Fawley Parish Council – Microsoft 365 Tenant Security Audit

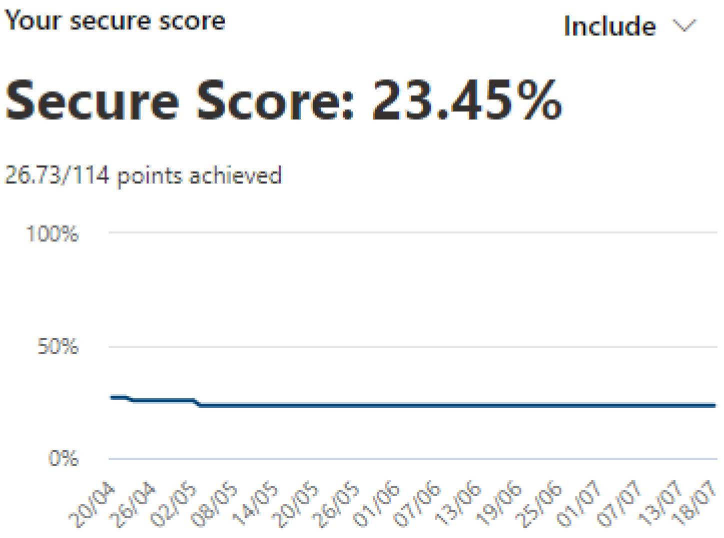
In this document you will find an in-depth analysis of your current Microsoft 365 Tenant.

At the end of each topic, a table will be shown, displaying the action needed to be taken to completely secure your Microsoft 365 Platform.

If you have any questions, please give us a call on 02380 000 999.

Microsoft Secure Score

Microsoft Secure Score is a numerical summary of your security position based on system configurations, user behaviour, and other security-related measurements. It isn't an absolute measurement of how likely your system or data will be breached. Rather, it represents the extent to which you have adopted security controls in your Microsoft environment that can help offset the risk of being breached. No online service is immune from security breaches, and secure score shouldn't be interpreted as a guarantee against security breach in any manner. However, Netserve use this service to help see the impact of your before and after our security report, below is summary of how your secure score looks at the moment at the time of the audit:

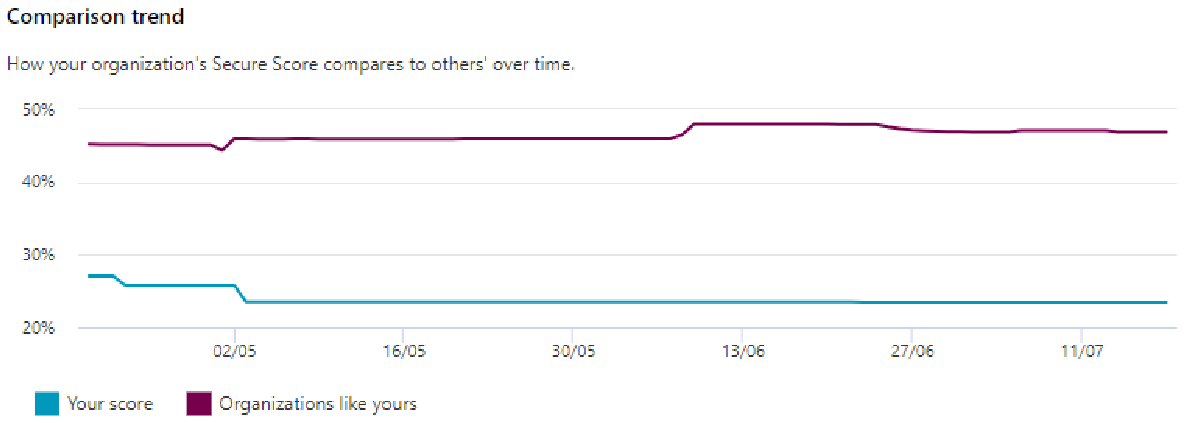


Your secure score

Include

Secure Score: 23.45%

26.73/114 points achieved



Comparison trend

How your organization's Secure Score compares to others' over time.

