May 2021

Microsoft 365 Tenant Security Audit

City of Austin, TX

Objective

Analyze and develop a series of operational recommendations for improving the City of Austin Azure AD / Microsoft 365 cloud environment and ongoing management. The following technical areas were reviewed as part of this engagement.

- Windows Active Directory (local)
- Azure Active Directory
- Exchange Online
- SharePoint Online
- OneDrive for Business Online

This assessment reports on actionable findings and targets areas that will reduce risk, data loss, and improve productivity for the City of Austin. Remediation of the findings in this report will significantly reduce risk, data loss potential, and account compromise. However, threats to cloud services are constantly evolving.

Content has been removed to protect client information and to show a limited number of findings in the ***SAMPLE*** report.

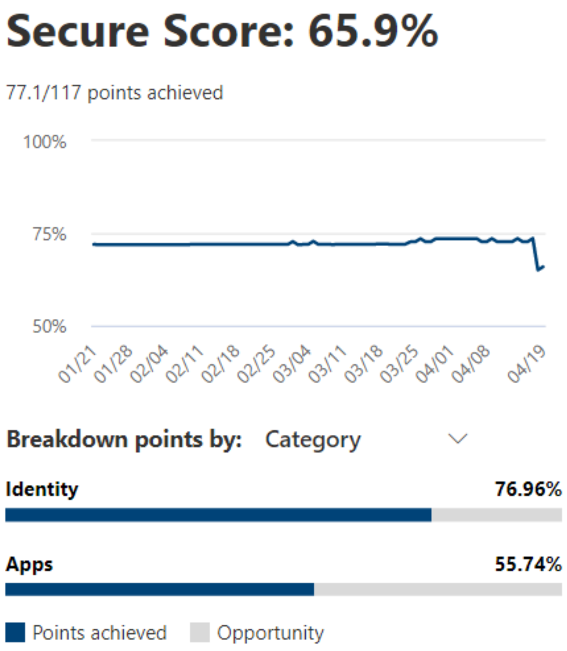
Contents

Microsoft 365 Tenant Summary:

The City of Austin Microsoft 365 tenant was established in August of 2016 and hosts several SMTP domains controlled by City of Austin. The Microsoft 365 tenant currently holds all mailboxes and public folders. Identities. Attributes, and password hashes are synchronized from the local City of Austin Windows Active Directory.

Microsoft Secure Score:

Secure Score is a security analytics tool that will help you understand what you have done to reduce the risk to your data and show you what you can do to further reduce that risk. We think of it as a credit score for security. The current secure score for City of Austin Microsoft 365 tenant is 66.



Secure Score: 65.9%

77.1/117 points achieved

Breakdown points by: Category

Identity 76.96%

Apps 55.74%

Licensing:

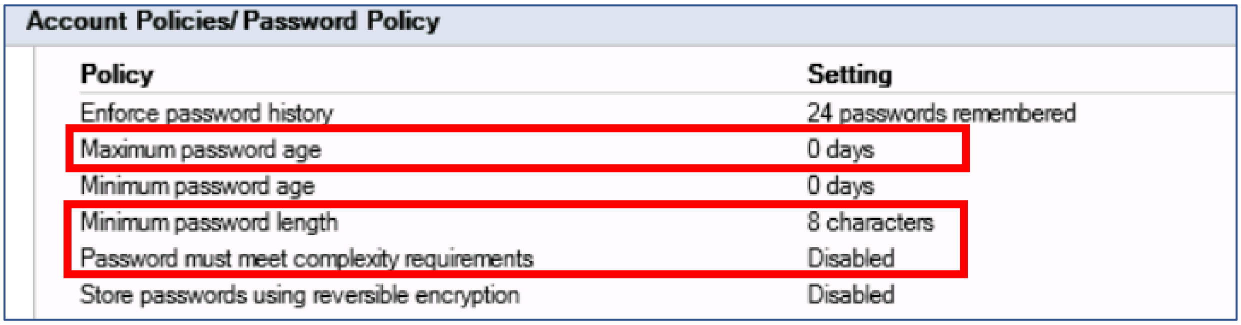
License Name	Purchased	Assigned
Office 365 Government E1	497	447
Office 365 Government E3	794	790
Exchange Online Archiving for Government	530	447
Office 365 Advanced Threat Protection for Government	1291	1291
Project Online Professional for Government	13	5
Visio Online Plan 2 for Government	16	12

