software Defined WAN (SD-WAN) there's a preview feature called [informed network routing](#) that will further help optimize your connectivity by enabling data sharing between Microsoft and the SD-WAN provider to automatically reroute traffic where appropriate. Today only Cisco's IOS XE SD-WAN is supported but expect others to be added as the preview progresses.

The new [Productivity Score](#) is designed to help you understand where your business is at in its digital transformation journey and tracks metrics across two categories, People experiences and Technology experiences.

MICROSOFT 365 DESIRED STATE CONFIGURATION

PowerShell has long had a feature called Desired State Configuration (DSC) – define how a system (VM, Application etc.) should look, apply the policy and the Local Configuration Manager ensures that the system have the right settings, checking periodically for drift. This is called Infrastructure as Code and is [now available for M365](#) so you could have a test tenant where you evaluate new configurations and settings which you can then export and apply to your production tenant. It can also be used to export all your configurations as a "backup", periodically reporting on changes in configuration and compare your tenant's settings with best practices.

CHAPTER 5 - AZURE ACTIVE DIRECTORY

Behind O365 lies a directory which holds user accounts, groups and other security objects.

While they have similar names, Azure Active Directory (AAD) is very different to AD on premises.

In this chapter we'll look at AAD and how you interact with it for O365.

MEET AAD & HYBRID IDENTITY

AD uses Kerberos and Group Policy, has a hierarchical structure and is based on LDAP, none of which are cloud friendly. AAD operates over HTTPS, can be accessed from a REST API and supports modern authentication protocols such as Security Assertion Markup Language (SAML), WS-Federation and OpenID Connect for authentication and OAuth for authorization. It also supports federation so you can connect it to other authentication systems.

There are three types of authentication supported in AAD: **Cloud based**, **Directory synchronization** and **Single Sign On (SSO) with AD FS**. The first one is appropriate when you don't have AD on premises (or you want to retire it) and you create accounts in the cloud only. It's definitely the one with the simplest set up. The other two require you to link your on-premises AD to your AAD tenant through the free [AAD Connect](#) tool.

AAD CONNECT - YOUR UMBILICAL CORD

AAD Connect has had several predecessors over the years with different names – if you find an installation using DirSync or AAD Sync make sure to upgrade to AAD Connect as those tools are no longer supported.

AAD Connect [supports connecting multiple on-premises directories to AAD](#).

You can install the tool directly on a DC or on a member server. There's no true active / active HA option but you can set up a second installation of [AAD Connect](#) on a separate server in [Staging mode](#) and do a manual failover if the primary server is going to be offline for some time.

AAD Connect will synchronize user and group accounts in OUs you select (or the entire directory – not recommended) to AAD. You then assign licenses to those user accounts and they can start using cloud services. Note that this also means that on-premises is always the place to create new accounts, and update, disable or delete existing ones.

There are a [few choices](#) in how you handle passwords in AD. The simplest one is to use **Password Hash Synchronization** which takes on-premises password hashes, hashes them again with a modern algorithm and stores the hash of the hash in the cloud. This gives your users SSO (even though technically it's "same sign in" as the two user accounts are in two different directories). Another benefit of this method is that Microsoft can alert you when they find credentials on the web / dark web with accounts from your tenant where the passwords match.

If you're adamant that your user's passwords can't be stored in the cloud ([not even a hash of a hash](#)), **Pass-through authentication (PTA)** is another option. You [set up agents](#) on several (minimum 3, maximum 40) Windows Server 2012 R2+ servers (no inbound ports required) and when a user signs in at [www.office.com](#) for instance, AAD will verify that the correct password is given by communicating with your AD on-premises through the PTA agents.

Both PTA and Password hash sync optionally lets you enable [Seamless Single Sign On](#) (Seamless SSO) where the user logs on to AD and when they access [www.office.com](#) they're automatically logged in.

The traditional way of not storing password hashes in the cloud is to use **AD Federation Services (ADFS)**. This is [much more complex and requires several servers](#) to be set up on-premises (or as VMs in Azure) but does offer more flexibility. If your organization has already deployed AD FS for other purposes, setting up federation with O365 is not a huge project but my (and Microsoft's) recommendation is to stick with PTA or Password Hash Sync. Given the recent Solarwinds supply chain breach and subsequent intrusion into various organizations using ADFS, along with Microsoft's recommendation over the last few years to migrate from ADFS to Azure AD, if you have ADFS deployed, it's [time to make the move](#).

A new feature is [AAD Connect Cloud Sync](#), which was known as Cloud Provisioning during the preview. Today you'd mostly use this if your main organization is synchronizing using AAD Connect but you acquire other businesses with separate AD forests and you want their AD accounts to be synchronized to your AAD tenant. AAD Connect Cloud Sync relies on simple agents that are installed on-premises and all the configuration is performed in the cloud, in contrast to AAD Connect where all the configuration is managed on-premises. I expect Cloud Sync to eventually replace AAD Connect.

AZURE MFA

One of the best things that AAD unlocks is the easy set-up of Multi Factor Authentication (MFA) for logins. Passwords are one of the weakest links in today's IT landscape and the majority of the breaches we see are due to someone's credentials being compromised. One solution to this problem is using MFA (sometimes known as 2FA or two step authentication) where authentication not only requires a username and password but also a device or a biometric gesture to be present. This drastically reduces (by 99.9% according to Microsoft) the success of credential attacks.

MFA can call your phone, send a text message with a code, or send a notification / require a code from the free [Microsoft Authenticator app](#). Unless absolutely required, do not use phone call or SMS, they're more insecure than the app options.

As a baseline all your privileged accounts (Global / Exchange / SharePoint / Compliance administrators etc.) MUST use MFA. [This is free at all tiers of O365](#) and is [simple to set up](#) and the user experience is relatively seamless if you install the app on your smartphone. If you're an IT decision maker, expect to receive pushback from your administrators on this point but to maintain an acceptable security posture, this step is non-negotiable – all administrators HAVE TO use MFA. As an aside I've been using Azure MFA for my own business tenant and all my client's tenants that I administer for several years now.

You must however plan for times [when Azure MFA is unavailable](#) and this includes creating one (preferably two) Global Admin cloud accounts that are exempt from MFA and any CA policies.

These accounts should have very long and complex passwords that are only available to high-ranking administrators and should have monitoring enabled so that if they're ever used alerts go off. These break glass / emergency access accounts should only be used to recover user access, for instance if AAD MFA is down you might disable MFA requirements for the duration of the outage to enable users to login and be productive.

Enabling MFA for your end users requires some planning and end user training. The level of tech familiarity your users have and whether they're normally working from corporate offices influences how to implement MFA. Administrators always get MFA for free, if you're on the Business SKUs MFA is built in but both lack the advanced features that AAD Premium P1 (M365 E3) or AAD Premium P2 (M365 E5) offer. These include One-time bypass, MFA for on-premises applications Trusted IPs/[Named locations](#); which lets you define corporate office IP address ranges where users will not be prompted for MFA. Note that all MFA levels lets you (if you allow this feature) remember MFA on a trusted device

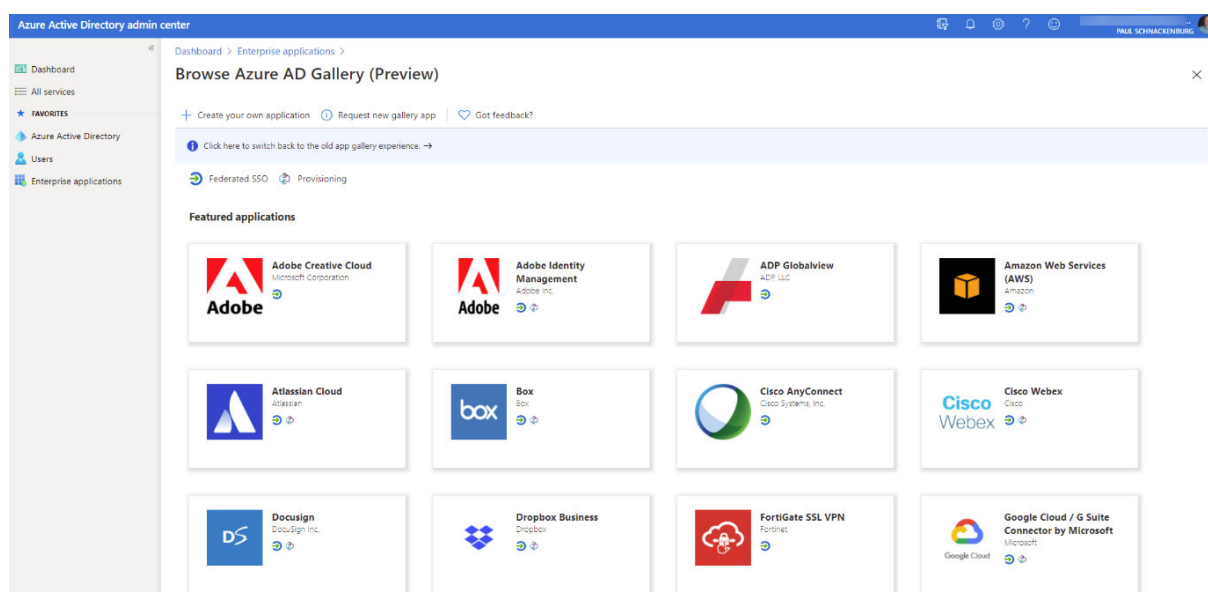
for a set number of days (7-60). If a user has logged on to a device and successfully performed MFA, they won't be prompted on that device for the time period and if the device is lost or stolen either the user or you can "un-trust" these devices easily.

Recently Microsoft enabled [Security Defaults](#) for new tenants, and you [can enable it manually](#) for your existing tenants. This will enforce MFA for all users and administrators, using the Microsoft Authenticator app only, blocks legacy authentication (see [chapter 13](#)) and controls access to the Azure AD portal. While these security enforcements are a good starting point for a small business with limited requirements, I advise caution for more complex organizations, as there's no way to exclude break glass accounts or service accounts from MFA, or ways to handle users who don't have / can't access the authenticator app on a phone.

If you want to analyze your user's MFA configuration for improvement, you can get a script [here](#).

PUBLISHING APPLICATIONS

One of the most powerful features of AAD is the ability to [publish applications](#) (third party and [on-premises](#)) to your end users. These show up right next to the normal Office applications at myapplications.microsoft.com or www.office.com for users to launch with a single click.



Publishing Applications using AAD

Take a corporate Twitter account for instance where several users have the username and password to send tweets on behalf of the company. Not only will you need to reset the password as soon as someone leaves the company (you don't want them tweeting after they've been fired) but you have little control over who else that password is shared with. If you publish Twitter through AAD and create an AD group to put users in that should have access, you simply add a user account to that group, they'll automatically have single-sign-on access to Twitter in the My Apps portal without ever knowing the password and once they leave the company and their account is disabled, they can't access it any longer. For some out of the 3700+ applications supported out of the box you can even configure [automatic provisioning](#) so that when you add a user to the AD Salesforce group an account is automatically created for them in Salesforce – again without them even knowing the password to it.

Recently added is the AWS Single Sign-On app [making short work of integrating AAD and AWS](#).

PREMIUM FEATURES

AAD P1 doesn't just unlock more MFA features, it also allows you to [ban commonly used passwords](#) in your on-premises AD (including [custom passwords](#)), enable users to [reset their own passwords](#) when they have forgotten them, integrate [MFA with Conditional Access](#) and let users register for both MFA and self-service password reset (SSPR) in [the same experience](#).

The P2 level adds the full experience of AAD Identity Protection where you get [reports and can block authentications](#) based on the risk level of the user account and the sign in or even trigger an [“extra” MFA prompt](#) based on the risk profile of the authentication attempt. P2 also offers [Privileged Identity Management \(PIM\)](#) where you convert all administrative accounts to eligible accounts and users have to request elevation when they need to perform administrative tasks (known as “Just in Time administration”).

Instead of assigning administrative roles in AAD to individual user accounts you can [now use groups to grant admin access](#). The groups need to have a specific attribute set (isAssignableToRole) to true and static (rather than dynamic – automatically assigning user accounts to a group based on an attribute like “department” in the directory) user account membership.

Where AD has a hierarchical structure, relying on Organizational Units (OUs) to structure your user, machine and group accounts based on department, geography or other approach, AAD is a flat structure. [Administrative Units \(AUs\) are new feature](#) that aims to change this, using AUs you can structure user and group accounts and then [delegate administrative permissions](#) to a single AU or AUs. The AU admins need AAD Premium licensing. Note that unlike OUs where an account can only be in a single OU, a group or user account can be a member of multiple AUs (up to 30).

If you have a large environment and Premium P2 licenses, consider using [entitlement management](#), a way to group application, group membership (including Teams) and site access into a single access package. These are useful for internal users (“you are the new person in Marketing – here’s your package that gives you all the access you need”) and can also be used to grant access to external users. For particular partner organizations that you work with frequently you can even set it up so that their users can apply for packages, self-service style. Entitlement management can also get IT out of the role of assigning permissions by delegating package assignment to business users.

CONDITIONAL ACCESS POLICIES

Both P1 and P2 unlocks another powerful feature in AAD, [Conditional Access \(CA\)](#). This lets you build policies around application access (both cloud and on-premises applications) based on the user account and what groups they’re a member of, which application they’re accessing, the state of their device, their location, the sign-in risk and which type of client application they’re accessing it from. These “if this – then do that” rules greatly enhance the security of your data by managing risk factors

affecting identity and access in M365. To make sure you don't create a policy that locks out the CEO 5 minutes before his board presentation by mistake, the new option to deploy CA policies in [Report-only mode](#) lets you evaluate the impact the policies will have without actually enforcing them.

Released at the end of 2020 is [the API for accessing CA policies](#). This makes it possible to backup (using PowerShell for example) your CA policies, restore them, monitor changes and treat them as code rather than manually manage them in the portal. You could also test policies in a test tenant before exporting them from there and importing them in your production tenant after they pass validation.

MANAGING THE ACCOUNT LIFECYCLE

Once you implement AAD Connect make sure you update your process documentation to take into account the full lifecycle of user accounts, such as making sure they're given the right licenses, are added to the right groups, and when it comes time to disable the account [the right steps](#) are followed.

To make sure that users (and guests) don't accumulate access that they no longer need, use [Access Reviews](#) (Premium P2) which now lets you review all guest accounts in one operation, rather than on a per Team/M365 Group basis.