2 Factor Authentication Setup:

Here are the current list of users that have 2FA Disabled:

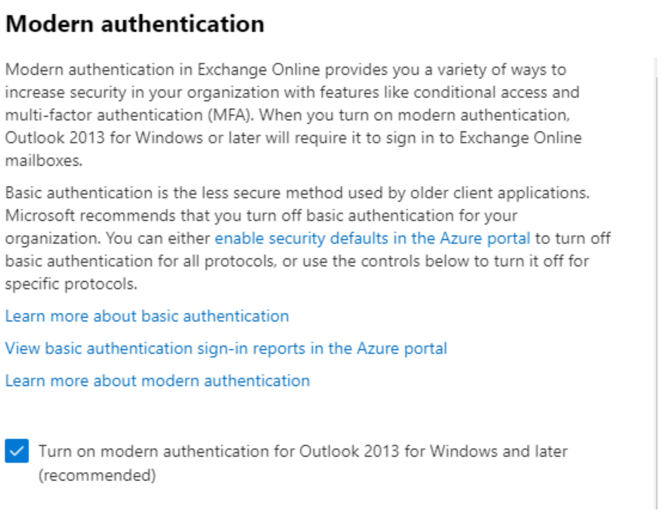
As you can see all users currently have this disabled. The table below lists the action we want to take to secure your Microsoft 365 Platform.

Display name	User principal name	MFA Status
Alan Alvey	Alan.alvey@fawley-pc.gov.uk	Disabled
Alexa Carcas	Alexa.carcas@fawley-pc.gov.uk	Disabled
Allan Glass	Allan.glass@fawley-pc.gov.uk	Disabled
Amy Andrew	youthworker@fawley-pc.gov.uk	Disabled
Beverley Thorne	Beverley.thorne@fawley-pc.gov.uk	Disabled
Centre Manager	joshua.bond@fawley-pc.gov.uk	Disabled
Chas Mcgill	Chas.Mcgill@fawley-pc.gov.uk	Disabled
Dan Poole	dan.poole@fawley-pc.gov.uk	Disabled
Daniel Johnson	dan.johnson@fawley-pc.gov.uk	Disabled
David Mcelhenny	David.mcelhenny@fawley-pc.gov.uk	Disabled
Deputy Clerk	sue.markides@fawley-pc.gov.uk	Disabled
Ethan Cain	ethan.cain@fawley-pc.gov.uk	Disabled
Finance	danni.alexander@fawley-pc.gov.uk	Disabled
Grounds Manager	jason.mansbridge@fawley-pc.gov.uk	Disabled
James Trollope	james.trollope@fawley-pc.gov.uk	Disabled
Josie Poole	Josie.poole@fawley-pc.gov.uk	Disabled
Jubilee Hall	jubileehall@fawley-pc.gov.uk	Disabled
Kathryn Ashdown	kathryn.ashdown@fawley-pc.gov.uk	Disabled
Ken Smith	Ken.smith@fawley-pc.gov.uk	Disabled
Kyran Sugars	kyran.sugars@fawley-pc.gov.uk	Disabled
Maintenance	maintenance@fawley-pc.gov.uk	Disabled
Matthew Hartmann	matthew.hartmann@fawley-pc.gov.uk	Disabled
Michael Billings-Wakerley	michael.billings-wakerley@fawley-pc.gov.uk	Disabled
Natalie Smith	Asst.youthworker@fawley-pc.gov.uk	Disabled

Netserve ash	netserveash@fawley-pc.gov.uk	Disabled
Operations	operations@fawley-pc.gov.uk	Disabled
Paul Saunders	paul.saunders@fawley-pc.gov.uk	Disabled
Reception	reception@fawley-pc.gov.uk	Disabled
Richard Gosnold	richard.gosnold@fawley-pc.gov.uk	Disabled
Sally Read	Sally.read@fawley-pc.gov.uk	Disabled
Shay Milgate	Shay.milgate@fawley-pc.gov.uk	Disabled
Steph Bennett	stephanie.bennett@fawley-pc.gov.uk	Disabled
Steve Chiverton	steve.chiverton@fawley-pc.gov.uk	Disabled
Till	till@fawley-pc.gov.uk	Disabled

Current State	Your current level	Our Recommendations
No users with 2fa enforced	X	Enable all
Some Users with 2fa enforced		Enable remaining
All Users with 2fa enforced		No further action required

LEGACY AUTHENTICATION



Modern authentication

Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA). When you turn on modern authentication, Outlook 2013 for Windows or later will require it to sign in to Exchange Online mailboxes.

Basic authentication is the less secure method used by older client applications. Microsoft recommends that you turn off basic authentication for your organization. You can either enable security defaults in the Azure portal to turn off basic authentication for all protocols, or use the controls below to turn it off for specific protocols.

