Office 365 Security Audit Guide

**Microsoft Secure Score**

Check the Microsoft Secure Score before and after audit to track progress and look for areas of improvement. It may take 48 hours for score to fully update.

<https://security.microsoft.com/securescore?viewid=overview>

**Install the Microsoft Exchange Online PowerShell module**

**(From Edge browser)**

Office 365 Admin > Exchange > Classic Exchange Admin Center > Hybrid >

Configure (PowerShell Module)

**Connect to Exchange Online PowerShell and Office 365 Admin**

Check SharePoint Kbase for admin login

Launch Exchange PowerShell and enter the following command to connect:

Connect-EXOPSSession

**Enable Organization Customization**

Enable-OrganizationCustomization

**Enable audit log search**

Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true

**Create a secondary global administrator**

Office 365 Admin > Users > Add a user

New account: mcallen@theirdomain.onmicrosoft.com

Deselect automatically create password and use password generator to create password

Add account info to the Kbase

Do not use a license to create account, ***Set as Global Admin***

Enable MFA for the new account. Ideally use the Authy shared McAllen account

If asked for phone number, use: **502-767-1917**

If asked for email, use: **helpdesk@mcalleninc.com**

**Enable multi-factor authentication for all user and admin accounts**

Office 365 Admin > Search, ‘MFA’ > configure

Check that all **licensed accounts** have MFA enforced or enabled

If unlicensed and account is not in use, block user sign-in

<https://o365reports.com/2019/05/09/export-office-365-users-mfa-status-csv/>

Run PowerShell script “GetMFAStatus.ps1” located in McAllen Base to export a detailed list of MFA, license, and admin status of user accounts.

Install-Module MSOnline

Set-ExecutionPolicy Unsigned

**Set passwords to never expire**

Office 365 Admin > Setup > Set passwords to never expire

**Enable self-service password reset**

***MFA should be enabled for all accounts before using self-service passwords reset***

Office 365 Admin > Setup > Let users reset own passwords > Get Started > All > Save

Registration > Require users to register when signing in? > No (need to test)

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

**Check accounts for existing forwarding rules**

Removing any existing auto-forwarding left from before the implementation of the new role

As the forwarding can be set to both internal and external recipients you might want to export a list of the mailboxes which had configured the settings before the Role Assignment Policy modifications. This will allow you to remove only the forwarding to external addresses with precision:

Create a folder on the C drive called ‘mcallen’ (if one doesn’t exist)

Get-Mailbox -ResultSize Unlimited -Filter {(RecipientTypeDetails -ne "DiscoveryMailbox") -and ((ForwardingSmtpAddress -ne $null) -or (ForwardingAddress -ne $null))} | Select Identity | Export-Csv c:\mcallen\ForwardingSetBefore.csv -append

Check the Excel File in the McAllen folder

Ignore the below command if the excel file is empty.

If you want to remove any kind of forwarding regardless the location:

Get-Mailbox -filter {(RecipientTypeDetails -ne "DiscoveryMailbox") -and ((ForwardingSmtpAddress -ne $null) -or (ForwardingAddress -ne $null))} | Set-Mailbox -ForwardingSmtpAddress $null -ForwardingAddress $null

**Disable automatic forwarding to external domains**

Disabled automatic forwarding to external domains from *Exchange Admin Center > Mail flow > Remote Domains* OR

The cmdlet below will disable the forwarding to all external domains. If you want to restrict this for particular domains only replace you can do so as well.

Set-RemoteDomain Default -AutoForwardEnabled $false

https://docs.microsoft.com/en-us/archive/blogs/exovoice/disable-automatic-forwarding-in-office-365-and-exchange-server-to-prevent-information-leakage

**Check accounts for existing inbox rules**

As that setting will be applicable for all newly sent emails but will not eliminate the rules, you can use the cmdlet below will export a list of the mailboxes which have forwarding, redirection or message deletion rules configured, review them and remove them upon demand as well:

foreach ($a in (Get-Mailbox -ResultSize Unlimited |select PrimarySMTPAddress)) {Get-InboxRule -Mailbox $a.PrimarySMTPAddress | ?{($\_.ForwardTo -ne $null) -or ($\_.ForwardAsAttachmentTo -ne $null) -or ($\_.DeleteMessage -eq $true) -or ($\_.RedirectTo -ne $null)} |select Name,Identity,ForwardTo,ForwardAsAttachmentTo, RedirectTo, DeleteMessage | Export-Csv c:\mcallen\InboxRules.csv -append }

Check the Excel file

Ignore the below command if the excel file is empty.

