ramsac
the secure choice

Microsoft 365 admin management: the roles & responsibilities of being an admin

So, you're a Microsoft 365 administrator...

You may not even know it yet, but every Microsoft 365 suite will have its dedicated administrators. Capable of differentiating tasks and permissions, admins play a critical role in gatekeeping your Microsoft 365 ecosystem. This will help your organisation spread tasks to the most relevant people, keeping data safe and secure.

What's inside:

In this guide we cover:

A technical review of administration in 365 ---- 9

Best practices for admin accounts ---- 12

The typical admin tasks you'll encounter ---- 15

Administrating Microsoft 365 products – a closer look ---- 17

- Teams ---- 18
- SharePoint ---- 19
- Exchange Online (Email) ---- 19

The roles and responsibilities of being a Microsoft 365 admin – getting started

When you set up Microsoft 365 within your company, you will need to appoint at least one Microsoft administrator. Administrators are in charge of setting up other users' accounts, assigning licences and so much more.

Whether you're new to the admin role or you're upgrading your administrator responsibilities, you'll likely have questions about optimising your time as an admin, as well as managing the roles and responsibilities of other users.

In order to answer your questions, here's everything you need to know about Microsoft 365 administrator roles.

What does a Microsoft 365 admin do?

A Microsoft 365 admin will do three things:

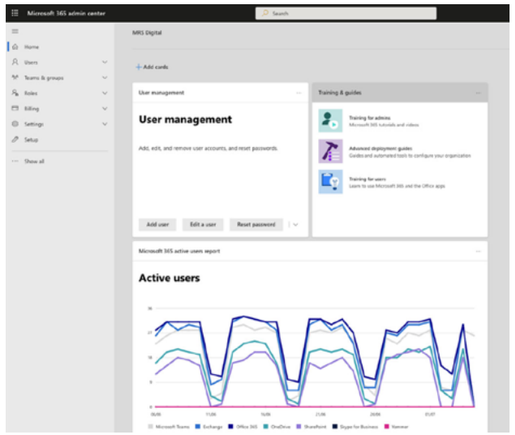
1. Administer licences to users, including other admin levels
2. Manage the organisation account from the Microsoft 365 admin centre, an online portal
3. Raise support queries with Microsoft and assist users

What's the difference between Office 365 and Microsoft 365 admin centres?

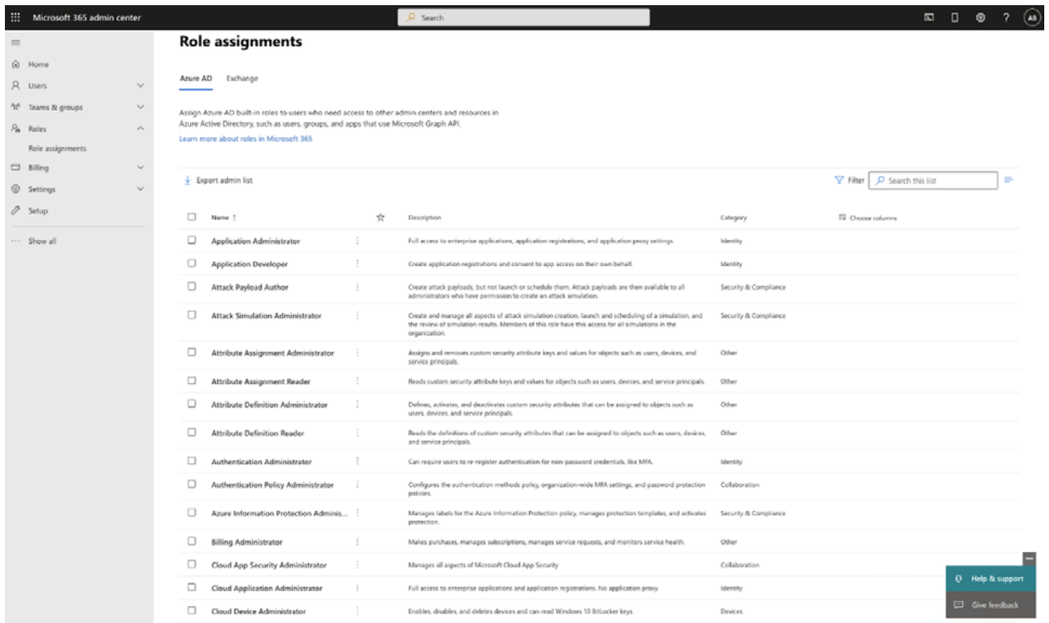
If you're confused about what you're actually an admin of, don't worry. Essentially, Microsoft rebranded its Office 365 admin centre to form part of the existing Microsoft 365 centre. Now, everything is rolled into one, and what you may have previously accessed from the Office 365 admin centre, is now found in the Microsoft 365 admin centre.