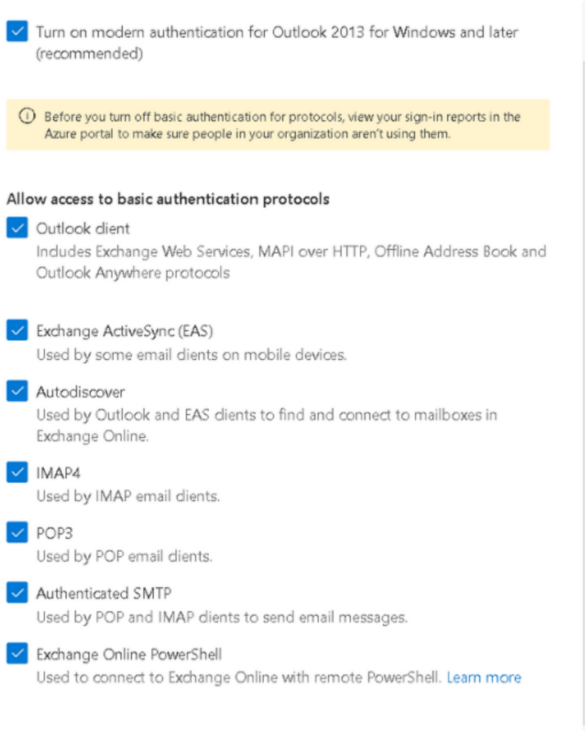
Learn more about basic authentication

View basic authentication sign-in reports in the Azure portal

Learn more about modern authentication

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

As you can see the Tenant currently has Modern authentication ENABLED. This enables less secure access to your mailboxes as well as backdoor access to OneDrive if it is used. It is best to have this enabled to ensure the security methods and protocols you use for your domain are safe and up to date. This is what it should be:



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

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

Allow access to basic authentication protocols

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

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

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

☑ IMAP4
Used by IMAP email clients.

☑ POP3
Used by POP email clients.

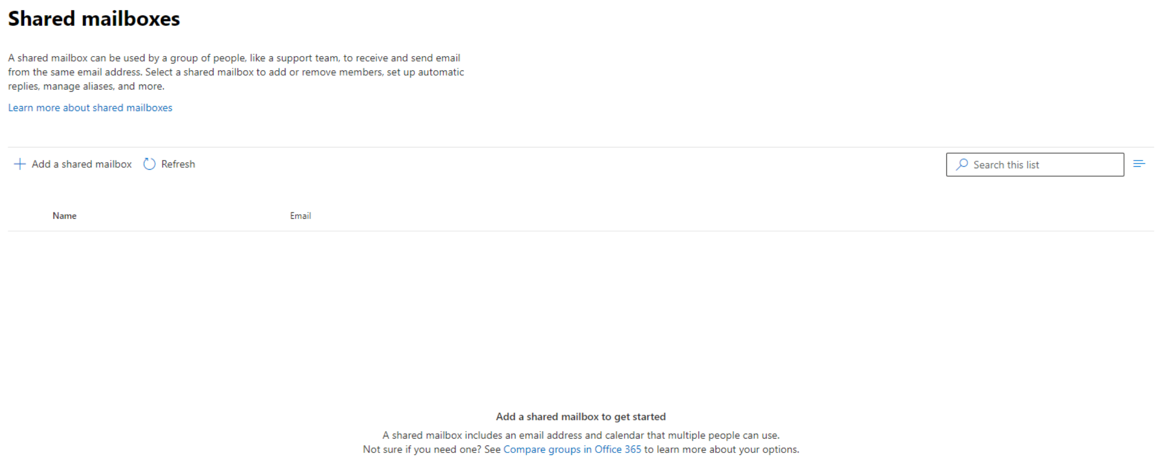
☑ Authenticated SMTP
Used by POP and IMAP clients to send email messages.

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

Current State	Your current level	Our Recommendations
Modern Authentication Disabled		Enable all
Modern Authentication Enabled	X	No further action required

BLOCKING SIGN-ON FOR ALL SHARED MAILBOXES

Users should not sign into shared mailboxes interactively, but rather open shared mailboxes as delegates. Shared mailboxes are often easy targets with weak passwords and no MFA. This is why we will be disabled this by default for your Shared Mailboxes. Here is a list of your current shared mailboxes, please let us know if any of these need their permissions updated:



Shared mailboxes

A shared mailbox can be used by a group of people, like a support team, to receive and send email from the same email address. Select a shared mailbox to add or remove members, set up automatic replies, manage aliases, and more.