Remove-InboxRule -Mailbox user@domain.com -Identity "RuleName"

**Create mail flow rule to block and alert users of auto-forwarding to external domains**

Another option which you might consider, as it will be notifying your users as well, is to configure a transport rule to handle the blocking of any auto-forward message types:

Note: Applying the following action 'Enable Client Rules Forwarding Block Advanced Action' from Secure Score in Office 365 Security and Compliance Center will create a new transport rule for your organization.

#It will stop external messages leaving your Tenant, that are of the type AutoForward, mitigating the use of Client created external mail forwarding rules and malicious Remote Domain entries as a data exfiltration vector.

Exchange Admin Center > Mail Flow, Rules > New Rule > More Options

Rule name: *Block and notify auto forwarding*

Conditions:

The Sender > is external/internal > 'Inside the organization'

The Recipient > is external/internal > 'Outside the organization'

The message properties > message type > 'Auto-Forward'

Do the following:

Block the message > Reject the message with the explanation >

Explanation: *External Mail Forwarding via Client Rules is not permitted*

Save

**Create Safe Attachments Policy to block messages with detected malware**

MAY NOT BE AN OPTION DUE TO LICENCES

Office 365 Admin > Security > Threat Management, Policy> Safe Attachments

Create New (or edit existing) > Apply to domain > Block current and future messages and attachments with detected malware

**Enable Common Attachment Types Filter blocking in anti-malware policy, modified to include all malicious file types and notify users**

Office 365 Admin > Security > Threat Management, Policy> Anti-malware

Create New (or edit existing default) >

Enable common attachments filter > Customize file types > Select all

Notify internal senders when messages are quarantined > Save

**Enable auto-quarantine of high confidence spam and phishing emails and enable end-user notifications**

Office 365 Admin > Security > Threat Management, Policy > Configuration Analyzer

Anti-spam recommendations

**Check configuration analyzer for and other recommendations not currently implemented**

Office 365 Admin > Security > Threat Management, Policy > Configuration Analyzer

**\*Below only necessary if you need to disable auto-forwarding on an account-by-account level\***

**Modify the Default Role Assignment Policy for all users by replacing MyBaseOptions with MyBaseOptions-DisableForwarding**

Enabled Organization customization in Office 365 tenant via PowerShell:

Enable-OrganizationCustomization

Create new mail management role 'MyBaseOptions-DisableForwarding'

#As you can’t modify the build-in role MyBaseOptions, you need to create a new role to replace it with.

#Create a new management role based on the MyBaseOptions role:

New-ManagementRole MyBaseOptions-DisableForwarding -Parent MyBaseOptions

#Remove the forwarding parameters from the MyBaseOptions-DisableForwarding role

Set-ManagementRoleEntry MyBaseOptions-DisableForwarding\Set-Mailbox -RemoveParameter -Parameters DeliverToMailboxAndForward,ForwardingAddress,ForwardingSmtpAddress

#Note: If you want to retrieve the parameters that will be left available for the Set-Mailbox cmdlet after the modification of the role which you’ve created:

(Get-ManagementRoleEntry MyBaseOptions-DisableForwarding\Set-Mailbox).parameters

#As you have created the role, you have 2 options – modifying the default policy for all users or creating a different policy and assign it to a targeted group of people.

#3.1. Modify the Default Role Assignment Policy for all users by replacing MyBaseOptions with MyBaseOptions-DisableForwarding.The easiest way to do this is from **Exchange Admin Center > Permissions > User Roles > edit the Default Role Assignment Policy > clear MyBaseOptions and then select MyBaseOptions-DisableForwarding**.

