



**Hardening  
Office 365  
Playbook:  
SMB Edition**

## Purpose

The primary purpose of this document is to minimize the potential for a data breach or a compromised account by following Microsoft security best practices and step through the actual configuration.

## Audience

This document was designed for the SMB market who primarily work with the Business skus (Premium/Essentials) available from Microsoft.

## Versioning

Version	Date	Author	Notes
1.0	June 2018	MSP4MSPs	Original document published

Checklist:

Secure Score	
<a href="#">Enable MFA</a>	<a href="#">Review Mailbox Forwarding Rules Weekly</a>
<a href="#">Enable Client Rules Forwarding Block</a>	
<a href="#">Enable Audit Log Search</a>	<a href="#">Review the Mailbox Access Non-Owners Report Biweekly</a>
<a href="#">Enable Mailbox Auditing for All Users</a>	<a href="#">Review the Malware Detections Report Weekly</a>
<a href="#">Set Up Outbound Spam Notifications</a>	
<a href="#">Review Role Changes Weekly</a>	<a href="#">Review your account provisioning activity report weekly</a>
<a href="#">Designate More than 1 global Admin</a>	<a href="#">Do not allow Calendar details sharing</a>
<a href="#">Configure Expiration Time for External Sharing Links</a>	<a href="#">Review Sign-Ins after Multiple Failures report weekly</a>
<a href="#">Enable Versioning on all SharePoint Online Document Libraries</a>	<a href="#">Tag Documents in SharePoint</a>

Exchange Online Protection/Antispam Policies	
<a href="#">Configure Connection Filtering</a>	
<a href="#">Configure Spam Filtering</a>	
<a href="#">Configure Outbound filtering</a>	
<a href="#">Configure Mail Flow Rules</a>	
<a href="#">Configure Malware Settings</a>	

DNS Settings	
<a href="#">Configure SPF Record</a>	
<a href="#">Configure DKIM Record</a>	
<a href="#">Configure DMARC Record</a>	

## Contents

Use Office 365 Secure Score .....	5
Enable MFA .....	6
Enable Client Rules Forwarding Blocks .....	10
Enable Audit Log Search .....	11
Enable Mailbox Auditing for All Users .....	14
Set Up Outbound Spam Notifications .....	15
Review Role Changes Weekly .....	16
Review Mailbox Forwarding Rules Weekly .....	17
Review the Mailbox Access by Non-Owners Report Bi-Weekly .....	17
Review the Malware Detections Report Weekly .....	18
Review your Account Provisioning Activity Report Weekly .....	22
Do not Allow Calendar Details Sharing .....	23
Review Sign-Ins after Multiple Failures report weekly .....	25
Designate More than 1 Global Admin .....	27
Do Not Allow External Domain Skype Communications .....	29
Configure Expiration Time for External Sharing Links .....	31
Enable Versioning on all SharePoint Online Document Libraries .....	33
Tag Documents in SharePoint .....	38
Exchange Online Protection/Antispam Policies .....	48
Connection Filtering: .....	48
Spam Filtering: .....	51
Outbound filtering: .....	56
Mail Flow Rules: .....	56
Malware: .....	58
DNS Settings .....	60

## Using Office 365 Secure Score

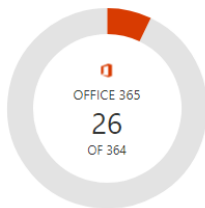
Microsoft Secure Score

Your Secure Score Summary

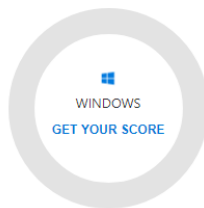
26

Jun 6, 2018 6:00 PM

Of 364



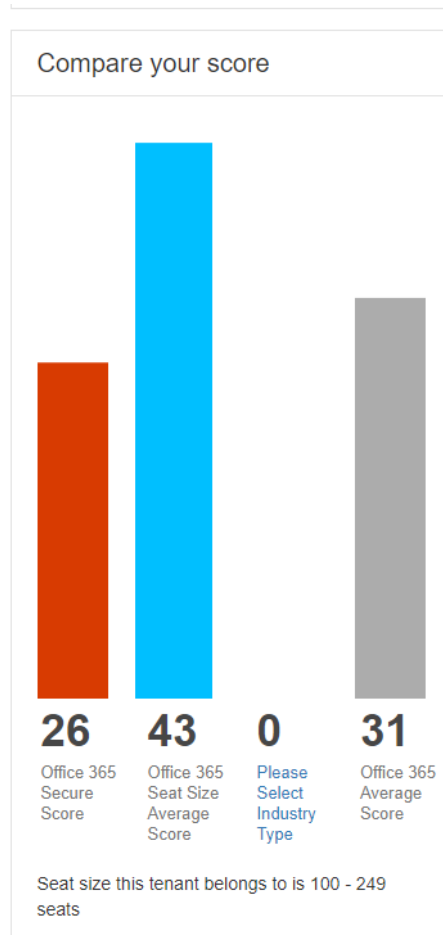
For more information about your Secure Score go to: [Score Analyzer](#)