Learn more about shared mailboxes

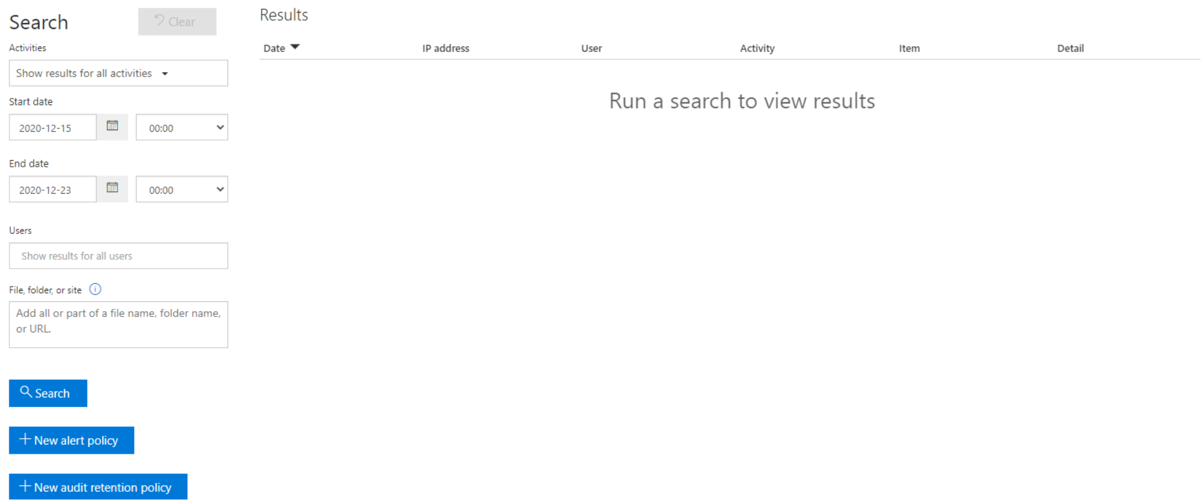
Add a shared mailbox to get started

A shared mailbox includes an email address and calendar that multiple people can use.
Not sure if you need one? See Compare groups in Office 365 to learn more about your options.

Current State	Your current level	Our Recommendations
Shared Mailbox Sign in Enabled		Disable Shared Mailbox Sign-in
Shared Mailbox sign in disabled	X	No further action required

Unified Audit Log

If a user deleted a document or if an admin reset someone's password, we can search the Office 365 audit log to find out what the users and admins in your organization have been doing. We are able to find activity related to email, groups, documents, permissions, directory services, etc. This is turned off by default and needs to be on to monitor these things. After this report we will be enabling this on your tenant.



Activities: Show results for all activities

Start date: 2020-12-15 00:00

End date: 2020-12-23 00:00

Users: Show results for all users

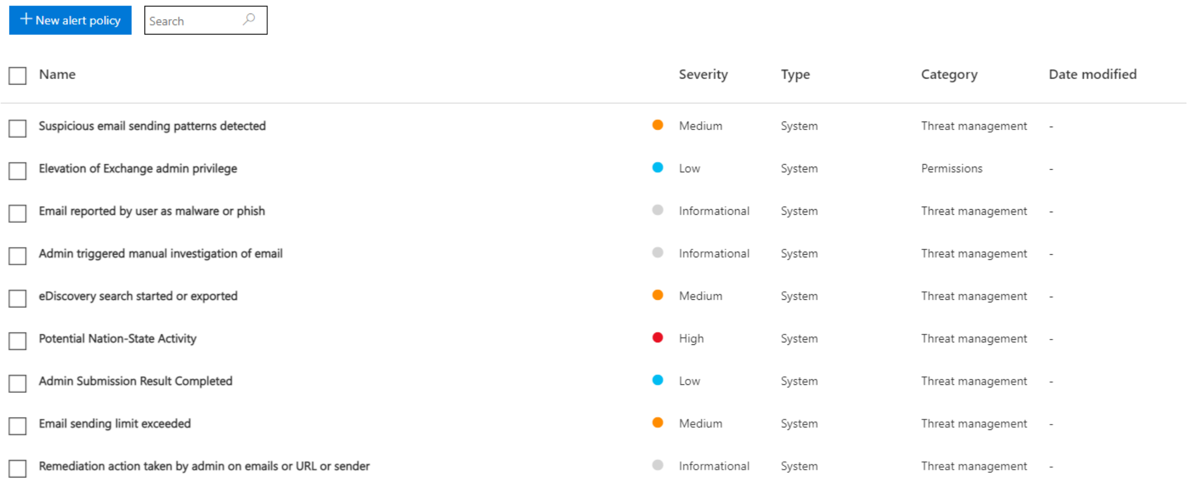
File, folder, or site: Add all or part of a file name, folder name, or URL.

