Office 365 Review

Sample Report

Table of Contents

Key Observations and Recommendations

This section provides key observations and relevant recommendations.

Office 365 Review

Kaon Security performed a detailed review of the current configurations of Microsoft Office 365 and Office 365 specific items within Azure Active Directory for SAMPLE ORGANISATION and found the following issues:

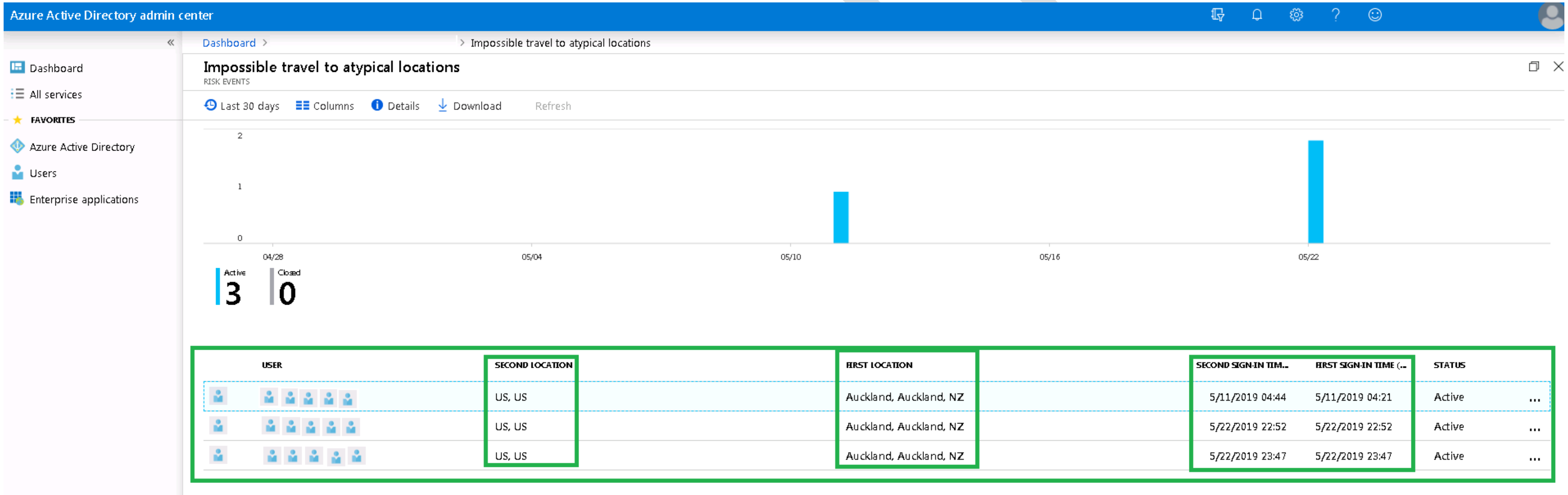
1. App registration is allowed for non-administrative users. This unmoderated registration process could allow a user to register insecure applications, resulting in data and device compromise.
2. SAMPLE ORGANISATION infrastructure allows users to join any new device to their Office 365 account without a defined approval process. In the case of a compromised account, an attacker would have easy access to register rogue devices.
3. TEXT REMOVED.
4. TEXT REMOVED.
5. TEXT REMOVED.
6. TEXT REMOVED.
7. TEXT REMOVED.
8. TEXT REMOVED.
9. TEXT REMOVED.
10. TEXT REMOVED.
11. TEXT REMOVED.
12. TEXT REMOVED.
13. TEXT REMOVED.
14. TEXT REMOVED.
15. TEXT REMOVED.
16. TEXT REMOVED.
17. TEXT REMOVED.
18. TEXT REMOVED.
19. TEXT REMOVED.
20. TEXT REMOVED.
21. TEXT REMOVED.
22. TEXT REMOVED.
23. TEXT REMOVED.
24. TEXT REMOVED.
25. TEXT REMOVED.
26. TEXT REMOVED.
27. TEXT REMOVED.
28. TEXT REMOVED

Remediation

This section highlights various remediation points categorised in order of their effectiveness and complexity to implement.

Urgent Attention Required

This section looks through some of the items in urgent need of review or analysis. We consider these items to potentially be active risks and recommend attending to them ASAP.