How do I know if I am an admin of Microsoft 365 within my business?

You can quickly check admin status within your 365 account by checking inside the admin centre.



1. **If an error message appears**, such as one that's denying your permissions to access the page, or "perform this action", then you won't have admin access.
2. **If you have access to this portal**, you are a 365 admin.



There is, however, a scenario where you may need to do some troubleshooting to see the Admin view of your 365 suite. When you have access, you can confirm this status by reviewing "Roles" in the right-hand control panel record. Under this section, this will tell you whether your account is listed as a "**Global Admin**" or another type of admin.

Becoming an admin

The task of changing admins within 365 accounts is easy and it should only take you up to 15 minutes to set up.

You can contact your Global Admin to upgrade your role if you require admin access within Microsoft 365.

You should limit the number of users assigned as "Global Admins", as this can escalate into a security risk. Rather than have too many admins with sweeping access to Microsoft services within your subscription plan, **we recommend that you carefully consider who needs the highest level of access.**

A technical review of administration in Microsoft 365

About admin roles in 365

Every Microsoft 365 subscription comes with admin roles that will need to be assigned to different users across your business or organisation. Assigned with these responsibilities (of which we'll break down later), these 365 admins can manage various administration tasks from within the Microsoft 365 admin centre.

The basic purpose of these admin roles is to serve broader business functions, such as authorising access to potentially confidential files, folders and even areas of an Intranet. When an account becomes an 'admin', they will have unique permissions above standard users across your organisation; and this gives them the influence to complete specific tasks within the admin centres for different 365 products.

Too Busy? A growing business needs to focus on what it does best. That might mean, as your team grows with your organisation, that there's increasingly less time available to work through the basic admin and setup in 365. When this becomes a time-sink, consider working with a Microsoft Gold partner like ramsac to set everything up.

There are multiple different admin user types within Microsoft 365, each with unique permissions, or lack thereof. These can be critical in managing the security of data, such as file sharing or password resets.

What are the different admin roles in Microsoft 365?