FINDING – Weak Domain Password Policy

The same username and passwords are leveraged across the City of Austin domain, workstations, and the Microsoft Azure / Microsoft 365 cloud. The password policy enforcement at City of Austin is extremely relaxed and does not enforce any complexity or minimum requirements. This will almost certainly lead to Microsoft 365 accounts being accessed by malicious entities. EMA recommends the following baseline as a minimum.

- Enforce Password History: **24 Passwords Remembered**
- Maximum Password Age: **90 Days**
- Minimum Password Length: **12 Characters**
- Password must meet complexity requirements: **ENABLED**

Current City of Austin Domain Password Policy



Account Policies/ Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	0 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

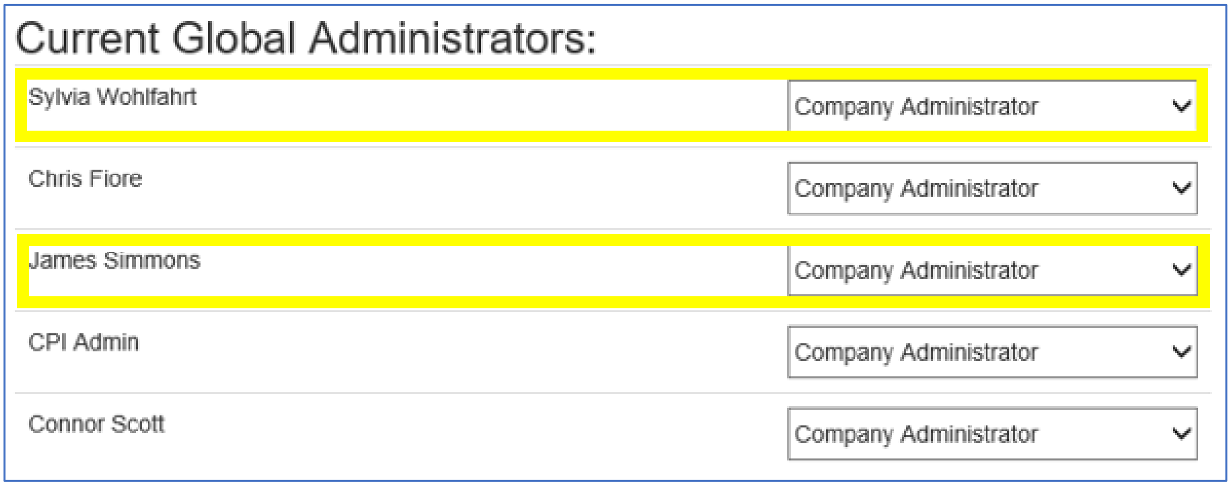
FINDING - Enable Multi-Factor Authentication (MFA) for all global admins

It is recommended to enable MFA for all Microsoft 365 admin accounts because a breach of any of these accounts can lead to a breach of any of your Microsoft 365 stored data.

When you enable MFA for your Global Administrators, they will be prompted to authenticate with a 2nd factor upon logging into Microsoft 365 web services. The second factor is most commonly a phone call or text message to a registered cell phone number where they type in an authorization code, or with a mobile application called Azure Authenticator.   We found that you had 5 admins out of 6 that did not have MFA enabled.

FINDING – Global Admin Accounts

There are accounts remaining as global admins in the City of Austin tenant that belong to former employees. The more global admin users you have, the more likely it is that one of those accounts will be successfully breached by an external attacker.