For a smaller O365 or M365 tenant chances are you'll never even need to go to the full Azure AD portal and instead you'll just do your user management in the M365 portal ([Chapter 2](#)). It's a good idea however to explore the "full" AAD portal over at <https://aad.portal.azure.com>.

If you're keen to try out upcoming features in AAD, use the Preview hub to learn about and turn on public preview features.

Azure Active Directory admin center

Dashboard > PAUL SCHNACKENBURG

PAUL SCHNACKENBURG | Preview hub

Azure Active Directory

Save | Discard | Got feedback?

The following preview features are available for your evaluation. Help us make them better!

Search [Add filters](#)

Name	Category	Services	Type	State
Enhanced group management	Administration	Group management	Public	<input type="checkbox"/> Off
Assign cloud groups to built-in roles	Authorization	Role management	Public	
Integration assistant	App access	App registration	Public	
Switch tenant	Administration	Directory management	Public	
Unified tenant search	Administration	Directory management	Public	
Enhanced user management	Administration	User management	Public	<input checked="" type="checkbox"/> On
Enhanced searching and sorting for devices	Administration	Device Management	Public	<input type="checkbox"/> Off
Bulk download for devices	Administration	Device Management	Public	

Azure AD Preview hub

CHAPTER 6 – CLIENTS

There are many pieces of software you can use to connect to M365 – in this chapter we'll look at these and how you manage them from a governance point of view.

DESKTOP CHOICES

Microsoft recommends the latest version of Chrome, Edge, Firefox or Safari or Internet Explorer 11 for accessing O365.

If you have the rich Office desktop client installed all supported versions should work with O365 but using the Apps for enterprise version for both Windows and Mac that's included with Business Premium and E3+ is preferred. You can [control which users get the recommended Current Channel](#) and who gets the Monthly Enterprise channel or the Semi-Annual Enterprise Channel flavor.

If you want to live on the edge you can enroll in the [Office Insider program](#) to beta test new features.

Outlook Web App (OWA) or Outlook for the web deserves special mention as it's extremely capable and not a “watered down” version of Outlook that runs in a browser. In fact, Microsoft often tests new features and approaches in the web client because they can deploy changes much quicker.

You can use OWA policies to [control which features](#) are available to your end users.

You can control which protocols users can use to connect to Exchange with [Client Access Rules](#).

MOBILE CHOICES

For many years the preferred way of connecting to Exchange online for email was to use ActiveSync, a protocol that both the mail client in iOS and Android supports (sort of – not all features were supported by each vendor). Microsoft now recommends using the free Outlook client app which lets Microsoft introduce new features much faster, without having to wait for Apple or Google to catch up. This app has been steadily growing in capability, including the ability to connect to Gmail and other email services and is now used by well over 100 million people.

ONEDRIVE

There's a legacy client (Groove.exe) for syncing your OneDrive files, today it should only be used if you're connecting to on-premises OneDrive or SharePoint as it will eventually be deprecated.

The newer sync client is automatically installed when Apps for enterprise is installed and you can control its behavior using [this Group Policy template](#).

TEAMS

The Teams application ([chapter 10](#)) is Microsoft's all in one collaboration client with support for instant messaging chats, group chats, voice calls, video calls and if you have the licensing, PSTN calling to and from normal phones. Teams is replacing Skype for Business and starting in early 2019 the client is automatically installed when you install Apps for enterprise, if you need to deploy it using your favorite software deployment tool use this [MSI](#).

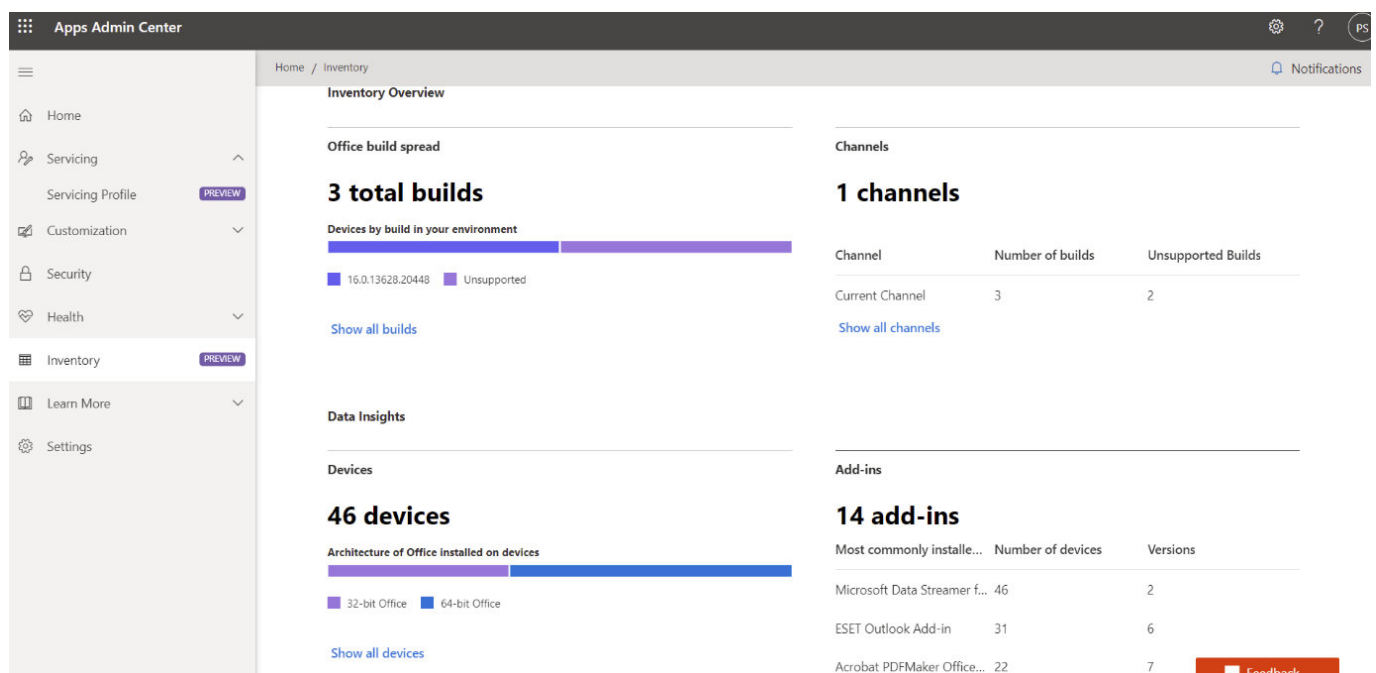
APPS ADMIN CENTER

[This site](#) is a very interesting take on cloud management for Apps for Enterprise (Office on the Windows desktop). Instead of managing the customization settings using the [Office Deployment Tool \(ODT\)](#)

you use the cloud portal to create the required XML files. The Apps Admin Center [does so much more](#) [however](#), it inventories your Office installations across your tenant, tracks with versions and build numbers are installed, which ones are out of support and lets you build Servicing Profiles to deploy newer versions of Office. It also uses Security Policy Advisor to analyze current usage of the apps and lets you create and deploy policy configurations to all Apps for Enterprise installations (without relying on GPOs or MDM) plus tracks which add-ins are in use across all your devices.

If you have a large amount of users, you may want to disable the option for users to download Apps for enterprise from www.office.com (M365 portal – Settings – Services & add-ins – Office software download settings) and instead distribute it using a file share. If your business is using System Center Configuration Manager, it can be used to [deploy and update Apps for enterprise](#).

Since there's no additional licensing required you should definitely investigate if the Apps Admin Center can make your life as an Office 365 administrator easier.



Apps Admin Center

If you need to provide a modern printing environment for your users without having to bother with print servers or installing individual drivers for each printer on each device, consider [Universal Print](#) [which recently became generally available](#).

CHAPTER 7 – EXCHANGE ONLINE

Email is the lifeblood of business communication, even in this age of Teams and Slack and numerous other communication tools. It's the lowest common denominator – the one tool that you can always use to reach someone if you've got their email address. And email is a commodity – every business needs it, but no business is going to be more competitive by running it “more efficiently” than another.

IT'S A HYBRID WORLD

One of the strengths of O365 over Google Workplace for instance is the clear migration path from what you have today to the cloud, because of Microsoft's large footprint in corporate datacenters around the world.

If you have Exchange 2013+ on-premises you can pick any of the migration methods we looked at in [chapter 3](#), some of which provide a hybrid co-existence. The full hybrid option lets you continue running your on-premises infrastructure for as long as you'd like and move mailboxes in batches to the cloud on your own schedule. You can even move mailboxes back to on-premises should the need arise. As you'd expect there are many details to manage in [a hybrid setup](#), including [prerequisites](#), [ActiveSync connectivity](#) and [mailbox permissions](#) – especially when a user on-premises has permissions to a mailbox in the cloud or vice versa.

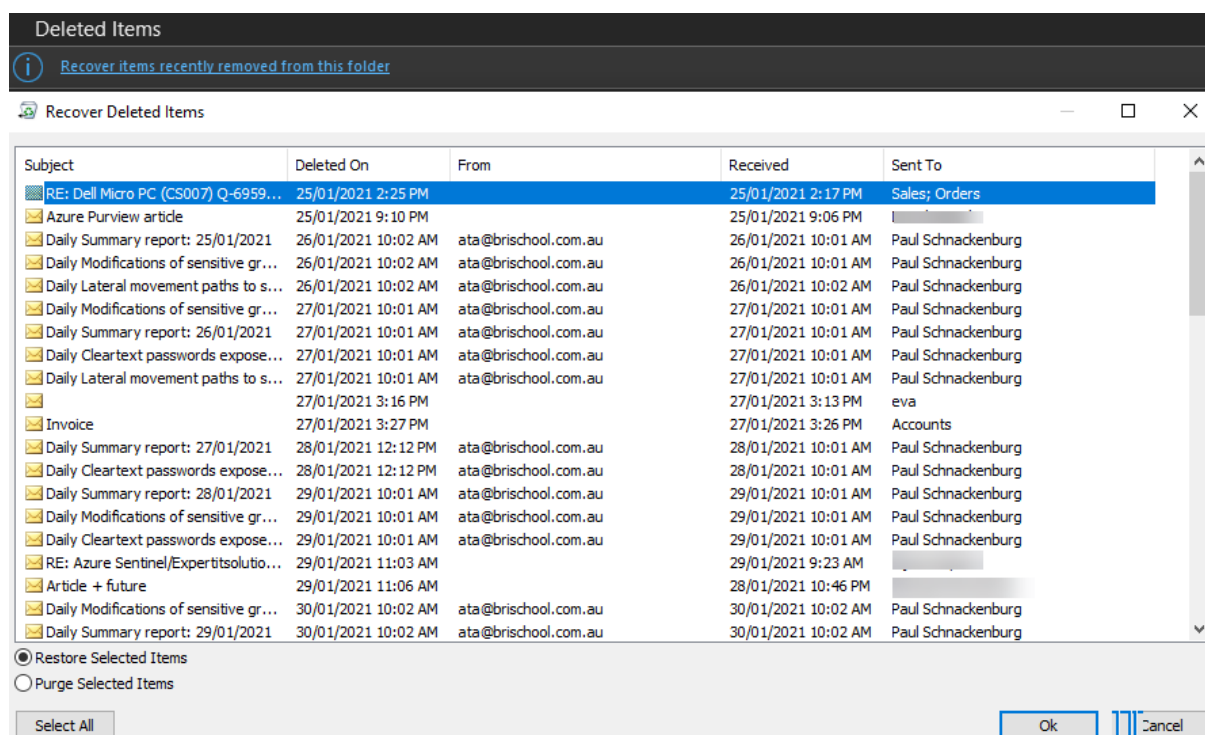
BACKUP AND NATIVE DATA PROTECTION

One thing to realize about O365 is that Microsoft is going to make sure that you don't lose your mailbox data which they do through the native data protection in Exchange – keeping three copies

of your mailbox data on separate servers, along with a “lagged copy” (behind in time, for instances where the data is corrupted rather than lost) on a fourth server.

They DON'T however keep backup copies of your data going back into the past which may or may not be an issue for your business, depending on your regulatory needs. There are several third-party services on the market which will do backups of your Exchange and SharePoint online data.

Altaro has a solution, both for [businesses](#) and for [Managed Service Providers](#) (MSPs).



Recover Deleted Items in Outlook

When you delete an item (email, calendar appointment, contact etc.) in Outlook it's moved to Deleted Items. If you then empty deleted items (or delete a particular item) it's still recoverable for up to 30 days by default (14 days for mailboxes created before 2017) – go to the Deleted items folder and click on the blue link “Recover items recently removed from this folder”. You can [increase this time period](#) up to 30 days.

Similarly a deleted user account and mailbox [can be recovered](#) if no more than 30 days have passed.

AUTODISCOVER

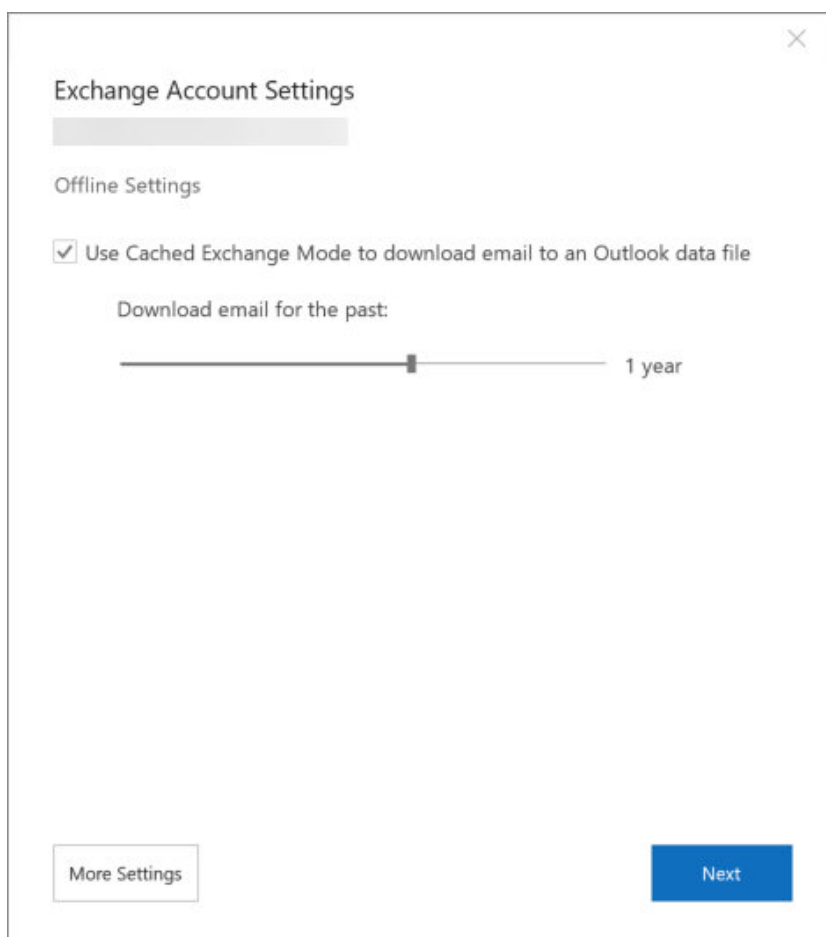
Whether your Exchange server is in the cloud or on-premises it's important that client applications can find it – this is the job of the Autodiscover records in DNS. There are a number of other DNS records required for O365 – find them in [this article](#).