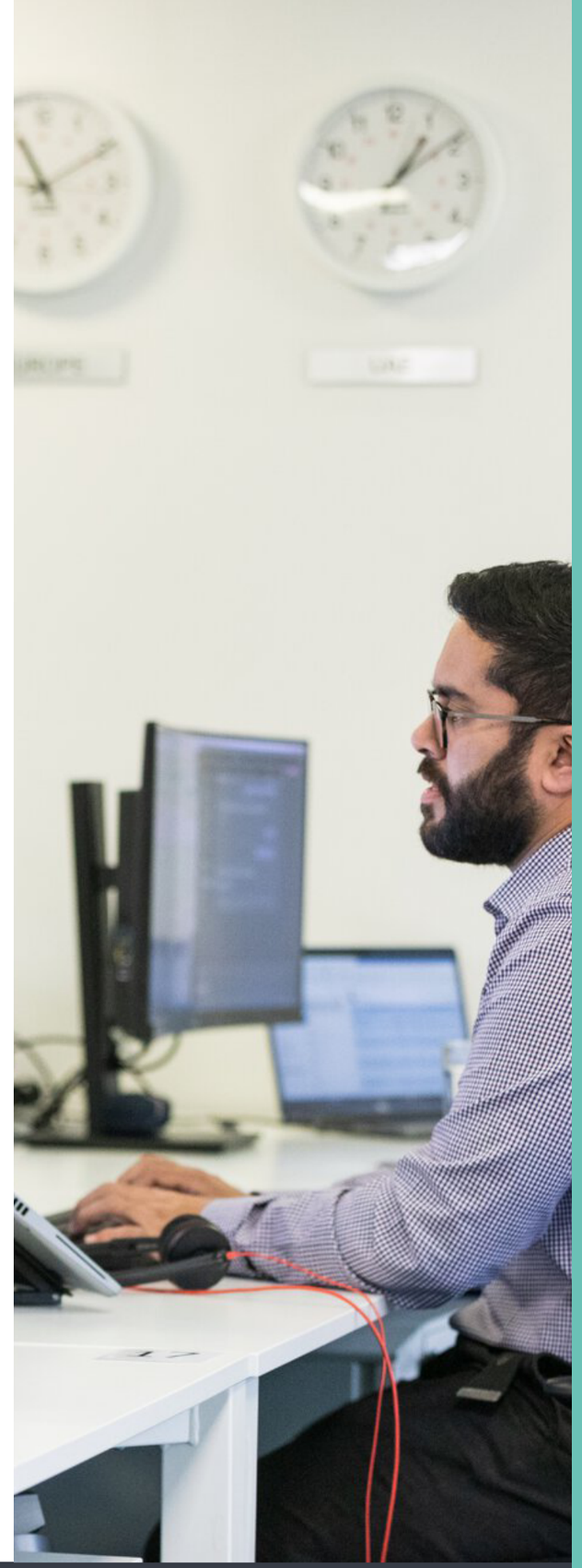
Role	
Global admin	Global admins are in charge of everything inside of Microsoft 365. The global admin role is automatically assigned to the person who signed up, but you can add more. Global admins can manage everything that all other admins can, and more.
Exchange admin	This role enables users to manage user inboxes, 365 groups, and Exchange online.
Office apps admin	An Office apps admin can monitor the health of Office across a business, manage service requests and assign policies.
Global reader	A global reader can view all global administration features, but does not have permission to make edits to settings.
Helpdesk admin	This role enables the admin to help users to reset passwords, as well as open and manage support requests.
Service admin	This admin can submit support requests for Azure, Microsoft 365, and Office 365.
SharePoint admin	The role provides full access to SharePoint online amongst management permissions in Office 365 groups.
Teams admin	The admin has full access to the Teams admin centre.
Licence admin	This role can assign licences to new users and revoke old licences.
User admin	This role can be assigned to manage access, user password resets, and user groups within an organisation's 365.
Billing admin	Permissions will allow the admin to manage and control billing details, as well as see invoices.
Groups admin	A groups admin manages Microsoft's groups, and can assign policies to individual groups, as well as restore data.
Password admin	The only ability that this role gives someone is to be able to restore passwords for non-admin users.
Power Platform admin	Relevant for those who use Power Apps, Power Automate and data loss protection, this admin can manage admin features for any Power apps and manage service requests for this app.
Reports reader	With this level of access, a user can read and view reports, including the Microsoft Graph API to enable company-wide 365 reporting.
Service support admin	Similar to the helpdesk admin, a service support admin manages help desk tickets, and can open and close them, but can't action basic requests.
Message centre reader	This user can monitor the message centre and get weekly insights into the message centre across the organisation.

Comparing admin access

A lesser-known feature that's controllable within the admin centre – managers can compare up to three roles to quickly identify the appropriate role to assign to a new or existing user. This feature is useful in filtering down the different levels of permissions available across user types.

How does it work?

Within admin view, you can nominate up to three different admin user types in a comparison view to benchmark permissions between users. This is especially helpful where you're undecided about the best role type to assign, and you want to minimise unnecessary permissions, therefore keeping data safer.



Best practices for admin accounts

“Best practice”, in the context of your Microsoft 365 Administrator accounts, is as much about how to operate permissions, as it is keeping these secure.

1 Don’t forget the basics – including password management

It goes without saying that administrator accounts should be following the standard practices of all users across an organisation. This means using long, complex passwords to keep an admin secure – and keep these refreshed and regulated thoroughly.

These basic security practices still apply to those users with higher permissions, especially administrators, who will need to regularly ensure that best practice is followed accross an organisation. In fact given that admin accounts have access to all the data in the system, it’s even more important that accounts are secure.