Current Global Administrators:

Sylvia Wohlfahrt	Company Administrator
Chris Fiore	Company Administrator
James Simmons	Company Administrator
CPI Admin	Company Administrator
Connor Scott	Company Administrator

FINDING - Enable mailbox auditing for all users

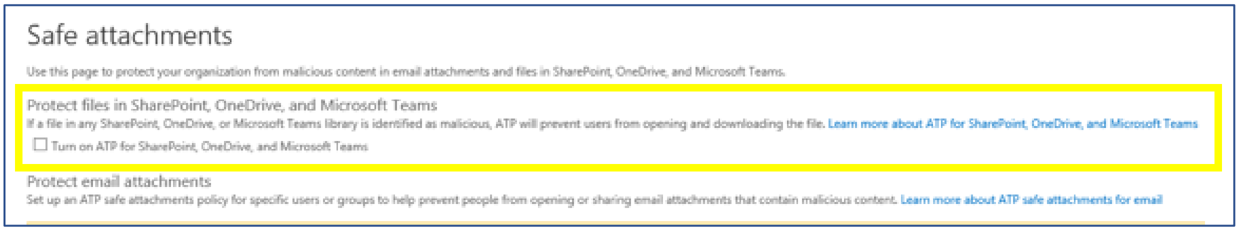
It is recommended to enable mailbox auditing for all users that have mailboxes in your Microsoft 365 tenancy. By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached.

FINDING - Enable Advanced Treat Protection (ATP)

Advanced Threat Protection (ATP) New malware campaigns are being launched every day and Microsoft 365 has a solution to help protect your email, files, and online storage against them. By protecting against unsafe attachments and expanding protection against malicious links, it complements the security features of Exchange Online Protection to provide better zero-day protection. ATP is comprised of three main components; Safe Attachments, Safe Links, Advanced Phishing Filtering.

ATP Safe Attachments

City of Austin should enable the ATP Attachment protection for files that reside in SharePoint, OneDrive, and Teams to provide the most secure ATP settings.



Safe attachments

Use this page to protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Microsoft Teams.

Protect files in SharePoint, OneDrive, and Microsoft Teams

If a file in any SharePoint, OneDrive, or Microsoft Teams library is identified as malicious, ATP will prevent users from opening and downloading the file. Learn more about ATP for SharePoint, OneDrive, and Microsoft Teams

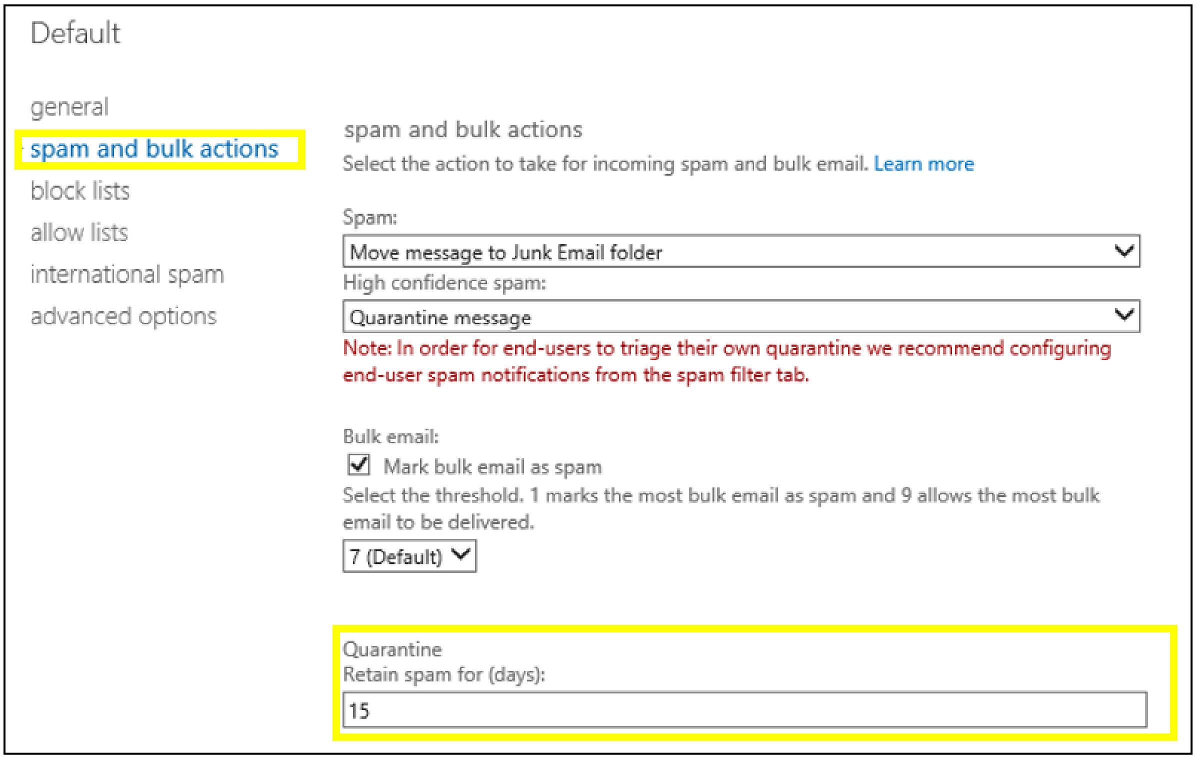
☐ Turn on ATP for SharePoint, OneDrive, and Microsoft Teams