If you have a hybrid Exchange deployment the Autodiscover records need to point to your on-premises Exchange 2010/2013 Client Access Server or your 2016/2019 Mailbox Server.

MANAGING MAILBOXES

There are many tasks associated with mailbox management, one of them is [quota management](#).

F3 licenses get 2 GB quotas, E1 are set at 50 GB (with a 50 GB archive) and E3+ have 100 GB quotas with unlimited archive mailboxes. The difference between a mailbox and an archive mailbox is that the archive is only available when you're online. You can control how much mailbox data is stored offline on each device with a slider in Outlook.



Outlook offline cache setting

If you're migrating large mailboxes to Office 365, ensure they're smaller than 100 GB and no item is larger than 150 MB before starting the move.

In the Exchange console you can configure settings for a mailbox such as adding email aliases, see quota usage, control which clients (OWA, Unified Messaging) and the protocols (EAS, MAPI, IMAP and POP) the user can use, message retention and mailbox delegation. This last option lets you configure other users to Send As emails this user, Send on Behalf where the recipient can see that the email is sent on behalf of the user and Full Access.

MAILBOX ARCHIVE

As mentioned earlier you can enable [an Archive mailbox](#) for mailbox content which essentially serves as a “bottomless” storage area for older content, hopefully stopping users from adopting PST files as an archiving solution. Note that archive folders are not available in Outlook when you're offline and also not in EAS mail clients. The Outlook mobile client (iOS and Android) also cannot access Archive mailboxes. You can enable [auto expanding archives for E3 and E5 licensed users](#) using PowerShell:

Set-OrganizationConfig -AutoExpandingArchive

You can also enable Archive mailboxes on a per user basis. Note that the Archive folder that's created in a mailbox when you right click an item and select archive isn't related to the Archive mailbox.

MAIL FORWARDING

Be aware that users can set up their mailboxes to forward mail to an external email address (optionally delivering to both inboxes). This is something you should keep an eye on because while there may be legitimate business reasons to forward mail, it's also a favored attack vector for hackers where they silently can monitor traffic and then use that for various nefarious purposes. There's a report

in the Mail Flow dashboard to show you what forwarding rules exist. You can also block [users from being able to forward mail](#) in several ways.

SHARED MAILBOXES

There are times when you'd like a mailbox that doesn't "belong" to a particular user such as sales@ or support@ where you have a team of users accessing the same alias. As long as [the Shared mailbox](#) doesn't have a larger quota than 50 GB or uses an Archive mailbox it won't consume a license.

It's also one option for handling staff that have left your company while you still need to monitor their email for incoming emails, converting their mailbox to a shared mailbox and assigning access to the appropriate staff will free up the license to be assigned to a new user. From a security point of view, make sure direct logins to shared mailboxes is blocked – users should only access shared mailboxes by adding them as an additional mailbox in Outlook.

MAIL CONTACTS AND USERS

Both Mail Contacts and Users show up in All contacts, the Global Address List (GAL) and the Offline Address Book (OAB). A contact is a pointer to an email address in an external system, whilst a user is also a pointer to an external address, but the user has O365 credentials to be able to access SharePoint Online or OneDrive for Business. The latter is a remnant of on-premises Exchange, modern external sharing such as Teams, Planner and others use [Azure Business to Business \(B2B\)](#) collaboration for guest access.

DISTRIBUTION LISTS

Grouping email addresses together to facilitate communication with teams of people is something that email systems have been doing for decades – in the Exchange Online Admin Center (EAC) you can create Distribution Lists (DL). Note that the default is to create [an O365 Group](#) instead and in fact [Microsoft is pushing to replace DLs with Groups](#). [Dynamic Groups](#) make maintaining membership easier, basing the membership on an AAD attribute such as "department" – if that's set to Marketing for instance, the user is automatically included in the right group.

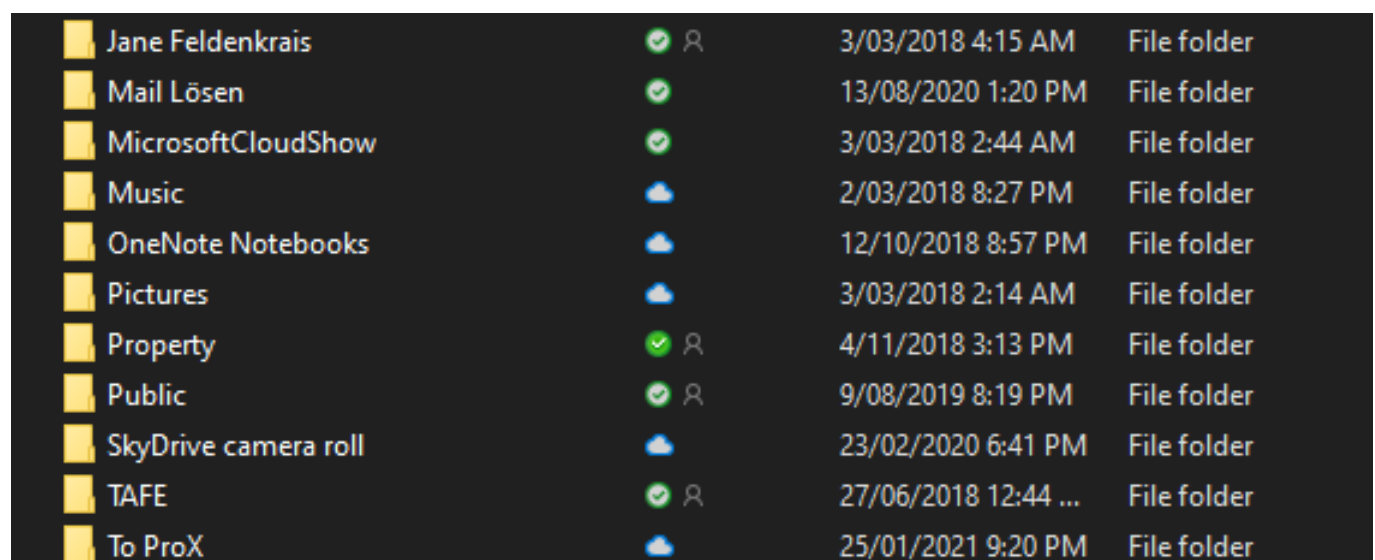
CHAPTER 8 – ONEDRIVE FOR BUSINESS AND SHAREPOINT

Sharing files and providing as intranet platform is a core part of O365, in this chapter we're looking at OneDrive for Business (OD4B) for personal file storage and sharing as well as web-based collaboration in SharePoint.

ONEDRIVE FOR BUSINESS

OD4B builds on SharePoint Online to provide each licensed user with their own document storage; 1TB for most SKUs. This quota [can be increased](#) for all users or individual users if the need arises.

Once you store files in OD4B you can access them from any device, through clients for Android, iOS, Windows, MacOS and a web interface. There are [some limitations](#) on file names, types and sizes to be aware of. The OD4B sync client lets you [see all files](#) on a device that you have synced, they can be in an **Online-only** state where you see them but they're not actually present on the device, when you open such a file it's downloaded and cached and thus **locally available**, a user can also pick one or more files to always keep on this device.



Jane Feldenkrais		3/03/2018 4:15 AM	File folder
Mail Lösen		13/08/2020 1:20 PM	File folder
MicrosoftCloudShow		3/03/2018 2:44 AM	File folder
Music		2/03/2018 8:27 PM	File folder
OneNote Notebooks		12/10/2018 8:57 PM	File folder
Pictures		3/03/2018 2:14 AM	File folder
Property		4/11/2018 3:13 PM	File folder
Public		9/08/2019 8:19 PM	File folder
SkyDrive camera roll		23/02/2020 6:41 PM	File folder
TAFE		27/06/2018 12:44 ...	File folder
To ProX		25/01/2021 9:20 PM	File folder

You can restrict synchronization to only [domain joined devices](#). To help users manage the contents of common folders you can use [Known Folder Move \(KFM\)](#) to synchronize the content of the Desktop, Documents and Pictures folders to OD4B and thus between devices.

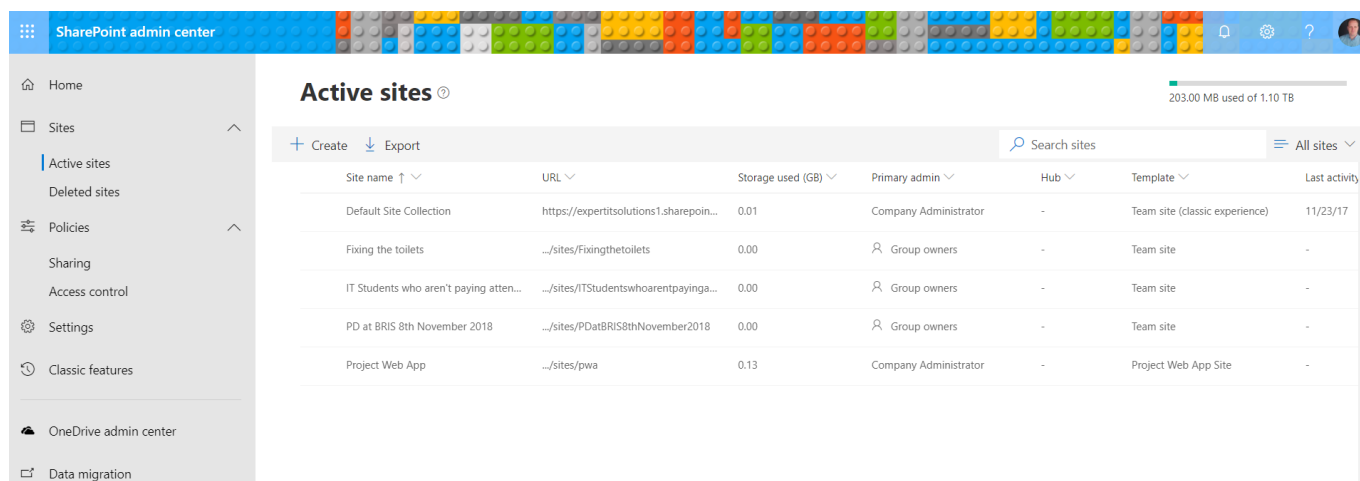
SHAREPOINT

If you're an on-premises SharePoint administrator, you'll be familiar with managing the underlying infrastructure of your servers as well as the complex web of sites and document workflows that end users consume on top of it. If you're only now meeting SharePoint in the cloud for the first time, you'll likely have a very different experience where you see SharePoint simply as the underlying document storage for other applications (Teams, Groups, Planner) and perhaps as the platform for your company's intranet.

Building blocks in SharePoint are **sites** where content is stored, and you can control the layout, theme, navigation and security with classic and modern flavors. If you're starting out or creating new sites, Modern sites are [the way to go](#) and there are a few different types available such as [Communication sites](#), [Team sites](#) and [Hub sites](#). Part of a larger vision for SharePoint, the modern sites and pages are very useful as they adapt to screen resolutions across smartphones and different size computer screens.

Search lets you find sites, files (including OneDrive for Business files), people and news content and if there are pictures in the content Artificial Intelligence (AI) will have extracted metadata and (if present) text content from those images. If you have configured [a hybrid deployment](#) your on-premises documents will show up in the search results as well. **Apps** are add-ins / Web parts that expand the functionality of sites and **Site collections** are a way to group sites with a similar purpose together.

[SharePoint Syntex](#) is a new technology that uses AI and ML to automate content processing and transforms content into knowledge. It understands your documents, processes forms and is applicable to large organizations with complex workflows and processes.



SharePoint Online Admin Center

Be aware of [the limits of SharePoint Online](#), particularly the total storage available which is 1 TB + 10 GB per license purchased. Search is an area that you want to [spend some time customizing](#) so your end users have a good experience. Sharing is another area that you want to control as [how users can share content](#) internally and (critically) externally directly influences the balance between collaboration and security.

Sharing

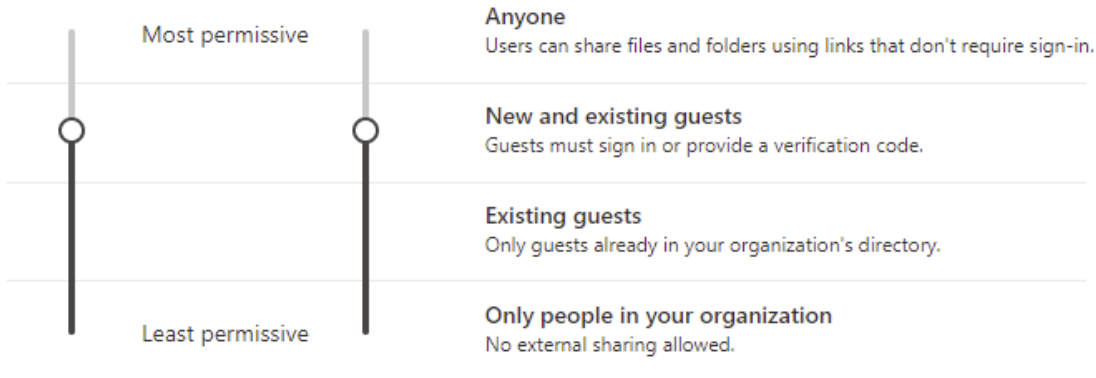
Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more](#)

External sharing

Content can be shared with:

 SharePoint

 OneDrive



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
- People who use a verification code must reauthenticate after this many days

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

SharePoint and OD4B external sharing control

Migrating content from on-premises SharePoint Server and network file shares to O365 is the job of [the SharePoint Migration Tool](#), as well as numerous third party services. If users accidentally delete files or ransomware has encrypted stored files you can use [the Restore Files](#) interface to restore files and folders or entire libraries from up to 30 days in the past. There's also [the Recycle bin](#) (93 days retention) for individual file restores and [Restore Files](#) for OneDrive.