Run a search to view results

Current State	Your current level	Our Recommendations
Audit Log disabled	X	Enable all
Audit log enabled		No further action required

Enabling Alert Policies

Enabling Alert Policies does exactly what it sounds like. You set parameters and conditions and if those conditions get met, then it will notify an administrator, an email of your choice or the user triggering the action. All of these are off by default, but we will be enabling these and getting the alerts sent to our mailbox and we will notify you of any threats. Examples of alerts are shown below:



□ Name	Severity	Type	Category	Date modified
□ Suspicious email sending patterns detected	Medium	System	Threat management	-
□ Elevation of Exchange admin privilege	Low	System	Permissions	-
□ Email reported by user as malware or phish	Informational	System	Threat management	-
□ Admin triggered manual investigation of email	Informational	System	Threat management	-
□ eDiscovery search started or exported	Medium	System	Threat management	-
□ Potential Nation-State Activity	High	System	Threat management	-
□ Admin Submission Result Completed	Low	System	Threat management	-
□ Email sending limit exceeded	Medium	System	Threat management	-
□ Remediation action taken by admin on emails or URL or sender	Informational	System	Threat management	-

Current State	Your current level	Our Recommendations
Alert Policies Disabled		Enable all
Alert Policies Enabled	X	No further action required

Self Service Password Reset

With self-service password reset in Azure Active Directory, users no longer need to engage help desk to reset passwords. This feature works well with Azure AD dynamically banned passwords, which prevents easily guessable passwords from being used. Having this enabled stops the chance of a hack attempt through password cracking. In this scenario, an attacker has acquired access to a service interface, or to a data store that allows them to try many different password combinations for an account. Using specialized software and high-capacity computing, attackers can complete many thousands of combinations in a very short amount of time. If the password is very short, very weak, very common, or the same as another account password owned by the user, the chances are very good that an attacker can guess the password and compromise the account. Therefore, we would recommend enabling this.

Current State	Your current level	Our Recommendations
Self-Service Password Reset disabled	x	Enable all
Self Service Password Reset Enabled		No further action required