Protect email attachments

Set up an ATP safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious content. Learn more about ATP safe attachments for email

FINDING – Quarantine Retainment

Microsoft has recently increased how long quarantined emails can be retained. The old maximum was 15 days, the new maximum is 30 days.



Default

spam and bulk actions

Select the action to take for incoming spam and bulk email. Learn more

Spam:
Move message to Junk Email folder

High confidence spam:
Quarantine message

Note: In order for end-users to triage their own quarantine we recommend configuring end-user spam notifications from the spam filter tab.

Bulk email:

☑ Mark bulk email as spam

Select the threshold. 1 marks the most bulk email as spam and 9 allows the most bulk email to be delivered.

7 (Default)

Quarantine
Retain spam for (days):
15

FINDING – International SPAM setting disabled

International Spam settings can filter email messages that are written in specific languages or sent from specific countries and regions. You can configure up to 86 different languages and 250 different regions. The service will apply the configured action for high-confidence spam (Junk Mail). The City of Austin currently has less than 10 blocked countries and less than 10 blocked languages. Our recommendation is to filter as many *non-English* and *non-U.S.* based communications as possible to avoid unsolicited email.

FINDING – DKIM Not Enable for Outgoing Email

DKIM (Domain keys Identified Mail)

DKIM is a method to validate the authenticity of email messages. When each email is sent, it is signed using a private key and then validated on the receiving mail server (or ISP) using a public key that is in DNS. This process verifies that the message was not altered during transit.

Currently DKIM is not enabled on outgoing email messages sent from the City of Austin tenant.

Remediation:

1. Establish Required DNS for DKIM
2. Enable DKIM for @austintexas.gov

FINDING – DMARC not established $

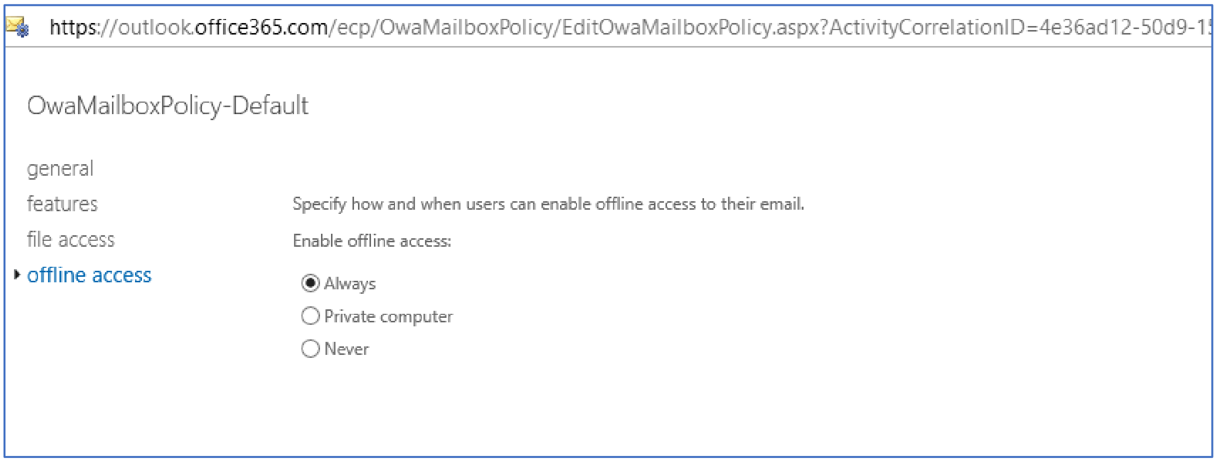
DMARC (Domain-based Message Authentication, Reporting & Conformance)