CHAPTER 9 OFFICE 365 GROUPS

O365 Groups are a basic building block, in this chapter we'll look at the different uses of them.

GROUP TYPES

An area that often confuses new O365 administrators is [the different types of groups](#), here's a short rundown to sort it out:

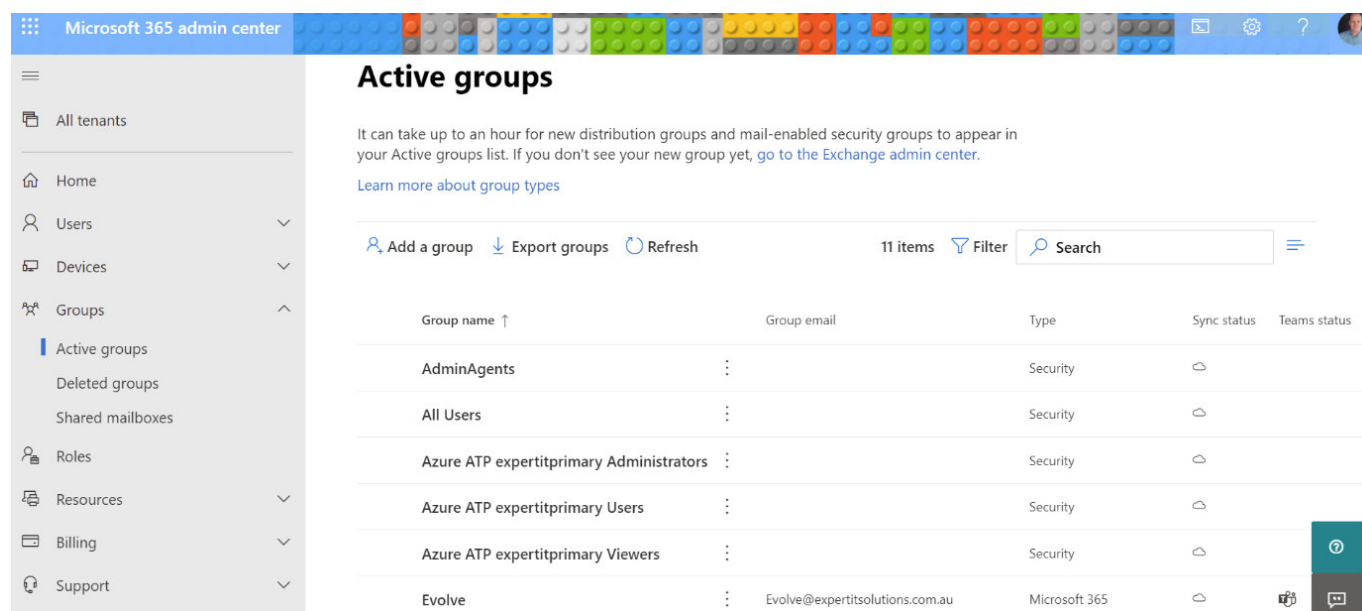
- **Office 365 Groups** (the type covered in this chapter)
- **Distribution Groups** ([Chapter 7](#))
- **Security Groups** are used to grant access to resources
- **Mail-enabled Security Groups** are also used to grant access and can also be emailed which will mean all members will receive a copy of the email
- **Shared Mailboxes** ([Chapter 7](#))

While you can create Office 365 Groups directly, you're more likely to interact with them as a building block, providing a single identity for all of O365, that services such as Teams, Yammer and others use.

In addition, Outlook can use O365 groups, SharePoint Modern Team sites are built on them, and Stream and PowerBI use them to control access.

If configured thus you can write O365 Groups back to your on-premises AD where they manifest as distribution groups. You can't nest O365 Groups into other groups, and they can only contain actual O365 user accounts whilst Exchange Distribution groups can contain user accounts, mail users and contacts (see [Chapter 7](#)). Unless you've changed the defaults, any user in your tenant can create

an O365 group which could [lead to governance issues](#). You can instead [designate users](#) who can create groups. You can also use various [policy settings](#) to control O365 Group behavior in your tenant, such as [expiration policies](#) to manage the lifecycle of groups and you can control [the naming of groups](#) through policy.



Groups in the M365 Admin Center

It's easy to [share content from within an O365 group](#) with external users and O365 groups are also a shared repository of historical content as anyone who is a member can see all the content going back to when the group was first created. Each licensed user in your tenant gives you five B2B [guest licenses](#), and you can use one time passcodes for external guests who don't have a Google, Microsoft Account (MSA) or an account in Azure AD. This licensing model for external users is changing, Microsoft is bringing together Azure B2B and B2C (using Azure as a store for Consumer identities for your in-house developed application) and the coming license model means each tenant can have up to 50,000 external users at no extra cost. Note that guests have full access to all group content by default. You can [control which domains](#) external users have to be (or can't be from) for external access.

Today when you create a group it's **private** where the Owners of the group must approve a request to join, you can also make a group **public** where anyone can join. You can change the tenant default which will ensure new groups are public or you can change the setting on a group after you've created it. Each group can have up to 100 owners and over 1000 users; an individual user cannot create more than 250 groups. Like other constructs in O365 you have 30 days to [restore a group](#) once it's been deleted while individual documents are housed in the SharePoint recycle bin for 93 days.

[Dynamic groups](#) are a neat way to reduce the administrative overhead of managing group membership manually, based on queries of AAD attributes, although be aware that it requires AAD Premium P1 licensing.

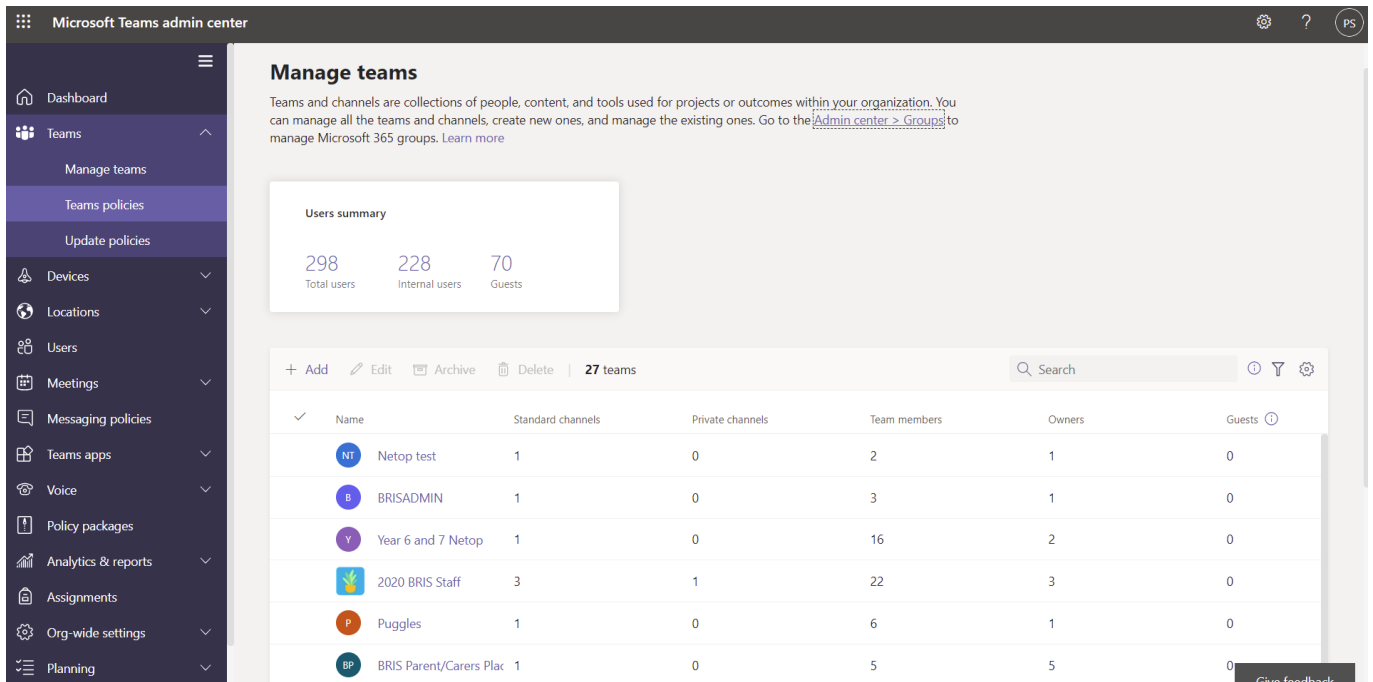
CHAPTER 10 – TEAMS

There has been many instant messaging / chat applications attempting to take on business communication and without a doubt Microsoft's Teams is the best yet. This is in no small part fueled by the Covid-19 pandemic which has seen Teams usage grow from 13 million daily active users in July 2019 to 115 million (!) in October 2020. In this chapter we'll see what Teams can do for your business communications and collaboration.

MEET TEAMS

A lot of development is going into Teams to make sure it's the best place for groups of people to work together, here's [the glossy vision](#). There's [a free version of Teams](#) (up to 300 users) as well as the version included in O365.

A Team [can have up to 10,000 users](#) but in my experience, it works best with smaller teams (up to a few hundred). If you're delivering a webinar style event with people listening, there's a 20,000 attendee limit. There are client applications for Windows, MacOS (both updated bi-weekly), iOS and Android as well as a web-based interface (updated weekly). Like many things in O365 there are two components to successful adoption, the technical side and the user training side.



Teams Admin Center

Note that Skype for Business Online, in some ways the predecessor to Teams, is being retired with a final date of July 31st, 2021. The on-premises Skype for Business server is not affected by this date.

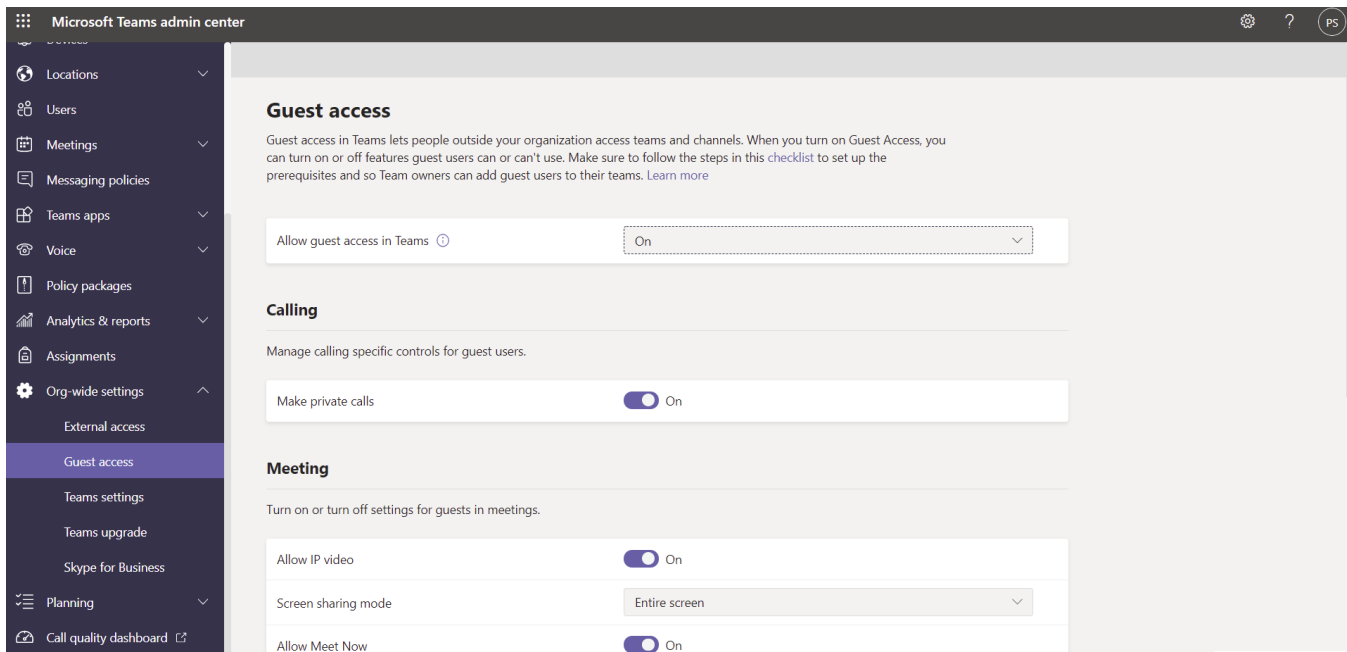
If you've deployed Skype for Business start [planning your migration](#).

If you have conference rooms, make sure you consider the technology you outfit them with, [Teams Rooms](#) are a powerful way to use technology to connect staff in the office with staff working from home.

MANAGING TEAMS

Your main interface is [the Teams portal](#), and there's [a PowerShell module](#) available. Underneath each Team is an O365 Group ([Chapter 9](#)) with the chat messages stored in Azure table storage, shared files in the Team's SharePoint library and personal files in each user's OD4B, voicemail and calendars are stored in user's Exchange mailboxes, and meeting recordings in Azure media services. If you're in a larger business, make sure to [plan for governance](#) of Teams early in your deployment. Visit your Tenant's Team's **Guest access settings** to make sure you have a good balance between security

and collaboration for your business. Another handy feature is the ability to use [templates for Teams creation](#), including creating your own custom templates.



Teams Guest Access settings

Each Team has a default General channel, and you can further create channels to organize communications, within each channel you can add tabs for Planner, OneNote, PowerBI, Stream, Wiki, websites and third-party apps. To limit the proliferation of Teams in your organization you can [limit who can create Teams](#) (by default all users can), as well as use [Private Channels in a Team](#). You could have a Team for the Sales department with a private channel for only sales managers to discuss confidential information for instance.

There's also the ability, called Teams Connect, to share a Channel with an external user, rather than sharing a whole Team. The main benefit for the invited user is that they can be in logged in with their own tenant account and access the shared channel chat and documents without the need to sign out and sign back into Teams using their guest account.

Delivering presentations using Teams is common, the new [PowerPoint Live feature](#) makes it more interactive by allowing attendees to interact with the presentation at their own pace and [Presenter mode](#) gives you more control over how your presentation delivery shows up for the audience.