2 Embrace multi-factor authentication

Available to Microsoft 365 administrator accounts, multi-factor authentication will allow for an additional layer of protection. As an administrator is a user with greater permissions, an account breach can be costly, affecting the data integrity of your business if permission becomes compromised.

MFA should be in place for all users but it’s absolutely essential that all admin accounts are protected.

3 Limit admins within your organisation

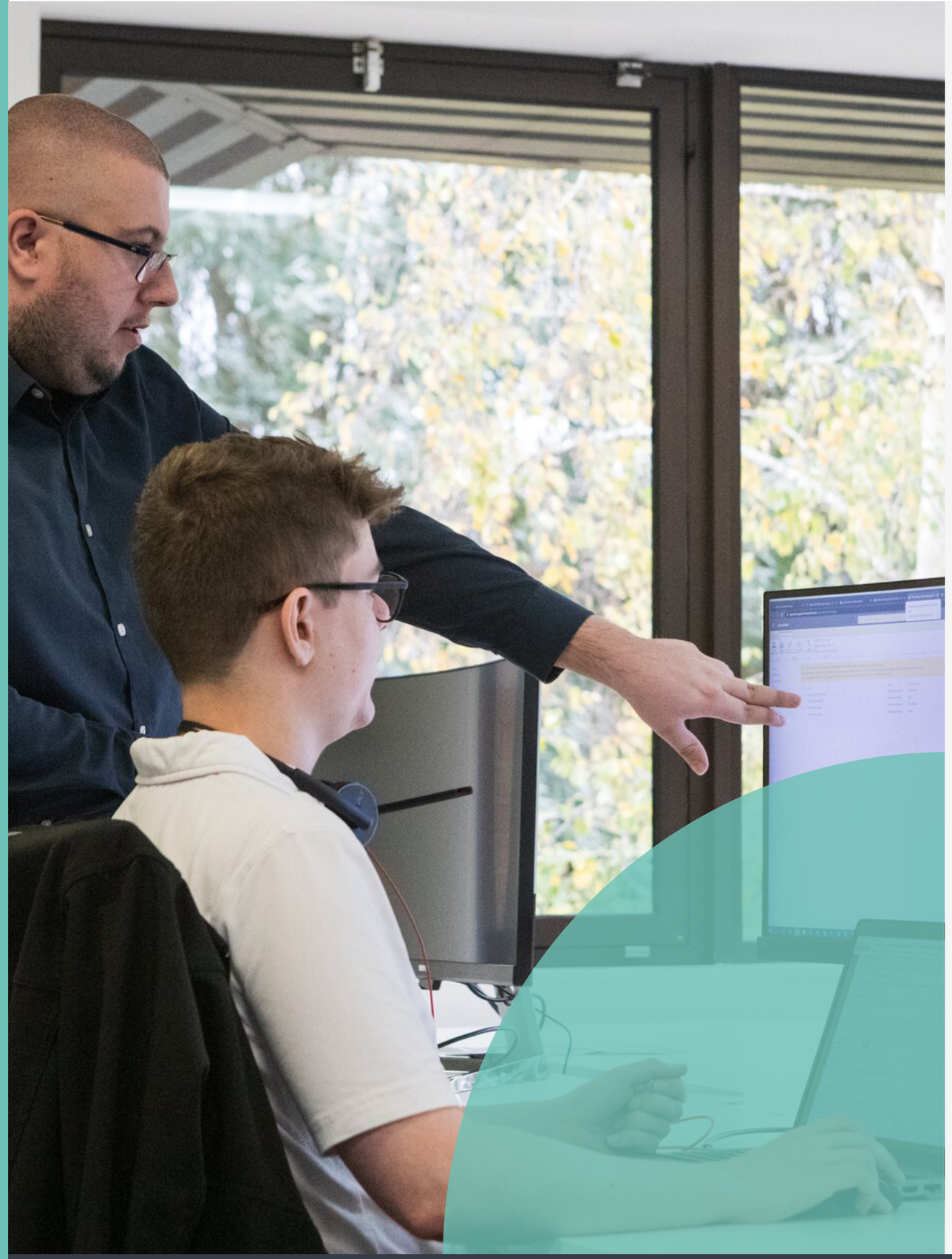
For everyday purposes, ensure that your organisation limits user permissions wherever possible to limit the potential impact of a breach. Users with fewer permissions are safer from the likelihood of a breach, but this will never eliminate the possibility fully. Only through best practice, including strong password techniques, can every user within your organisation evade cybercrime.