DMARC is a standard that prevents malicious use of your email domains to send email without your permission — also known as spoofing, phishing, or whaling. With SPF and DKIM, it is up to the receiving email system to decide what to do with the results. DMARC takes it a step further and gives you full control to set a policy to reject or quarantine emails from sources you do not specify as trusted. Like SPF and DKIM, this policy resides in DNS.

Full DMARC conformance will protect both your internal users and external customers from emails spoofing or phishing from the City of Austin controlled domains.

FINDING – Outlook Web Access (OWA) Offline Access

By default, Microsoft 365 (Exchange Online) allows users to enable an offline cache of all their email when using OWA. This can lead to corporate data loss when an employee is leave City of Austin or if their personal computer is compromised. EMA recommends disabling Offline OWA access to limit data loss.



https://outlook.office365.com/ecp/OwaMailboxPolicy/EditOwaMailboxPolicy.aspx?ActivityCorrelationID=4e36ad12-50d9-1

OwaMailboxPolicy-Default

Specify how and when users can enable offline access to their email.

Enable offline access:

● Always
○ Private computer
○ Never

FINDING - Azure Active Directory Connect – DIRSYNC Version

Microsoft Azure AD Connect (Directory Sync) is installed on **Ulster-O365.ulster.county**. Directory Synchronization between the local City of Austin Active Directory and the Microsoft 365 online directory is scheduled to run every 30 minutes.

Microsoft Azure AD Connect (AADC) is not running the latest version from Microsoft as of July 2018.

AADC Server	Installed Version	Latest Version
Ulster-O365.ulster.county	1.1.819.0	1.1.880.0

Actions and Status

Urgent Actions

These findings require immediate attention and represent material deficiencies in the City of Austin Microsoft 365 environment. Remediation of these items limit potential failure or exposure that will impact business operations resulting in potential loss of data, loss of revenue, compromised data, or reputation damage within industry

Priority	Remediation Task	Status	Date Discovered
1	Weak Domain Password Policy	NA – Being addressed with 3rd party software	**05/2021**
2	Enable MFA for all global admins	In-Progress Enabled Connor. Connor knows how to add individuals to MFA	**05/2021**
3	Remove Old Global Admin Accounts	Completed	**05/2021**
4	Enable Advanced Treat Protection (ATP)	In-Progress • Remediated Safe Attachments and Safe Links Policies. • Need to setup Anti-Phishing Policy. Connor knows how to add individuals to the policy	**05/2021**
5	Establish DMARC Conformance	Requires PSA or Agreement with EMA.	**05/2021**

Recommended Actions

These findings represent significant risk factors to the computing environment and should be scheduled for remediation as a priority once the urgent actions have been addressed.

Priority	Remediation Task	Status	Date Discovered
6	Client Access Rules	Completed	**05/2021**
7	Enable Common Attachment Types Filter	Completed	**05/2021**
8	Enable International SPAM settings	Completed	**05/2021**
9	Enable DKIM for Outgoing Email	Completed	**05/2021**
10	Disable OWA Offline Access	Completed	**05/2021**
11	Disable External Skype Access	Completed	**05/2021**

Maintenance Actions

These findings represent recommend best practice for the ongoing health and wellbeing of the City of Austin Microsoft 365 environment.

Priority	Remediation Task	Status	Date Discovered
12	Enable mailbox auditing for all users	Completed	**05/2021**
13	Increase Quarantine Retainment	Completed	**05/2021**
14	Upgrade Azure Active Directory Connect	Completed	**05/2021**
15	Correct Azure AD Connect Sync Errors	In-Progress	**05/2021**
16	Enable OneDrive Domain Security	Completed	**05/2021**

Priority Planning

Priority	Remediation Task	Status	Date Discovered
NA	Implement Azure AD Premium		**05/2021**