The screenshot displays the Microsoft Store interface. On the left, there are filters for 'Categories' (ranging from AI + Machine Learning to Sales) and 'Industries' (ranging from Agriculture to Retail & Consumer Goods). At the top, there are filters for 'Trials', 'Pricing Model', and 'Ratings', all set to 'All'. The main content area features a large card for 'Microsoft Teams' with a 'Get Microsoft Teams >' button. Below this, a section titled 'App results (795)' shows a grid of add-in cards. Each card includes the app's icon, name, developer, a brief description, a star rating, and a 'Get it now' button. The add-ins shown are: Decisions (42 reviews), Zoom for Teams (34 reviews), Asana for Teams (3 reviews), Adobe Creative Cloud (9 reviews), MIPA - Your Personal Assistant (26 reviews), MindMeister - Mind Mapping for Teams, ClickUp, MURAL, Lucidchart Diagrams for Teams, and Azure Boards for Microsoft Teams.

Teams Third-Party Add-Ins

A great feature (celebrated by teachers everywhere who's been trying to deliver education through Teams during the pandemic) is [breakout rooms](#). This lets you send or ask users to pick “rooms” where they can collaborate with a subset of the users in a Team during a meeting, and then return back to the main meeting later.

Recordings of Teams meetings (including transcriptions) used to be stored in Stream, now [they're saved in OD4B / SharePoint](#) where they can be shared easily (including with external attendees).

If you're an SMB (up to 300 users) and you need audio conferencing (attendees calling into your meetings via phone, rather than receiving the audio via the network connection), there's [a free offer](#) available until September 2021.

USING TEAMS

If you're used to communicating via email here are some guidelines to be effective with Teams.

Use @ mentions to draw something to the attention of a specific Team member (@AndyS), a channel or a whole team. Be generous with your Praise when someone does something good for the Team, and if you want to acknowledge a message just Like it, instead of adding to the noise with a text-based reply. When you're about to type something new – check if there's already a thread related to it and add to that instead and use the text styling (or a GIF / Sticker / Meme) when you want to get your point across and Sad, Angry or Happy reactions to contribute to the conversation when appropriate.

You can blur the background when you're in a video meeting, or [replace the background image](#) and if you have frontline workers that need to communicate with others, use [the Walkie Talkie](#) push-to-talk feature.

If you're on a mobile device you can use [Cortana voice assistance](#) to ask Teams to call a person or send a message to your next meeting. Teams will [automatically translate messages](#) in other languages to the language set in your personal settings. And there's [offline functionality](#), so if you're offline, Teams will save your unsent messages and send them when you're back online.

When you're in a meeting you can use [Together mode](#) which will show the video of each participant as if they were sitting in a lecture hall, removing the Brady bunch feel of the traditional grid of video feeds.

VIVA

If you needed any more proof how central Teams has become to Microsoft's vision and roadmap for modern collaboration and work, look no further than [the Viva](#) employee experience platform (EXP). Viva has four pillars, all surfaced in Teams, [Viva Connections](#) takes your SharePoint Online Home site, Line of Business (LOB) applications, and other internal news sources and lets you target company news and connections to the right people. [Viva Insights](#) is the next iteration of My Analytics to help staff manage time and avoid burnout, integration with Headspace for guided meditations and a virtual commute function to wrap up the workday. For Managers there's a de-identified view to see how a team is fairing from a stress, mental health and productivity point of view. There's also a Leaders view for executives to see the overall state of their staff. The third pillar is [Viva Learning](#), surfacing training courses and microlearning content (Microsoft Learn, LinkedIn Learning, Skillsoft, Coursera, EdX, Pluralsight with others to follow) to make learning a natural part of everyone's daily work. Managers can schedule trainings and staff can share particularly good courses with each other and they're all available directly in Teams. Finally, [Viva Topics](#) builds on Cortex / Syntex and uses AI to organize company-wide content (in-house projects, products, acronyms) and staff expertise and surfacing this as topic cards / pages in Teams, Microsoft Search SharePoint and Office. Think of this as Wikipedia for your business.

EXTENDING TEAMS

You can also use Teams to make voice and video calls to other people in the Team and if you add [PSTN calling](#) you can have Team be a soft phone client to make and receive phone calls from the phone network. Note that this is not available in all regions of the world as Microsoft in effect has to be a telecom provider for PSTN calling to work.

You can further [extend Teams with Bots](#) that can interact with your users naturally through chat or a notification bot that can push relevant information to your users.

With the advent of Slack (Team's main competitor) and Teams many people have (again) proclaimed the death of email. As usual we tend to see new technology as a direct replacement for the old while the reality is more nuanced. I find Teams more efficient for group-based work, the sharing of files and communication is superior to email but communication outside of projects I'm involved in still totally relies on email. And you can use email to send messages to a channel in a Team.

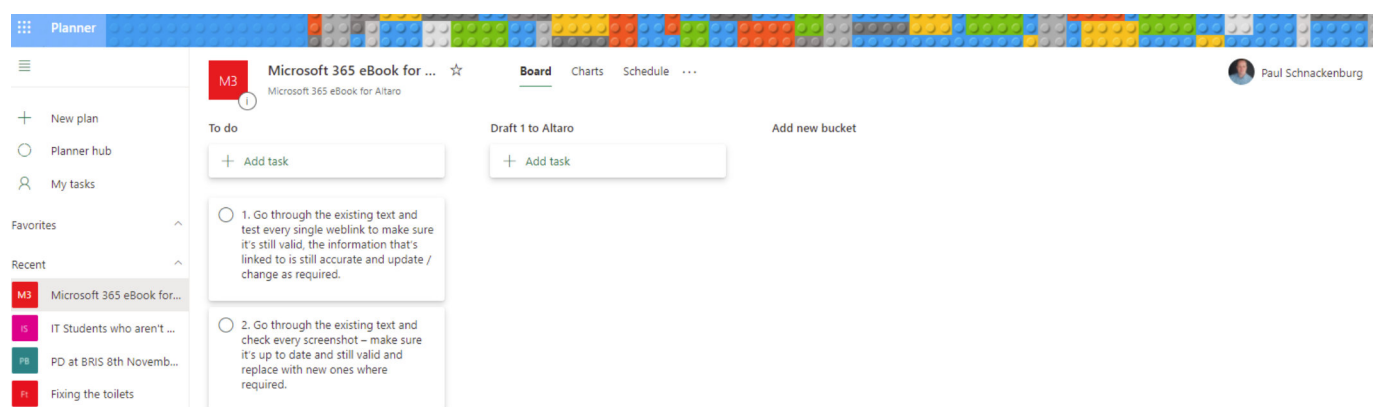
CHAPTER 11 - OTHER OFFICE 365 APPLICATIONS

There are many other applications and services in the O365 portfolio, in this chapter we'll some of them with a brief introduction.

PLANNER

Microsoft has had Project for large scale project management for many years but for small to medium undertakings it's overkill (there's a steep learning curve) and this is where Planner shines. If you've ever used Trello, you should be comfortable with Planner's workflow.

There's a web-based interface, along with iOS and Android clients but no PC client. If you add a Planner tab to a team you can create a new plan or attach an existing one. You organize tasks into buckets, assign tasks to different people and track progress of those tasks. Tasks can also be viewed in a Schedule (calendar) view and you can export a plan to Excel.



A Plan in Planner

Other task management offerings from Microsoft includes To-Do (mobile, web and PC clients are available) which integrates with Outlook tasks.

STREAM

This is the best way to share [video](#) inside your company and it's similar to YouTube. There are clients for iOS and Android and a web interface but currently there's no licensing in place for sharing videos with people outside your tenant.

When you upload a video it'll be processed and if the people in it are speaking English, Chinese, French, German, Italian, Japanese, Portuguese, or Spanish it'll [automatically generate captions](#) which are searchable in Stream, making it easy to find the right video or point in the video. It'll also attempt to recognize people in the video and if successful will list those people with the video information. Teams used to use Stream to store meeting recordings, but they're now stored in OD4B / SharePoint.

KAIZALA

This is an application similar to Teams, designed for frontline / transient workers with poor connectivity. Think of this as a managed version of WhatsApp.

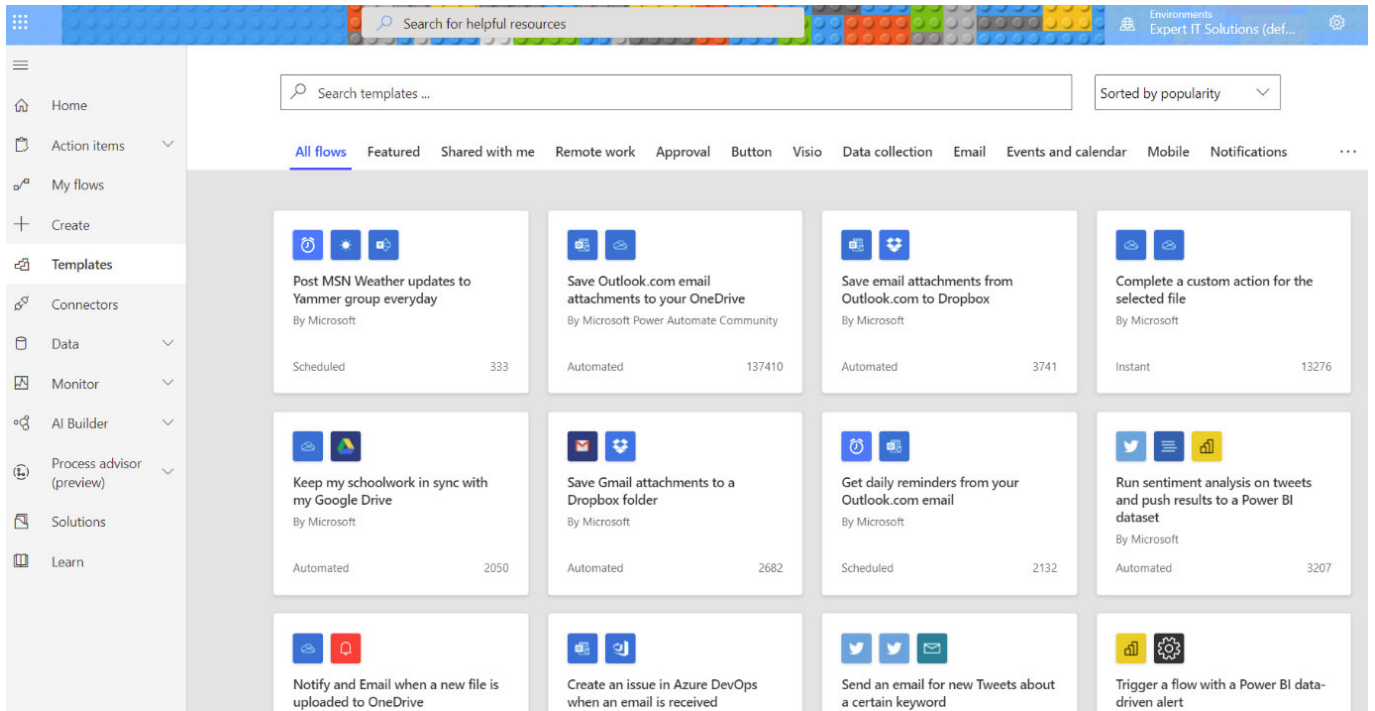
POWERBI

Visualizing data is important for any modern business who wants to be data-driven and [PowerBI](#) is Microsoft's answer. There's a desktop client where you build your dashboards, there's also a web interface. Licensing is [a bit of a challenge](#), depending on what you've built and who you want to share it with.

It's however a lot of fun to use and the results can be extremely useful for many aspects of your business.

POWER AUTOMATE

This deceptively simple, web-based tool is designed to automate tasks without having to write code (it used to be called Flow). Simply drag in actions, connect them to external systems and schedule them to run regularly or be triggered by an event. There are lots of templates to help you get started as well as connectors to hook into Microsoft and third-party systems. If you've used If This Then That or Zapier, [Power Automate](#) is easy to get started with.



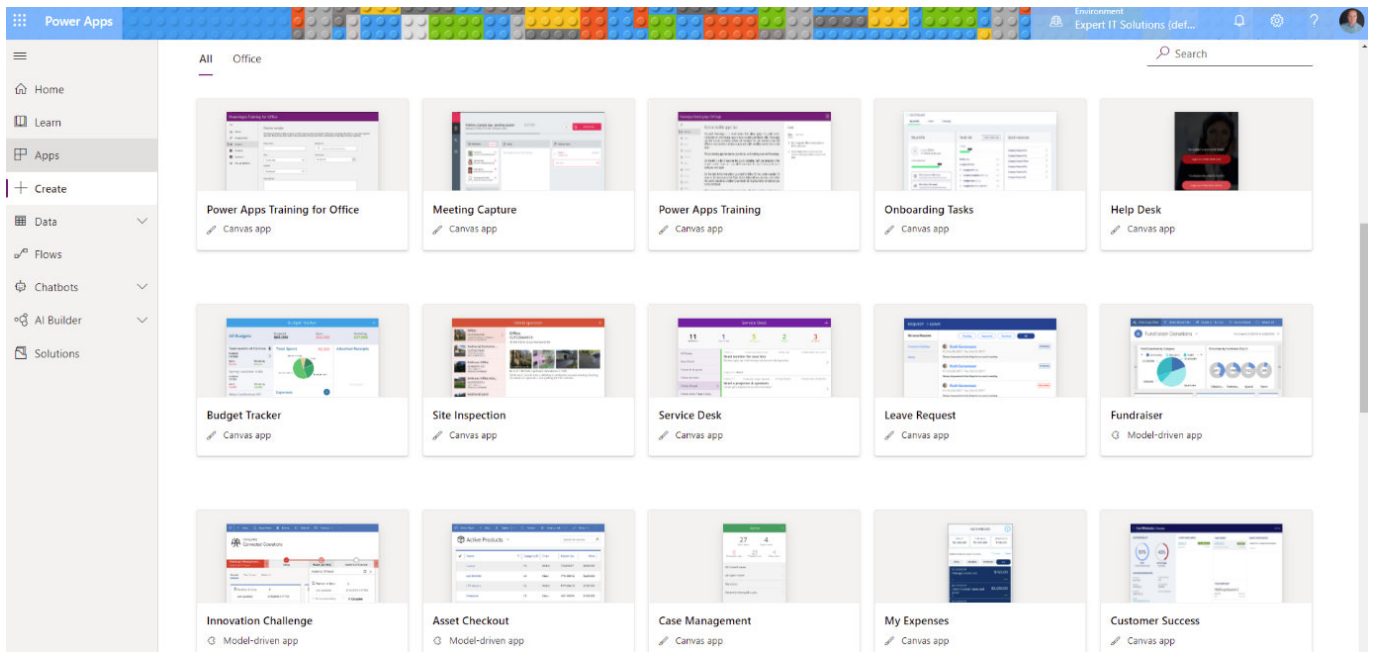
Power Automate Templates

POWERAPPS

Ever wished you could equip your staff with a custom mobile app to gather or access data in the field but realized the development costs were too high? [PowerApps](#) is the solution, providing a low code / no code development environment to build applications that connect to SharePoint, Excel, O365, Dynamics 365 or SQL server on-premises or in the cloud; or [the Dataverse](#) platform.