4 Create dedicated privileged admins

Admin accounts have much more control, and as such, they are at a greater risk of attack. We therefore recommend they are not used on a day to day basis. Admin users should have two accounts, one they use for day-to-day computing, and an admin account they only log into for admin tasks.

Admin Tip:

Becoming an admin comes with privileges and an even greater risk possibility. A security breach via a 365 privileged account will compromise information and data across your 365 services.



The typical admin tasks you'll encounter

Being tasked with higher permissions means that your day-to-day could be busy with essential admin duties, managing password resets, backing up 365, and more.

Managing services & add-ins

Managing services and additional add-ins across your company is critical to providing a more secure, productive workflow.

Controlled under 'Settings', service management is an important step in assigning and managing add-ins for different groups of workers, including customisation features.

Password policy

Admins have a responsibility when it comes to data security. Not only will admins need to be exemplary at staying on top of strong password health, amongst other security measures, they will need to ensure colleagues are upholding password policies.

User management

Within the admin account, administrators should pay close attention to different user types, upgrading permissions and resetting passwords. Keeping user information current, including account naming and assigned emails, is also critical in larger enterprises, when accounts evolve all the time.

Safe sharing practice

External sharing should be closely monitored and managed using the SharePoint Admin Centre, ensuring that users can't accidentally share sensitive or confidential information from SharePoint outside of the organisation.

Are there any “golden rules” for admin roles?

We’ve been helping businesses administrate Microsoft 365 for years, in all its forms.

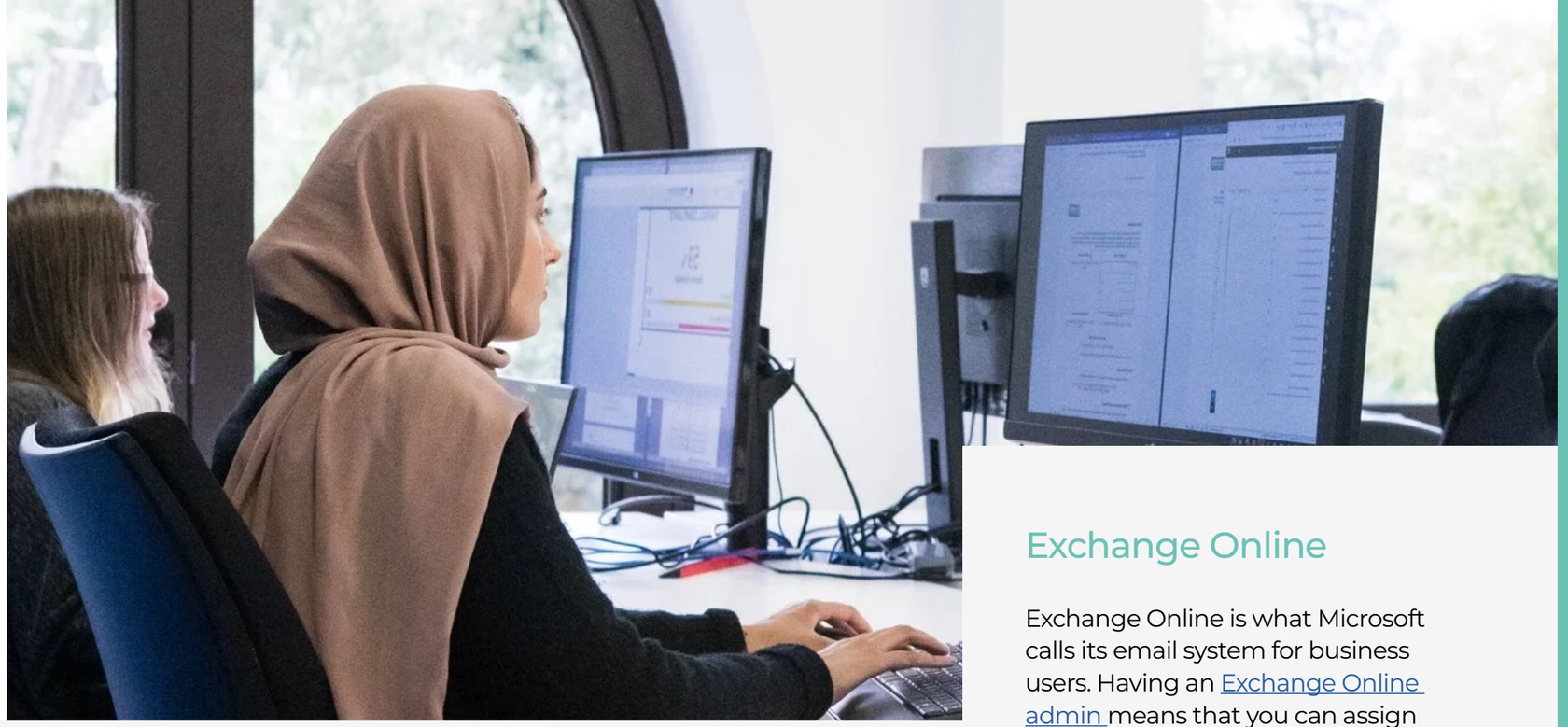
Here are some of the golden rules for Microsoft admins that we’ve learnt over the years:

Microsoft admin rules:

1. Give people the minimum access required, rather than the maximum
2. Limit the number of global admins
3. Enable multi factor authentication (MFA or 2FA) on all accounts
4. Prepare for “break glass” scenarios by having an emergency account without MFA on
5. Do not use Admin Accounts for day-to-day use. Create two separate accounts, one for every day use with non-admin privileges and an admin account that is only used for admin tasks.

Discovering different admin centres

For three of the major platforms within the Microsoft 365 landscape, Microsoft has created specific admin centres to allow for platform level management. These are for more intricate levels of access and mean that individuals within a company can manage day to day functions without the need for access to the rest of the Microsoft suite



Teams

Teams admins have specific roles, such as managing messaging, meeting policies and troubleshooting. Using the Azure Directory, you can assign different levels of Teams management access.

There are five Teams admin levels:

Admin level	What can they do?
Teams administrator	Manage their company's platform and all parts of the Teams platform including meetings, voice calls, messaging, and troubleshooting.
Teams communication administrator	Manage all calling and meeting features, including troubleshooting.
Teams communication support engineer	Manage advanced tools that troubleshoot communication issues.
Teams communication support specialist	Use basic tools to troubleshoot call quality.
Teams device administrator	Manage device configuration policies and set up Teams connected devices.

SharePoint

SharePoint admins can manage the day-to-day running of SharePoint, as well as onboarding and offboarding Microsoft 365 groups. You will need to assign a SharePoint licence to anyone who is a SharePoint admin, they can't fully manage it without it.

The core responsibilities of a SharePoint admin are:

1. Creating and deleting SharePoint sites
2. Managing sharing settings for organisations
3. Adding and removing site admins
4. Managing site storage limits

Exchange Online

Exchange Online is what Microsoft calls its email system for business users. Having an Exchange Online admin means that you can assign responsibility for a user to manage a company's emails, including recovery and mailbox sharing policies.

An Exchange Online admin is responsible for:

1. Recovering deleted items
2. Setting up archive and deletion policies
3. Managing how users can share information with external contacts, like calendars and contacts
4. Delegating 'send as' responsibility to allow users to send mail as other email addresses aside from their own
5. Setting up shared mailboxes and spam protection
6. Managing Microsoft 365 groups

So much more than Microsoft 365 Support – work with ramsac today

We help our clients to understand the roles and responsibilities of different users within their Microsoft 365 products. Segmentation of roles is critical to security and controlling how users interact inside (and outside of) your IT environment. But too much segmentation, on a granular level, can become a hinderance.

That's why we've been working with our partners to make these products more understandable and easier to navigate. Whether that's Microsoft Teams or SharePoint, our experts can help you make the most from 365.

Get in Touch

Find out more

For more information please get in touch:

Call: 01483 412 040

Email: info@ramsac.com

Visit: ramsac.com

ramsac Limited

Godalming Business Centre

Woolsack Way

Godalming, Surrey

GU7 1XW

ramsac.com

01483 412 040

ramsac
the secure choice