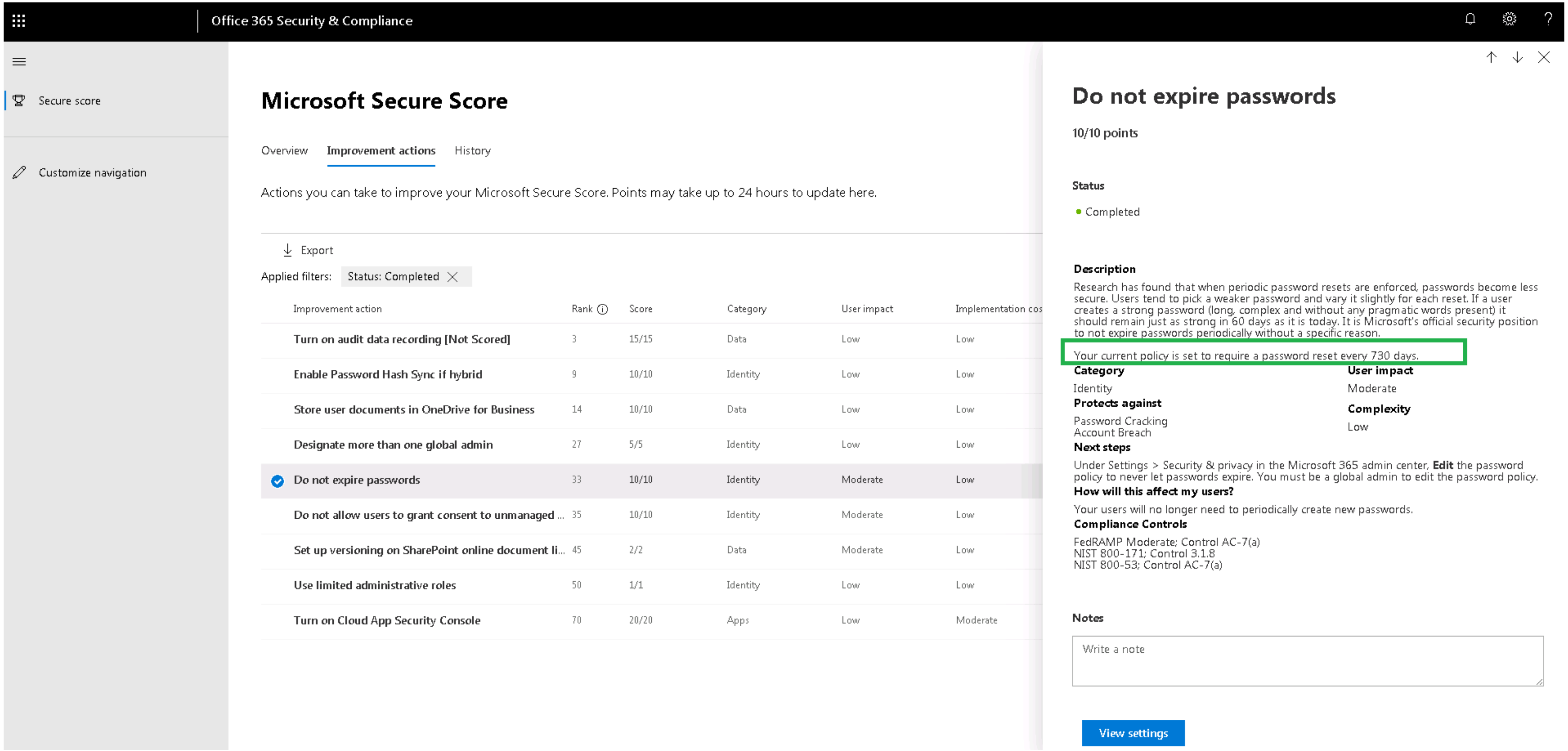
Impossible travel to atypical locations

RISK EVENTS

USER	SECOND LOCATION	FIRST LOCATION	SECOND SIGN-IN TIM...	FIRST SIGN-IN TIME (...	STATUS	
	US, US	Auckland, Auckland, NZ	5/11/2019 04:44	5/11/2019 04:21	Active	...
	US, US	Auckland, Auckland, NZ	5/22/2019 22:52	5/22/2019 22:52	Active	...
	US, US	Auckland, Auckland, NZ	5/22/2019 23:47	5/22/2019 23:47	Active	...

Quick Win - High Security Impact

This section looks through some of the high impact fixes with the least complexity to implement. We recommend following the steps as marked within the screenshots.



Microsoft Secure Score

Actions you can take to improve your Microsoft Secure Score. Points may take up to 24 hours to update here.

Applied filters: Status: Completed

Improvement action	Rank	Score	Category	User impact	Implementation cos
Turn on audit data recording [Not Scored]	3	15/15	Data	Low	Low
Enable Password Hash Sync if hybrid	9	10/10	Identity	Low	Low
Store user documents in OneDrive for Business	14	10/10	Data	Low	Low
Designate more than one global admin	27	5/5	Identity	Low	Low
✓ Do not expire passwords	33	10/10	Identity	Moderate	Low
Do not allow users to grant consent to unmanaged ...	35	10/10	Identity	Moderate	Low
Set up versioning on SharePoint online document li...	45	2/2	Data	Moderate	Low
Use limited administrative roles	50	1/1	Identity	Low	Low
Turn on Cloud App Security Console	70	20/20	Apps	Low	Moderate

Do not expire passwords

10/10 points

Status

● Completed

Description

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 60 days as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason.

Your current policy is set to require a password reset every 730 days.