The resulting app runs on iOS, Android, in a web browser or in Teams and SharePoint Online.

If you need to manage data in your apps there's [Dataverse](#) for Teams and the full Dataverse flavor.



PowerApps Templates

YAMMER

Before Teams the only way to do “social networking” inside of O365 was [Yammer](#), think of this as Facebook for your internal business (with invited external guests). The reality today is that if you’re just getting started Teams is a better bet than Yammer, unless you’re a very large business where Yammer still has the upper hand over Teams.

CHAPTER 12 - SECURITY IN O365

In the early days of cloud computing there was a lot of concern around the security of data moved to “someone else’s datacenter”. I think it’s clear to most CISOs today that the big providers do a much better job of IT security than most businesses can do (or have the budget to do). Their incentive is also strong, if a large breach happened it could affect many thousands of businesses and so they spend a lot of money on making sure their clouds are as secure as they can be.

That doesn’t mean however that you can leave it all to Microsoft. There are some areas that are still your responsibility such as the endpoints that your users use to access cloud services, any on-premises infrastructure that’s operating in a hybrid mode with O365 and user provisioning and de-provisioning. There are also many security controls in O365 that you need to customize to suit your business, where you and Microsoft share the security responsibility. In this chapter we’ll look at these controls and where and how you configure them.

The foundation for “how you think about security” should be Zero Trust, instead of trusting a connection based on where it’s coming from (“if it’s on the internal LAN it’s safe, from the outside it’s dangerous”), every access is checked against your Conditional Access rules which gives you [a much better security posture](#). And base [your security on identity](#) which is the new firewall and [keep up with new features in the security space](#).

When thinking about how to defend your systems, don’t forget to take into account attackers [moving from on-premises to the cloud](#), as we saw in the Solarwinds breach. If you have M365 E5 licensing, use the revamped [attack simulator tools](#) to test your users with fake phishing emails and provide bite sized training automatically to them based on their propensity to fall for them.

Remember AAD Premium P1 & P2 which you can purchase as add-ons to O365 (included in M365), we covered their security features in [Chapter 5](#).

MICROSOFT 365 DEFENDER

At Ignite in September 2020 [Microsoft renamed almost all of their security services](#). There were a series of “Advanced Threat Protection” (ATP) services, that naming has now been changed to the Microsoft Defender brand, but you’ll still find mentions of the old names in blog posts and even official documentation. It’s also part of the overall change from Endpoint Detection and Response (EDR) to Extended Detection and Response (XDR) where several different security services integrate across your infrastructure to protect your business. Here’s a rundown of the different Defender services:

- [Microsoft Defender for Office 365](#) – This provides protection for emails, SharePoint sites, OD4B and Teams
- [Microsoft Defender for Identity](#) – This monitors your on-premises Active Directory (AD), integrates with your Security Information and Events Management (SIEM) tool and alerts you to account breaches, lateral movement and attacks involving AD
- [Microsoft Defender for Endpoint](#) – Centralized management of anti-malware on all endpoints in your environment (Windows, Linux, macOS, Android and iOS)

Microsoft also offers Azure Sentinel - a cloud based SIEM; Cloud App Security (MCAS) – a cloud-based cloud app security broker; Azure Defender and Azure Active Directory. We’ll cover some of these in this chapter and some in [Chapter 13](#).

OFFICE 365 SENSITIVITY LABELS

Using [labels to classify data](#), either manually or automatically through crawling documents or emails lets you start to govern your business information. Once a document has been labeled you can use MIP or OME to protect it (see below), or control access on Windows endpoints through policy as well as manage access in Office for Mac, Windows, iOS and Android.

Data classification

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

The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create info type Refresh 201 items Search

Name	Type	Publisher
ABA Routing Number	Entity	Microsoft Corporation
Argentina National Identity (DNI) Number	Entity	Microsoft Corporation
Australia Bank Account Number	Entity	Microsoft Corporation
Australia Driver's License Number	Entity	Microsoft Corporation
Australia Medical Account Number	Entity	Microsoft Corporation
Australia Passport Number	Entity	Microsoft Corporation
Australia Tax File Number	Entity	Microsoft Corporation
Australian Business Number	Entity	Microsoft Corporation
Australian Company Number	Entity	Microsoft Corporation

Sensitivity info types

MICROSOFT INFORMATION PROTECTION

One of the most powerful and least deployed features is the ability to protect documents, no matter where they live. Traditional file / SharePoint document sharing tightly controlled access at the server level but as soon as a document is emailed to someone, or stored on a USB drive, that control is lost.

With Microsoft Information Protection (MIP) you can set up labels and rules that encrypt documents and that carry their user access with them so no matter how they're shared, only the right people have access. There's MIP for O365, included with O365 E3 / E5 and MIP for M365 E3 / E5, see [here](#) for a feature list in each flavor. If you're getting started with MIP, use the newer [unified labeling client](#). It's important to configure [super user accounts](#) so that you can access documents when a user leaves the company. The long list of sensitive information types (SITs) recently [became even longer](#) and it's now possible to customize the confidence levels of rules, copy the built in ones and customize them and create larger keyword dictionaries (catch every mention of a staff ID tag, or patient record number). Recently it [became possible to co-author protected documents in real time](#) (with AutoSave support!) and in larger deployments you can use variables in MIP rules to facilitate per-app content marking. As you adopt MIP at scale you'll want to track how it's being used in your organization, [unified analytics](#) will help you do just that and it now includes information about MIP usage in Apps for Enterprise as well as activity from the on premises AIP Scanner.

OFFICE 365 MESSAGE ENCRYPTION

In a similar way to how MIP allows you to share protected documents with anyone you can use [O365 Message Encryption](#) to send emails to anyone and know that only that person can access that email. Like MIP you can also set up rules so that emails with specific information in them (credit card numbers, social security numbers) are automatically encrypted.

DATA LOSS PREVENTION

The aim of [Data Loss Prevention \(DLP\)](#) is to help users do the right thing by alerting them when they're about to share sensitive data through email, SharePoint Online, OD4B or Teams. It can also be integrated with MIP as Microsoft continues the journey of unifying labeling and protection across

0365. DLP protection has been extended to Windows 10 (1809 or later) with [Endpoint DLP](#), which can block upload of documents with sensitive content to cloud storage, copying sensitive information to the clip board, USB storage, network shares or printing. There's also an extension for Google Chrome that extends DLP protection to browser tasks. DLP has also [been extended to on-premises](#) using the AIP Scanner to find sensitive documents and alert management for DLP violations is also vastly improved.

Edit rule

Use actions to protect content when the conditions are met.

^ **Audit or restrict activities on Windows devices** 🗑️

When the activities below are detected on Windows devices for supported files containing sensitive info that matches this policy's conditions, you can choose to only audit the activity, block it entirely, or block it but allow users to override the restriction. [Learn more](#)

<input checked="" type="checkbox"/> Upload to cloud service domains or access by unallowed browsers	ⓘ	Block ▾
<input checked="" type="checkbox"/> Copy to clipboard	ⓘ	Block ▾
<input checked="" type="checkbox"/> Copy to a USB removable media	ⓘ	Block ▾
<input checked="" type="checkbox"/> Copy to a network share	ⓘ	Block ▾
<input checked="" type="checkbox"/> Access by unallowed apps	ⓘ	Block ▾
<input checked="" type="checkbox"/> Print	ⓘ	Block ▾

AND

^ **Restrict Third Party Apps** 🗑️

Restrict Third Party Apps
Use one of the automatic actions provided by Microsoft Cloud App Security. [Learn more](#)

Box

Send policy-match digest to file owner ⓘ

Restrict external access ⓘ

Save Cancel

Endpoint DLP settings

EXCHANGE ONLINE PROTECTION

[Exchange Online Protection \(EOP\)](#) is the mail hygiene solution for Office 365 and can also protect your on-premises Exchange mailboxes if you're in a hybrid deployment ([Chapter 7](#)). There are a few settings you can control for EOP as well as some additional configuration you should consider for complete spam protection such as [Sender Policy Framework \(SPF\)](#), [Domain-based Message Authentication, Reporting, and Conformance \(DMARC\)](#) and [Domain Keys Identified Mail \(DKIM\)](#).

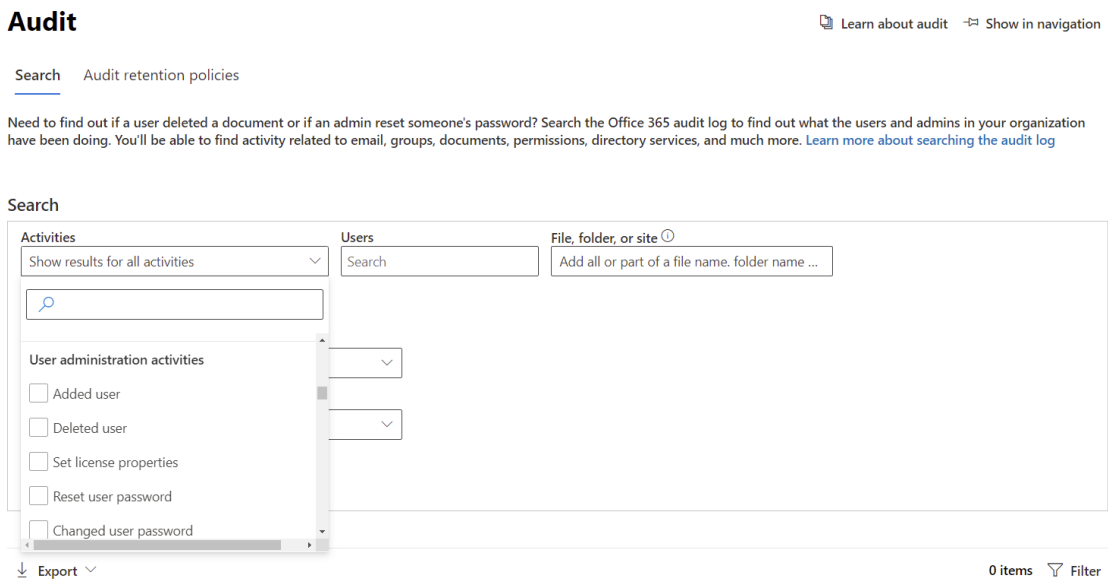
DEFENDER FOR OFFICE 365

Defender for O365 [protections](#) (available in O365 E5 or as standalone add-ons) builds on top of EOP and gives you **Safe Attachments** where attachments in incoming emails that may be malicious are opened inside a VM and checked before they're delivered to end users. **Safe Links** checks that links in emails and Office files aren't malicious at the time when users click on those links. **Anti-phishing** detects attempts to impersonate users, these protections [also extend to](#) SharePoint, OD4B and Teams.

If you find Defender for Office 365 too pricey (It's included in M365 E5, E5 Security or as a separate add-on) have a look at Hornet Security's [365 Total Protection](#) which comes in a Business and an Enterprise flavor. Business (\$2 per user per month) gives you granular control over email categories and content so that you can block unwanted emails. You can set email signatures with company disclaimers and use either PGP or S/MIME for email encryption, with certificate handling built in. The Enterprise flavor (\$4 per user per month) adds email archiving / journaling with up to 10 years retention, eDiscovery and sandbox analysis of attachments, URL rewriting and scanning (both in emails and in attachments) and Contingency Covering through an email failover environment when Microsoft 365 is down.

AUDITING

One of the great features of the unified platform of O365 is the ability to [audit user and administrator actions](#) across the entire platform.



At a minimum you want to [configure alerting](#) on AAD actions, go to the Security and Compliance portal – Search – Audit log search and see all the different activities you can audit and report on, as well as [create Alert policies](#) for. Prior to January 2019 you had to enable mailbox auditing to see user actions in their Exchange mailboxes, it's now [on by default](#).

New alert policy ✕

Name *:

Description

Alert type
 Custom ▾

Send this alert when... * ^

Activities *:

Users:

Send this alert to... * ^

Recipients *:

Creating an Alert policy

By default, Office 365 audit logs are kept for 90 days (AAD logs for 30 days), which may not be sufficient for your business or regulations you have to comply with. You have two options, use a third-party service to continuously export the logs and archive them for the time period you require, or assign M365 E5 (or M365 E5 Compliance / Discovery & Audit) licenses to the users who's logs you want to keep for longer. This unlocks the ability to keep the logs for 1 or 10 years.