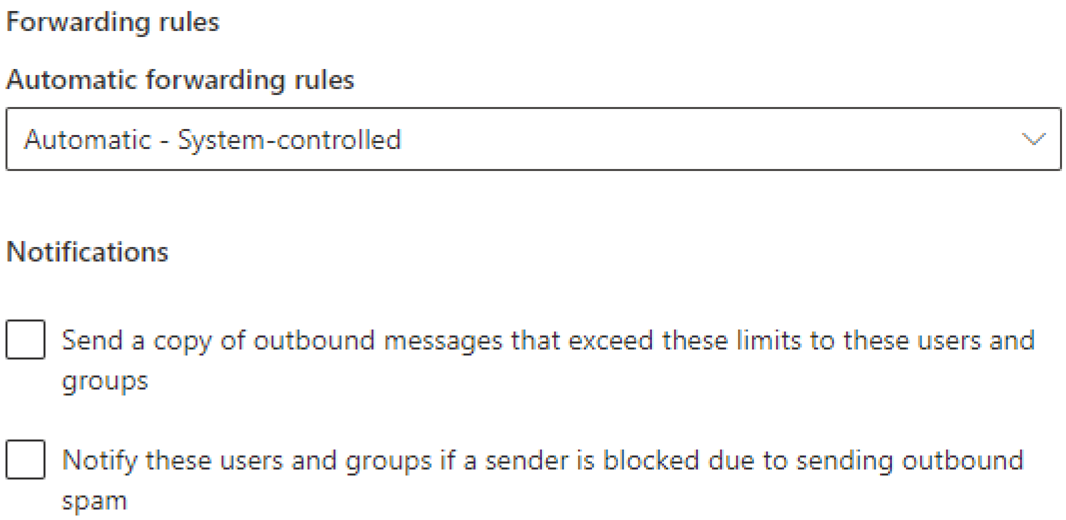
EMAIL AUTHENTICATION

Another thing we would recommend is by adding further email authentication onto your domain. Having already setup an SPF Record to your domain, as this is required by Microsoft 365, there are a few optional records to add, that would better help your spam protection on your emails. This is by adding both a DKIM Record and a DMARC Record to your domain. DMARC stands for Domain-based Message Authentication, Reporting, and Conformance. It is a relatively new email authentication protocol that protects your domain from unauthorized use, also known as email spoofing. DMARC is very effective for organizations because it uses both DKIM and SPF records to validate the sender of an email. A DMARC record allows a sender to indicate that their messages are protected by SPF and/or DKIM and tells a receiver what to do if neither of those authentication methods passes – such as junk or reject the message. DKIM on the other hand stands for Domain Keys Identified Mail, which is an email authentication method. This method is used to detect spoofed, or fake sender email addresses. It is also another way to link an email back to a domain. When using DKIM, a sender can attach DKIM signatures to an email (header that is added to the message and is secured with encryption), and once the recipient receives the email, they can verify that it is actually you who sent it. The biggest reason why DKIM is so important for your organization is because spoofing emails from trusted domains is a popular technique for phishing campaigns, and DKIM makes it harder to spoof emails from domains that use it.

Current State	Your current level	Our Recommendations
Spam Filtering Records not-added	X	Add records
Spam Filtering Records added.		No further action required

DISABLE MAILBOX AUTO-FORWARDING TO REMOTE DOMAINS

Another thing to harden your current Microsoft 365 is to disable auto-forwarding to other domains. Here are the current settings that are setup:



Forwarding rules

Automatic forwarding rules

Automatic - System-controlled

Notifications

□ Send a copy of outbound messages that exceed these limits to these users and groups

□ Notify these users and groups if a sender is blocked due to sending outbound spam

Current State	Your current level	Our Recommendations
Mailbox auto-forwarding Enabled	X	Disable all
Mailbox auto-forwarding Disabled		No further action required

All Mail Forwarding Results

Here are the results after a test on your tenant of all the active forwarders on your profile:

Source Email Address	Forwarding?	Destination Email Address:
N/A	N/A	N/A

Current State	Your current level	Our Recommendations
Mailbox forwarding Setup		Disable all external/Old forwarding
No Mailbox forwarding Setup	X	No further action required

User Admin Roles

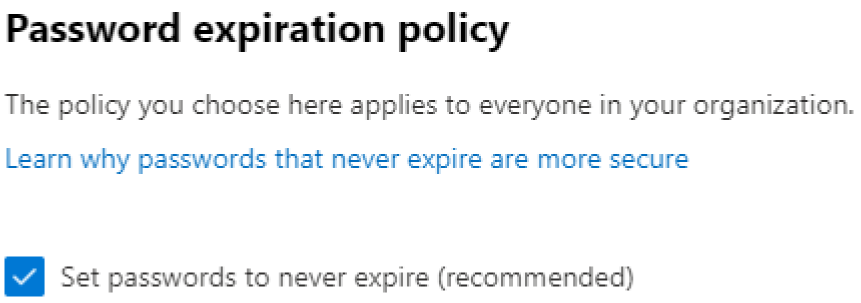
Below are the results of a report that shows which users have access rights and to what parts in your Microsoft 365 Tenant. Microsoft recommends having more than one Global Admin so users can still get access to the tenant in the event of one of the global admins being logged out. However, Microsoft recommends that day-to-day mailboxes should not have admin privileges and separate global admins should be created, this means that, as the admin accounts aren't being used day-to-day, there is a lot less risk of them being signed into.

joshua.bond@fawley-pc.gov.uk - User admin

Current State	Your current level	Our Recommendations
Mailboxes have Admin Rights	x	Create additional users with Global Admin Rights, and remove mailbox permissions.
Separate users have been created for users with Admin Rights		No further action required

Password Reset Policy

Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason and recommends that cloud-only tenants set the password policy to never expire.



Password expiration policy

The policy you choose here applies to everyone in your organization.

Learn why passwords that never expire are more secure

☑ Set passwords to never expire (recommended)

Current State	Your current level	Our Recommendations
Password Reset Policy Enabled		Enable, with 90 day reset.
Password reset policy Disabled	X	No further action required

ADVISORIES:

We have included some recommendations that are not compulsory but would help your business and employee’s security. Here they are:
- Using a password Manager to manage your password instead of an ordinary web browser, like this one: https://lastpass.com
- Bitlockering Laptops. This is something we manage and include in all of our setups, this is just to raise awareness that all devices including desktops are recommended to be bitlockered.
- Upgrade your Azure AD License to Azure AD Premium P1, this will include options like Conditional Access (Block Sign-in attempts outside of UK) and give the tenant the ability to disable the use of commonly used passwords, and set banned passwords, across Office 365 and Windows Logins. For more information, please speak to a member of the team.