#3.2. Create a new role assignment policy which will contain the MyBaseOptions-DisableForwarding role

New-RoleAssignmentPolicy -Name DisabledForwardingRoleAssignmentPolicy -Roles MyBaseOptions-DisableForwarding,MyContactInformation,MyRetentionPolicies,MyMailSubscriptions,MyTextMessaging,MyVoiceMail,MyDistributionGroupMembership,MyDistributionGroups, MyProfileInformation

#After creating the new policy, you can apply it to targeted user for example:

Set-Mailbox –Identity user@domain.com -RoleAssignmentPolicy DisabledForwardingRoleAssignmentPolicy

#Note: Give it some time to replicate after the change.

**Enable Security Defaults**

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-block-legacy-authentication>

This will do the following:

* Requiring all users to register for Azure AD Multi-Factor Authentication.
* Requiring administrators to perform multi-factor authentication.
* Blocking legacy authentication protocols.
* Requiring users to perform multi-factor authentication when necessary.
* Protecting privileged activities like access to the Azure portal.

**Before enabling, check the sign-in logs to verify they are not using legacy authentication methods.**

Azure Active Directory > Sign-ins > Add filter – Client App > Select all legacy

**Check Smtp Auth Client Report**

<https://protection.office.com/reportv2?id=SmtpClientSubmissionReport&pivot=SenderDomain>

Azure Active Directory > Properties > Manage Security defaults

OR Admin Portal > Setup > Enable Security Defaults

**Restrict anonymous users from joining Teams meetings**

1. Log into [Microsoft Teams admin center](https://admin.teams.microsoft.com/)  
2. In the left navigation, go to **Meetings** > **Meeting Settings**  
3. Under the Participants section, toggle “Anonymous users can join a meeting” to **Off**

**Do not allow users to grant consent to unmanaged applications**

To prevent users in your organization from allowing third-party apps to access their Office 365 information, and require future consent operations to be performed by an administrator, go to the [Azure Active Directory admin center](https://go.microsoft.com/fwlink/?linkid=2119526) > Enterprise applications > User settings > Enterprise applications. Set the toggle "Users can consent to apps accessing company data on their behalf" to **No**.  
  
Optionally, you can set up a process for your users to request access to third-party applications. In the Azure portal, configure an admin consent workflow by going to [Enterprise applications > User settings.](https://go.microsoft.com/fwlink/?linkid=2119526) Under Admin consent requests, set "Users can request admin consent to apps they are unable to consent to" to **Yes**. Select your preferences for the rest of the admin consent requests options. Select **Save**. It can take up to an hour for the feature to become enabled.

**Prevent sign-ins from outside the US**

*Requirements: Azure Active Directory Premium P1 or P2. Only possible if Security Defaults are not enabled.*

Azure Active Directory > Security > Named locations > + Countries locations > United States

Azure Active Directory > Security > Conditional Access > Policies > New Policy

Name: Block Sign-ins outside the US

Include: All users, exclude users if needed

Cloud app or actions > Include all cloud apps

Conditions > Locations > Include, any location; Exclude, US

Grant > Block access

By default, policy with be created in Report-only mode. Run this to test and check for affected users from the Azure Active Directory sign-ins page. Once tested, set policy to On.

## Billing Notes Template:

Remote Work:

- Create secondary global administrator account and enable multi-factor authentication

- Verify all licensed users and administrators have multi-factor authentication enabled

- Enabled self-service password reset

- Enabled audit log search

- Checked user mailboxes for existing forwarding rules

- Disabled automatic forwarding to external domains

- Created mail flow rule to block and alert users of auto-forwarding to external domains

- Check user mailboxes for existing inbox rules

- Enabled Common Attachment Types Filter blocking in anti-malware policy, modified to include all malicious file types and notify users

- Enabled auto-quarantine of high confidence spam and phishing emails and enable end-user notifications

- Check configuration analyzer for other recommendations not currently implemented

- Enabled Office 365 Security defaults to require MFA for new users and block legacy authentication methods

- Disabled access of unauthorized third-party integrated applications

- Restrict anonymous users from joining Teams meetings

<https://azurescene.com/2020/03/30/block-legacy-authentication/>