New audit retention policy

Description

Paul S Retention

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

Users

PS Paul Schnackenburg X Search

Record type

AzureActiveDirectory, DLPEndpoint, ExchangeAdmin, MicrosoftTeams, Quar... ▾

Duration *

- 90 Days
- 6 Months
- 9 Months
- 1 Year
- 10 Years

Priority *

10

Save

Cancel



Audit retention policy

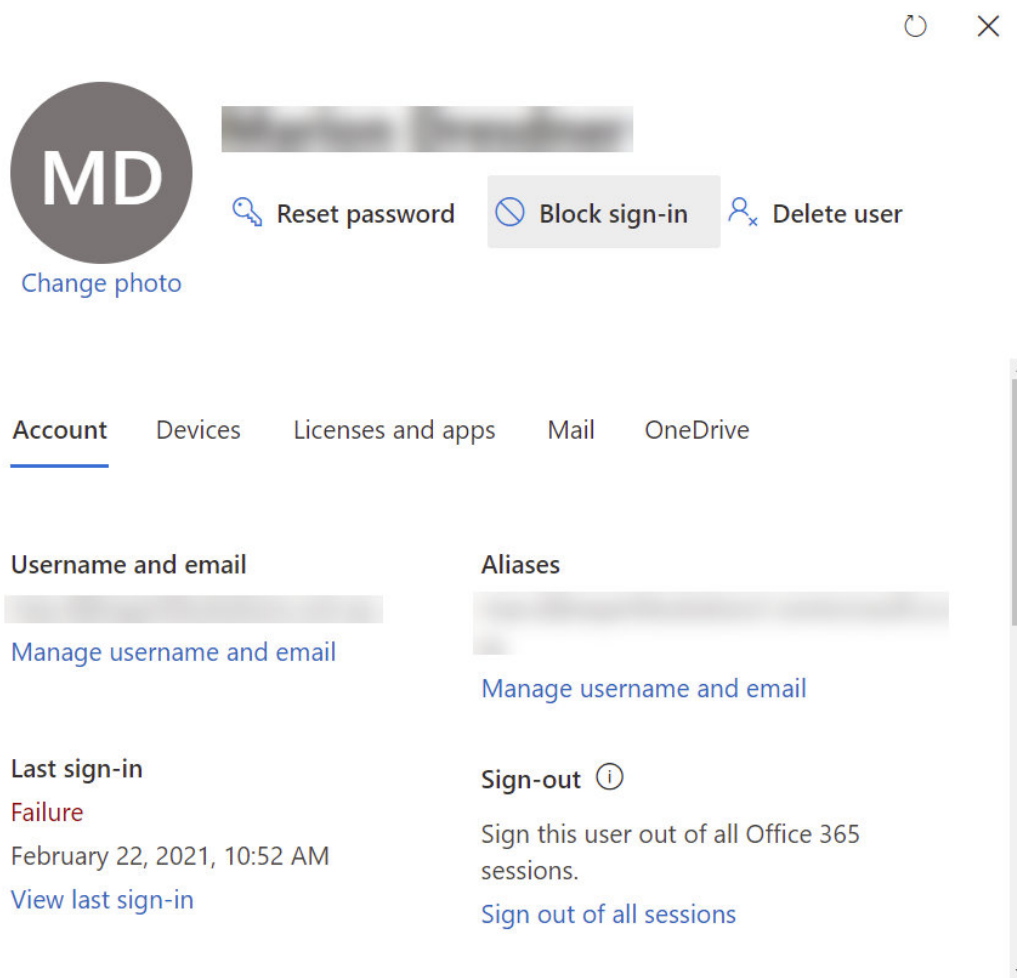
SAY GOODBYE TO PASSWORDS?

Ultimately the best way to manage passwords is to not have any stored in your directory and not have your users use any – this is called passwordless. There are [many steps on the journey towards this end goal](#), today you can use the Authenticator app to sign in on an Azure AD account (not as a second factor but as the only factor), or Windows Hello for Business or a FIDO 2 hardware USB/NFC key. [Recent announcements](#) make it even easier to move towards a passwordless nirvana.

In the meantime, enable [Password protection](#) to ban commonly used passwords (2000 in a list maintained by Microsoft plus up to 1000 custom words common in your organization/city/sports teams). This works seamlessly for cloud only accounts and [can easily be extended to on-premises AD](#). When you require your users to register for MFA, they're can also register for Self-Service Password Reset [at the same time](#).

BLOCK USER ACCESS

If you suspect or confirm that a user account has been compromised the first step should be to disable sign-in for the account in the Admin center.



Block sign-in for a user account

You should be aware however that the user (or the attacker) isn't immediately logged out from services they're accessing, and it can take up to an hour until the block takes effect, due to the lifetime of refresh tokens. The solution to this issue is [Continuous access evaluation](#) which today only applies to Exchange, Teams and SharePoint online connectivity and will block access in near real time (occasionally up to 15 minutes latency due to event propagation).

CHAPTER 13 – SECURITY IN MICROSOFT 365

There are many security tools in O365 but when you move to M365 you unlock a whole new set of advanced features for securing your business. In this chapter we're going to look at these tools, except for Endpoint Manager which we'll cover in [the next chapter](#) and Windows 10 which we'll cover in [chapter 15](#).

MICROSOFT DEFENDER FOR IDENTITY

With M365 E3 you get licensing for [Advanced Threat Analytics](#) (ATA), an on-premises server deployment that'll monitor your Active Directory environment and catch attackers in various stages of the kill chain; reconnaissance, lateral movement and domain dominance. ATA is in extended support since February 2021. With M365 E5 you can step up to [Defender for Identity](#) which does a very similar thing for your AD domains but without having to deploy the server infrastructure on-premises, only lightweight agents, the rest is taken care of by the cloud service. Both products are very good at catching attackers in your Windows network.

CLOUD APP SECURITY

When your users stayed in the corporate office all you needed to protect them was a good firewall but in today's world of "work anywhere, on any device" you need a new type of tool to protect them, a cloud access security broker. Microsoft Cloud App Security (MCAS) is part of M365 E5 and protects your users in real time when they access cloud services. The catalogue of over 17,000 different cloud services gives IT a way to discover and manage Shadow IT (cloud services that users have provisioned without the IT department knowing) across your user base.

Cloud app catalog

Filters: App tag: None Risk score: 0 10 Compliance risk factor: Select factors...

Security risk factor: Select factors...

Search for category...

- Hosting services 3.2K
- IT services 1.8K
- Accounting an... 1.4K
- E-commerce 766
- Business mana... 759
- Human-resour... 752

Show/hide category panel + New policy from search 181 - 200 of 17,090 apps Show details Table settings

App	Score	Actions
AWS IQ Customer support	9	✓ ⚙ ⋮
AWS CloudEndure Disaster Recovery IT services	9	✓ ⚙ ⋮
AWS Elemental MediaConvert Content sharing	9	✓ ⚙ ⋮
AWS Single Sign-On Security	9	✓ ⚙ ⋮

Cloud App Security SaaS catalog

SECURE SCORE

In [the last chapter](#) and this one we've looked at many of the security controls that you can use. But where do you start? How do you know what's most important to attend to? And where in all the different portals (or PowerShell) do you go to configure each setting?

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters:

Your secure score

Secure Score: 47.01%
400.5/852 points achieved

100%
50%
0%

11/17 11/24 11/30 12/06 12/12 12/18 12/24 12/30 01/05 01/11 01/17 01/23 02/04 02/09

Breakdown points by:

Identity	72.32%
Device	45.77%
Apps	18.75%

■ Points achieved ■ Opportunity

Actions to review

Regressed	To address	Planned	Risk accepted	Recently added	Recently updated
0	77	0	0	0	0

Top improvement actions

Improvement action	Score impact	Status	Category
Block Office communication application from creating child proces...	+1.06%	To address	Device
Block credential stealing from the Windows local security authority...	+1.06%	To address	Device
Block Office applications from creating executable content	+1.06%	To address	Device
Use advanced protection against ransomware	+1.06%	To address	Device
Block Win32 API calls from Office macros	+1.06%	To address	Device
Block execution of potentially obfuscated scripts	+1.06%	To address	Device

Secure Score overview

The answers to these questions are in Secure Score, now part of [the Security portal](#). Here you see an overall score for your tenant (for Identity / Data / Device / Apps and Infrastructure controls) and can compare it to the global average across O365, the average for your industry and for businesses of the same size. On the second tab you can see actions you should take to improve your score, how many points each action will give you and the user impact and administrative effort required.

↑ ↓ ×

Improvement actions > [Block credential stealing from the Windows local security authority subsystem \(lsass.exe\)](#)

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 locks down LSASS.

This security control is only applicable for machines with Windows 10, version 1803 or later. Attackers can use tools like Mimikatz to scrape cleartext passwords and NTLM hashes from LSASS.

Last synced 2/9/2021

	Points achieved	History
	0/9	No events

Manage
Share ▾
Save and close
Cancel

<p>Action plan</p> <p>Go to Threat & Vulnerability Management (TVM) to take action</p> <p>Tags: Add tags</p>	<p>At a glance</p> <p>Category: Device</p> <p>Protects against:</p> <p>Product: Defender for Endpoint</p> <hr/> <p>User impact</p> <p>Unknown</p> <p>Users affected</p> <p>Unknown</p>	<p>Implementation</p> <p>Prerequisites</p> <p>✓ None</p> <p>Next steps</p> <p>In Microsoft Defender Security Center's Threat & Vulnerability Management section, read the security recommendation and choose remediation or exception options.</p> <p>Implementation status</p> <p>2/2 exposed machines</p> <p>Learn more</p> <p>None</p>
---	--	--

Example action to improve your security

Clicking on an action provides details as to what risks the control mitigates, which compliance regulation it matches, the ability to click a button to go directly to the right area to configure it and the option to tell the system that you have already mitigated this risk with a third-party service.

As you implement more controls your score increases (it can take 24-48 hours), and you track your progress on the History tab. Secure Score is the BEST place to start improving your tenant's security posture.

I'd like to highlight another control (apart from MFA) that'll gain you a quick win to improve overall security – [blocking legacy authentication](#). This is because even if you have enabled MFA, attackers can still access your user's accounts with just a username and password through older protocols that don't

support MFA. To investigate if there are any legitimate connections using these older protocols (which will need to be upgraded or exempt from your block legacy authentication policy) go to the Azure AD portal, click on Sign-ins under monitoring, click Add filters, pick Client app, then click “None selected” and add all 13 legacy connection options.

Here you can see a tenant with MFA enabled but legacy authentication still enabled with numerous failed access attempts.

Dashboard > PAUL SCHNACKENBURG

PAUL SCHNACKENBURG | Sign-ins

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

Date: Last 24 hours Show dates as: Local 13 selected Add filters

Date	Request ID	User	Legacy Authentication Clients	IP address	Location	Conditional acc...	Auther
2/23/2021, 3:33:51 PM	9b68e29f-71c8-4797...	Paul Schnac	Autodiscover	202.72.243.198	Ulaanbaatar, Ulaanb...	Not Applied	Single-
2/23/2021, 1:18:52 PM	08ddd849-9da1-4d8...	Paul Schnac	Exchange ActiveSync	187.189.111.113	Monterrey, Nuevo L...	Not Applied	Single-
2/23/2021, 11:30:04 ...	71c77c2d-5e85-42c2...	Paul Schnac	Exchange Online Powershell	184.179.216.142	San Jose, California, ...	Not Applied	Single-
2/23/2021, 11:26:17 ...	7e9128f9-099e-411f...	Paul Schnac	Exchange Web Services	157.119.108.178	Gopanapalli, Telanga...	Not Applied	Single-
2/23/2021, 10:08:08 ...	36736dc1-7d5c-4c2...	Paul Schnac	IMAP	209.150.255.40	Bixby, Oklahoma, US	Not Applied	Single-
2/23/2021, 7:55:02 AM	cfb90f35-2f84-4c90-...	Paul Schnac	MAPI Over HTTP	200.62.146.174	Lima, Lima Province, ...	Not Applied	Single-
2/23/2021, 5:37:42 AM	46c0b591-0e8b-4dd...	Paul Schnac	Offline Address Book	177.19.165.26	Porto Alegre, Rio Gra...	Not Applied	Single-
2/23/2021, 5:36:22 AM	f307ebc5-652b-4780...	Paul Schnac	Other clients	142.54.225.52	Hartland, Wisconsin, ...	Not Applied	Single-
2/23/2021, 5:32:13 AM	f307ebc5-652b-4780...	Paul Schnac	Outlook Anywhere (RPC over HTTP)	170.247.41.191	Marica, Rio De Janeir...	Not Applied	Single-
2/23/2021, 4:29:59 AM	a7a77c51-1f17-45a6...	Paul Schnac	POP	190.3.194.237	Medellin, Antioquia, ...	Not Applied	Single-
2/23/2021, 2:39:42 AM	f4aa6c65-29f1-4718-...	Paul Schnac	Reporting Web Services	200.49.63.10	Salvador, Bahia, BR	Not Applied	Single-
2/23/2021, 12:08:29 ...	822711a6-5282-434f...	Paul Schnac	SMTP	109.251.55.235	Kyiv, Kyiv Misto, UA	Not Applied	Single-
2/22/2021, 11:50:54 ...	c912466a-b742-45ca...	Paul Schnac	Universal Outlook	72.217.158.214	Los Angeles, Californ...	Not Applied	Single-

AAD Sign-in attempts using legacy authentication

Once you’re certain there are no legitimate needs for legacy authentication, use [CA policies to block it](#).

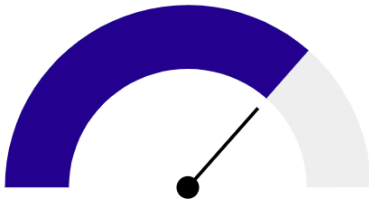
The concept of Secure score has spread to other parts of M365, in [Compliance Manager](#) there’s Compliance Score to indicate how compliant your business is with regulatory frameworks you have to comply with. Microsoft has recently added hundreds of additional regulations from all over the world to help you track your compliance, assign tasks users to achieve and maintain compliance.

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. [Find guidance and documentation](#)

Filter

Overall compliance score

Your compliance score: **73%**



12342/16787 points achieved

Your points achieved ⓘ

27/4472

Microsoft managed points achieved ⓘ

12315/12315

Key improvement actions

Not completed **305** Completed **1** Out of scope **0**

Improvement action	Impact	Test status	Group	Action type
Protect Authenticator Content	+27 points	None	Default Group	Operational
Limit Consecutive Logon Failures	+27 points	None	Default Group	Operational
Implement account lockout	+27 points	None	Default Group	Operational
Protect authenticators commensurate with use	+27 points	None	Default Group	Operational
Refresh authenticators	+27 points	None	Default Group	Operational
Protect wireless access	+27 points	None	Default Group	Operational

Compliance score in Compliance Manager

Productivity Score was covered in [chapter 4](#).

SECURITY IS EVERYONE'S RESPONSIBILITY

The last two chapters have given you a high-level overview of the many security features available across O365 and M365. The sad truth is that most small to medium businesses don't implement nearly enough of the features they have already paid for and even large enterprises struggle to get these protections in place for all their users. Don't be complacent, modern IT security is a battlefield and currently we are losing big time – most businesses are soft targets for the attackers.

CHAPTER 14 – MICROSOFT ENDPOINT MANAGER

M365 E3 and E5 brings you [Microsoft Endpoint Manager](#) (MEM), Microsoft's [Mobile Device Management \(MDM\) cloud service](#). In this chapter we'll look at how it can help you manage devices and PCs, mobile apps, protect company data and enforce security policies.

Note that MEM is the umbrella term for the cloud service Intune (which you'll see referenced in the documentation) and System Center Configuration Manager (SCCM), now called [Microsoft Endpoint Configuration Manager](#). This latter product is now the “edge computing” part of MEM, whereas Intune is the cloud service.

There used to be a requirement that Intune administrators were licensed for Intune but [this is no longer the case](#). Endpoint analytics is an interesting part of MEM, using signals from your devices to pinpoint problematic or slow PCs which [now also includes application reliability and restart frequency](#).