Category

Identity

User impact

Moderate

Protects against

Password Cracking
Account Breach

Complexity

Low

Next steps

Under Settings > Security & privacy in the Microsoft 365 admin center, **Edit** the password policy to never let passwords expire. You must be a global admin to edit the password policy.

How will this affect my users?

Your users will no longer need to periodically create new passwords.

Compliance Controls

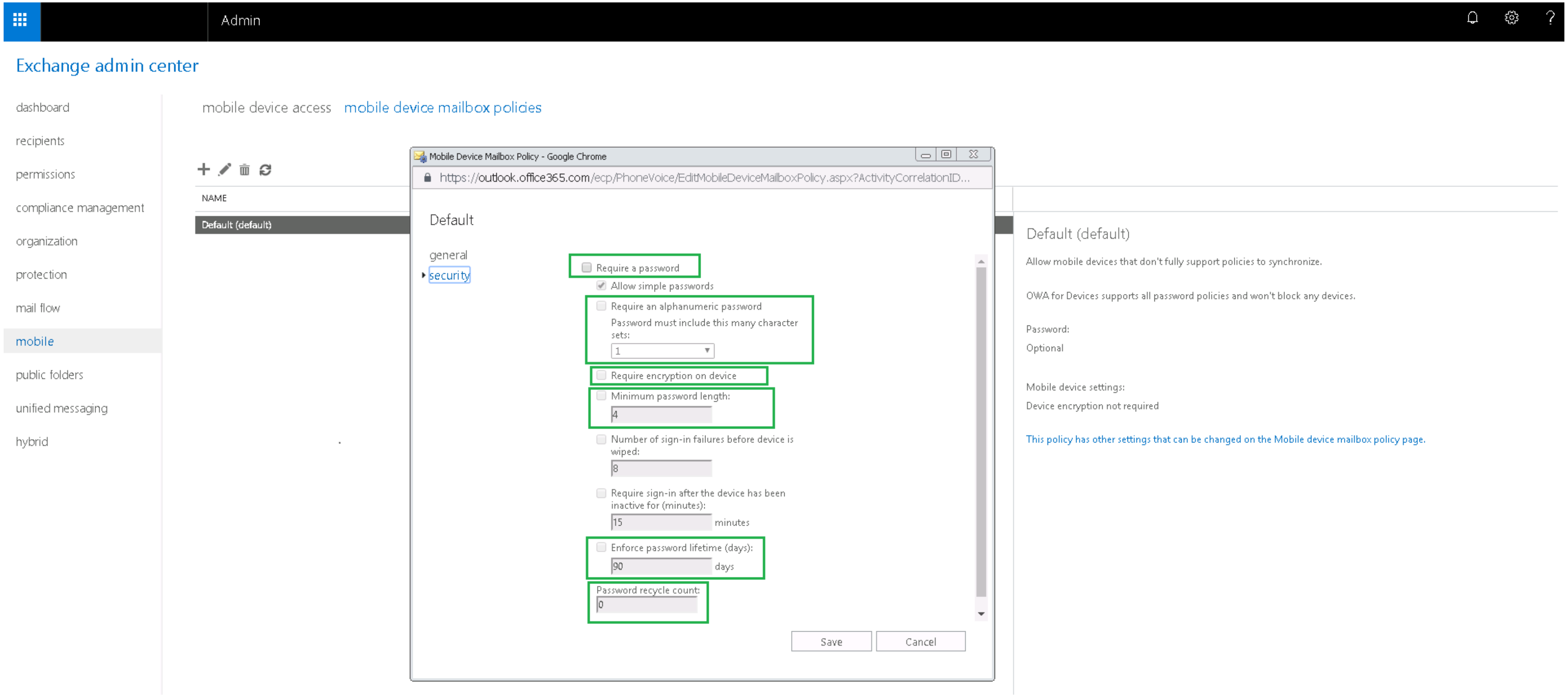
FedRAMP Moderate; Control AC-7(a)
NIST 800-171; Control 3.1.8
NIST 800-53; Control AC-7(a)

Notes

Write a note

Opportunities for Improvement

This section looks through some of the opportunities SAMPLE ORGANISATION can avail of at no additional cost. This would contribute significantly to improve the overall security posture of the Office 365 environment.



https://outlook.office365.com/ecp/PhoneVoice/EditMobileDeviceMailboxPolicy.aspx?ActivityCorrelationID...

Default

- □ Require a password
- ☑ Allow simple passwords
- □ Require an alphanumeric password
  Password must include this many character sets: 1
- □ Require encryption on device
- □ Minimum password length: 4
- □ Number of sign-in failures before device is wiped: 8
- □ Require sign-in after the device has been inactive for (minutes): 15 minutes
- □ Enforce password lifetime (days): 90 days
- Password recycle count: 0

Default (default)

Allow mobile devices that don't fully support policies to synchronize.

OWA for Devices supports all password policies and won't block any devices.

Password:
Optional

Mobile device settings:
Device encryption not required

This policy has other settings that can be changed on the Mobile device mailbox policy page.