1. MATT (**M**icrosoft 365 conditional **A**ccess **T**riage **T**ool) – is attached as a text file (“MATT – M365 cA Triage Tool.txt”) to copy and paste from – **we’re very excited about this** and **I think it will provide a lot of value to everyone** – I will cover running this during the webinar!

MATT (**M**icrosoft 365 conditional **A**ccess **T**riage **T**ool) – is a PowerShell script that you just need to copy and paste into the PowerShell 7.x command line and it will run and try and authenticate you twice (global admin needed) (also, sometimes initial authentication fails, so might need to be run twice if it does).  When it authenticates you, no need to check to consent for the entire organization.  This will put a report in the C:\Temp folder.

1. Also, there is another text file (“Verify Audit Logging.txt”) with a script that checks whether unified audit logging and mailbox audit logging are enabled.  Unified audit logging is for the tenant; mailbox audit logging is on by default and by user.  The disconnect script is contained in this text file, so copying and pasting the entire script will force the disconnect after being run.  This will produce a report in the C:\Temp folder.  We will show how to run this also during the webinar.
2. PowerShell 7.5 install link (both above scripts reference will require this; other scripts may or may not require this, but definitely work with 7.5)
	1. x64 (64 bit): <https://github.com/PowerShell/PowerShell/releases/download/v7.5.0/PowerShell-7.5.0-win-x64.msi>
	2. x86 (32 bit): <https://github.com/PowerShell/PowerShell/releases/download/v7.5.0/PowerShell-7.5.0-win-x86.msi>
3. Below are some links and notes on security settings we’ll be discussing as well.  The links are safe – you can always search through Microsoft 365 to find the actual settings, but providing here to make it easier.
4. Similar to the network, ensure global admin accounts are separate and cloud-only, as privileged access should not be assigned to an individual’s normal user account (e.g., create an admin.jdoe@company.onmicrosoft.com account and assign it global admin privileges). Note: Make sure to sign in and get MFA established on the new global admin account and remove global admin capability from the normal user account.  We will show how to do this on the webinar.
5. Block authentication flows (device auth). Conditional access policies are required in order to accomplish this, so licensing changes may be necessary (business premium at a minimum).
	* + See <https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-authentication-flows> for more details.
6. Block user consent.
	* + See <https://entra.microsoft.com/#view/Microsoft_AAD_IAM/ConsentPoliciesMenuBlade/~/UserSettings?Microsoft_AAD_IAM_legacyAADRedirect=true> for more details.
7. Block user ability to create app passwords.
	* + See <https://account.activedirectory.windowsazure.com/UserManagement/MfaSettings.aspx?BrandContextID=O365> for more details.
8. Block all external domains to prevent unmanaged external Teams users from starting a conversation with people in the organization
	* + (<https://admin.teams.microsoft.com/company-wide-settings/external-communications>).
9. Block ability for users to share their calendars with people outside your organization
	* + (<https://admin.microsoft.com/Settings> -> Org Settings -> Calendar).
10. Control external SharePoint sharing
	* + (<https://admin.microsoft.com/Settings> -> Org Settings -> SharePoint)
11. Ensure that "Users can register applications" feature is disabled within your Microsoft Entra ID settings so that only Microsoft Entra ID administrators can register third-party applications after these are reviewed and evaluated from the security standpoint.
	* + See <https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserManagementMenuBlade/~/UserSettings> for more details.
12. Exchange device ActiveSync Quarantine
	* + See <https://admin.cloud.microsoft/exchange#/mobiledeviceaccess>
		+ If using this, wanting to see device access that has been allowed, then run the script found in the attached text file (“Mobile Device Access.txt”) in PowerShell 7.x.  This will put a script in the C:\Temp folder.
		+ To remove access, navigate to <https://admin.cloud.microsoft/exchange#/mailboxes>, click on the user, then click on “Manage mobile devices” and select the device and click “Block access”.
		+ If doing this, or even if not doing this, the SIEM should be set to alert on all new Intune enrollments.
		+ There is a work around to not needing a SIEM – it sounds like you can alert the user themselves if a new device is enrolled.  The key here would be to create a mailflow rule to forward any email to that user to IT if it matches the specific subject line.  Seth Earby (searby@forsynse.com) will be putting a video together on how to do this, so I will have it available on my website once he’s done that.
13. Disable automatic forwarding to external domains
	* + <https://admin.cloud.microsoft/exchange#/remotedomains>
		+ Click on “Default” then “Edit reply types” then uncheck “Allow automatic forwarding”
14. Not necessarily a security related item, but if wanting to do a “catch-all” type of email address where if an email is sent to an address that isn’t a user (e.g., z@yourdomain.com), you can set it up to go to a “catch-all” address.  In our company’s case, I have those set to come to me (kkothari@sgcsecure.com).  It’s a manual process that needs to be kept up to date, but I wanted to share how we are doing this.
	* + Mail Flow: <https://admin.cloud.microsoft/exchange#/transportrules>
		+ Add Rule
		+ Name the rule
		+ After the “And” choose “Redirect message to”  ….  “these recipients”
			1. Specify the “catch-all” address(s)
		+ Except if “The recipient” … “is this person”
			1. Specify addresses you don’t want forwarded to the “catch-all”



1. “Block sign-in” for all shared mailboxes. Note: when creating a shared mailbox, this should be blocked by default.  Attached is a text file (“Shared Mailboxes.txt”) that identifies all shared mailboxes and whether they have blocked sign-ins or not and places a report in the “C:\Temp” folder.

If any aren’t blocked, determine why, and if sign-in isn’t needed, then go to <https://admin.microsoft.com/> -> Active Users -> Identify and click on the shared mailbox, the click the “Block sign-in” button.