If you have Windows 10 devices that serve specific functions (on a factory floor, at a nurses station in a hospital for example), you can use the recently released Cloud Configuration to [easily manage them entirely using MEM](#), with scripted, basic configuration settings.

Managing fleets of devices can be challenging, the new MEM [settings catalog](#) preview lets you easily customize, set and manage device and user policy settings.

MOBILE DEVICE MANAGEMENT

There are a couple of ways you can use MEM, if you have devices (smartphones, tablets, laptops) that are company owned you can [enroll them in Intune](#). This gives you a great deal of control over the device, including the ability to manage settings, apps and the option to wipe the device should it be lost or stolen. You can also use Intune to manage OS updates for Windows devices, push out applications to devices, configure Wi-Fi profiles and deploy certificates as well as block iOS jailbroken and rooted Android devices.

Fully managed, dedicated, and corporate-owned work profile

Android Enterprise

✓ Basics **2 Compliance settings** ③ Actions for noncompliance ④ Assignments ⑤ Review + create

^ Microsoft Defender for Endpoint

Microsoft Defender for Endpoint rules

Require the device to be at or under the machine risk score: ⓘ

^ Device Health

Require the device to be at or under the Device Threat Level ⓘ

Google Play Protect

SafetyNet device attestation ⓘ

^ Device Properties

^ System Security

Require a password to unlock the device. If not configured, the use of passwords is optional, and left up to the user to configure.

[Learn more](#)

Require a password to unlock mobile devices ⓘ

Required password type ⓘ

Android Compliance Policy in Endpoint Manager

If the device is a personal device, owned by the employee, they may not be comfortable with enrolling the device so you can use Mobile Application Management (MAM) for those devices.

MOBILE APPLICATION MANAGEMENT

This less intrusive approach lets you create [app protection policies](#) (APP) across specific applications, with email being the classic example. Users want to access business email on their personal smartphone so you put policies around it where they can only use Outlook (free mobile app for Android and iOS), not the built-in mail apps and you can further protect corporate data so that a user can't copy business data to a non-business app (personal email app etc.). If the device is lost or stolen, you can wipe the corporate data off it while leaving personal photos etc. untouched.

[Picking between MDM and MAM](#) is going to depend on many factors such as your userbase, your employment contracts, business and security needs and more; make sure you spend some time in [the planning phase](#) to get it right.

Another part of managing mobile applications might be to connect them back to on-premises resources securely, Microsoft now offers their own VPN for iOS and Android called [Tunnel](#) – and it's integrated into [the Microsoft Defender for Endpoint solution](#).

Create profile

▼ Firewall

▼ Internet Explorer

^ Local Policies Security Options

Block remote logon with blank password ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Minutes of lock screen inactivity until screen saver activates ⓘ	<input type="text" value="15"/>	<input checked="" type="checkbox"/>
Smart card removal behavior ⓘ	<input type="text" value="Lock workstation"/>	<input type="checkbox"/>
Require client to always digitally sign communications ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Prevent clients from sending unencrypted passwords to third party SMB servers ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Require server digitally signing communications always ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Prevent anonymous enumeration of SAM accounts ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Block anonymous enumeration of SAM accounts and shares ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Restrict anonymous access to named pipes and shares ⓘ	<input checked="" type="radio"/> Yes	<input type="radio"/> Not configured
Allow remote calls to security accounts manager ⓘ	<input type="text" value="O:BAG:BAD:(A;;RC;;;BA)"/>	<input checked="" type="checkbox"/>

MDM Security Baseline

MICROSOFT ENDPOINT CONFIGURATION MANAGER

If you have deployed MECM on-premises to manage your servers and traditional client PCs you can integrate Intune into your management flow [through Co-management](#) to leverage the best of both worlds and prepare your environment for a gradual migration to cloud management. Don't confuse this with [Hybrid MDM](#) which is the older, deprecated approach to marrying SCCM and Intune.

DEFENDER FOR ENDPOINT

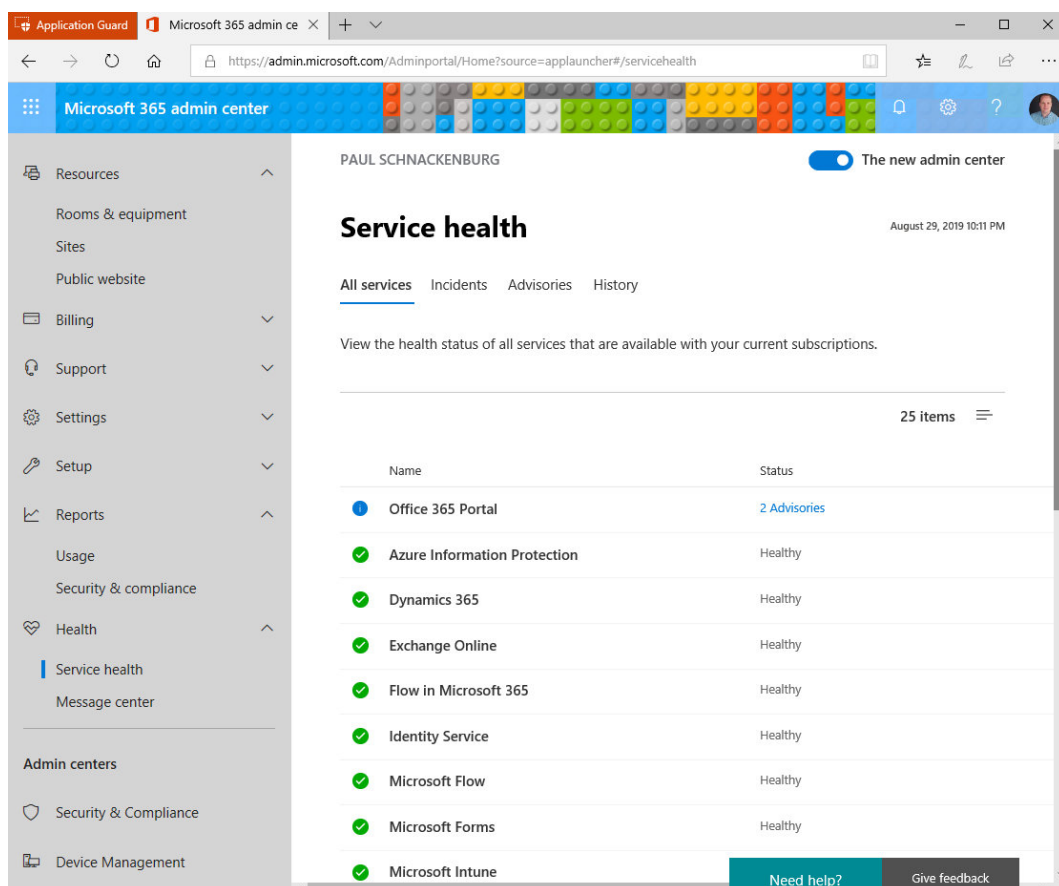
[Microsoft Defender for Endpoint](#) (MDE) is a full-fledged Endpoint Detection and Response (EDR) security solution using Machine Learning (ML) behavior analytics for Windows, MacOS, Linux servers, iOS and Android devices. It inventories installed applications (Windows and MacOS) and through [Threat and Vulnerability Management](#) (TVM) prioritizes which applications bring the most severe risks to your organization based on how widely deployed each application is. MDE also provides [Attack surface reduction rules](#) and [Next generation protection](#), along with many other security features. MDE is available with Windows 10 Enterprise E5, M365 E5 / E5 Security or as a standalone license.

CHAPTER 15 - WINDOWS 10 ENTERPRISE

The last pillar of M365 is Windows 10 Enterprise, five devices for each licensed user which will automatically upgrade Windows 10 Pro to Enterprise as soon as a user logs in. In this chapter we'll cover what additional security features this brings for your enterprise.

WINDOWS 10 ENTERPRISE

Enterprise adds [Defender Application Guard](#), [Defender Application Control](#) and [Defender ATP](#) on top of the security features you get in Windows 10 Pro. **Application Guard** protects your users when browsing potentially malicious sites using Edge in a hardware isolated manner. This technology has also [been extended to Word, Excel and PowerPoint](#). **Application Control** on the other hand builds on earlier iterations of AppLocker and blocks untrusted applications from running, including plug-ins and add-ins.



Browsing in an Application Guard window

[Always On VPN](#) doesn't require Windows 10 Enterprise and is a successor to [Direct Access](#), if you still need to use client VPN in your business.

Whilst it's not exclusive to Windows 10 Enterprise definitely look at [Windows Hello for Business](#) to improve your user's login experience as well as your security (a rare case of everyone wins in security) by moving away from passwords. Another feature not unique to Enterprise is [Windows Information Protection](#) (WIP) which extends the ability for Intune and SCCM to distinguish between corporate and personal data on a Windows 10 device and build policies to stop sensitive data leakage, WIP will be replaced by Endpoint DLP in the future ([chapter 12](#)).

If you're deploying large numbers of Windows 10 devices and you want to reduce the burden of wiping each new device and installing your custom image, [consider using Windows Autopilot](#), it's a powerful way to "deploy" Windows 10 by simply transforming the pre-installed image as it's delivered by your OEM.

CONCLUSION

We hope that this book and its links to more in-depth technical information has helped guide you on your journey to the cloud and once you have migrated, the continuing journey, as managing the ever-changing landscape of M365 is a never-ending ride.

ABOUT THE AUTHOR



Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. He works part time as an IT teacher at a Microsoft IT Academy. He also runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. Paul writes in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies. He has MCSE, MCSA, MCT certifications. He can be reached at paul@expertitsolutions.com.au, follow his blog at TellITasITis, <http://tellitasitis.com.au>.



Microsoft does not provide
Office 365 backup and
recovery services



Microsoft can't help with
unexpected data loss or
damage



Problems with
non-centralized data

Microsoft does not provide Office 365 backup and recovery services

Office 365 subscriber data – such as mailboxes and files stored within OneDrive and SharePoint Document Libraries - is not backed up by Microsoft as part of their subscription. Microsoft does not provide Office 365 data protection services. ([Read more here.](#))

- Microsoft provides the necessary infrastructure and must ensure that Office 365 works. However, as an Office 365 subscriber, it is up to you to protect your Office 365 data from aspects such as: human error (for example, deleted items), hacker and malware attacks, malicious user actions, etc.
- Microsoft doesn't provide native backup options for Office 365. It includes some basic archiving, retention and recovery features as well as versioning, but cannot guarantee full and fast restoration of data loss.

That's why you need to use a reliable backup and recovery solution to save your skin when things go wrong and to give you peace of mind.

Microsoft can't help with unexpected data loss or damage

If Office 365 contents are misplaced or deleted from the network or are damaged or destroyed, a robust backup solution ensures that you have access to a backed-up copy. This helps you avoid the issues and repercussions that arise when data goes missing.

Once a mail item is deleted or changed in Office 365, for example, it stays that way. Simple day-to-day scenarios could lead to data loss, such as:

- A system admin might unintentionally delete an Office 365 mailbox user.
- A user might intentionally or accidentally delete a file within OneDrive or SharePoint and only realise weeks later.
- A ransomware attack or virus infection could block or damage an organisation's mailboxes.

A backup solution is therefore a must as it allows you to restore a prior instance of that item.

Problems with non-centralized data

Your data can best be protected and stored centrally by backing up all the company's mailboxes and files into a single location. This way, you can also enjoy easy access, searching, browsing and recovery. Altaro Office 365 Backup's online console enables central management and monitoring of all your Office 365 backups.

[START YOUR 30-DAY TRIAL](#)

THE SOLUTION

It's essential for you to implement a reliable solution to back up your Office 365 mailboxes and your files in OneDrive and SharePoint Document Libraries.

Here's how Altaro can help you:

Altaro Office 365 Backup enables you to back up and restore all your Office 365 mailboxes – emails, attachments, contacts and calendars – and files stored within OneDrive and SharePoint through an online console, on an annual subscription, allowing you to easily manage your backups. Data is backed up to Altaro's Microsoft Azure infrastructure. Includes unlimited storage and 24/7 support. Altaro's 24/7 Lightning Fast Support Call Response Guarantee of under 30 seconds.

Benefits of the Altaro Office 365 Backup subscription program:



Back up your Office 365 mailboxes, OneDrive and SharePoint: Altaro enables you to back up and restore your Office 365 mailboxes with ease. If you wish to also back up your OneDrive and SharePoint accounts, you can choose to do so too.



Unlimited storage is included; no local storage infrastructure or software required: You don't have to think about setting up your own servers to save backups to – backups are saved to Altaro's Microsoft Azure infrastructure as part of the package.



Central management and searches: Manage and monitor all your users' Office 365 backups – for mailboxes, OneDrive and SharePoint accounts – through Altaro's cloud-based management console. This also allows for easy searching.



No extra fees: You get access to all product features across all your users, unlimited backup storage on Microsoft Azure infrastructure, 24/7 support, and our console for centralised management.



Quick and easy recovery: Access various restore options to restore misplaced, deleted, damaged or destroyed items.



Lightning-fast, 24/7 support: 22-second average support call pickup, live chat, speak directly with an expert, no tier 1 agents or gatekeepers.



Unbeatable value: Great pricing. Volume discounts apply, making it even more cost-effective as you scale to tens of thousands of users.

[START YOUR 30-DAY TRIAL](#)

ABOUT ALTARO

Altaro proudly forms part of the Hornetsecurity Group.

Founded in 2009, Altaro has grown rapidly over the years. We develop robust backup solutions to address the core data protection need of businesses and organizations worldwide , as well as the IT resellers, VARs, consultants and managed service providers who serve them.

Our aim is to exceed your data protection needs with reliable, affordable backup solutions backed by an outstanding, personal 24/7 Support team that's determined to help you succeed in protecting your environment.

ALTARO DOJO

The Altaro DOJO is a dedicated training and educational platform for system administrators and IT professionals. It is updated every week with high-quality, value-packed content every week including articles, guides and tips for Microsoft/Office 365!



Register to [the Altaro DOJO](#) now to gain unrestricted access to all content and stay notified when new content is released - it's free to join!

FOLLOW ALTARO AT:



SHARE THIS EBOOK:



PUBLISHED BY ALTARO SOFTWARE

<http://www.altaro.com>

Copyright © 2021 by Altaro Software

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without the prior written permission of the publisher or authors.

WARNING AND DISCLAIMER

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 authors 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.

FEEDBACK INFORMATION

We'd like to hear from you! If you have any comments about how we could improve the quality of this book, please don't hesitate to contact us by visiting www.altaro.com or sending an email to our Customer Service representative Sam Perry: sam@altarosoftware.com