Get the full security story with a [free Windows Defender ATP trial](#)

You can think of secure score like a credit score for Office 365. Secure Score figures out what Office 365 services you're using (like OneDrive, SharePoint, and Exchange) then looks at your settings and activities and compares them to a baseline established by Microsoft. You'll get a score based on how aligned you are with best security practices. The numerator is your current point value and the denominator is the amount of points available based on the security features you have available to configure. You can see the list of available security options for each Microsoft plan by clicking on [this link](#)

Microsoft compares your score to 365 accounts with a similar seat size as your organization and allows you to configure your Industry Type to compare your score to others in your industry as well.

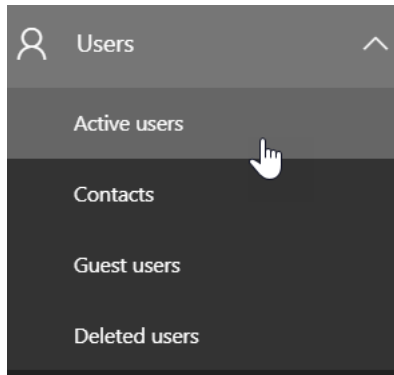


Below is a checklist to help boost your score:

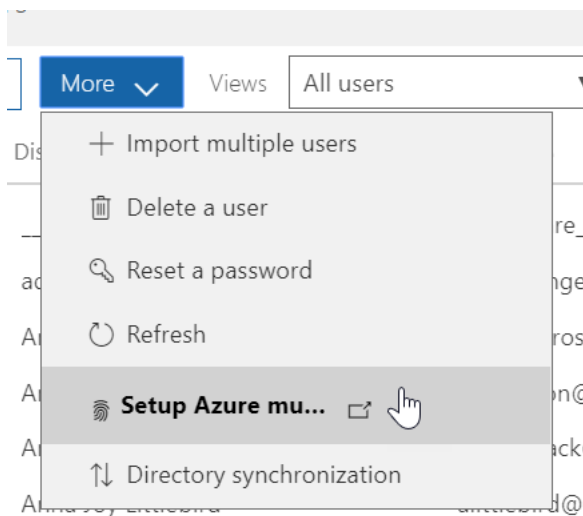
### Enable MFA

You should enable MFA for all of your user accounts because a breach of any of those accounts can lead to a breach of any data that user has access to.

1. Go to the 365 Admin Center>Users>Active Users



2. Click "More">Set Azure Multifactor Authentication



### 3. Select Users to Enable Multifactor Authentication

multi-factor authentication  
users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

[bulk update](#)

View:

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	[blurred]	[blurred]	Enabled
<input type="checkbox"/>	[blurred]	[blurred]	Disabled
<input checked="" type="checkbox"/>	[blurred]	[blurred]	Disabled
<input checked="" type="checkbox"/>	[blurred]	[blurred]	Disabled
<input checked="" type="checkbox"/>	[blurred]	[blurred]	Disabled
<input checked="" type="checkbox"/>	[blurred]	[blurred]	Disabled

19 selected

[quick steps](#)  
[Enable](#)  
[Manage user settings](#)

4. The next time the user signs in they will be prompted with the following:






For added security, we need to further verify your account



[Redacted email address]

Your admin has required that you set up this account for additional security verification. 

[Set it up now](#)

[Sign out and sign in with a different account](#)

[More information](#)

©2018 Microsoft

[Terms of use](#) [Privacy & cookies](#)



5. Depending on your settings they will enter a phone used for the second form of authentication. You can adjust the settings by going to "Service Settings" on the top of the multifactor page:

## multi-factor authentication

users service settings

app passwords

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app

remember multi-factor authentication

- Allow users to remember multi-factor authentication on devices they trust  
Days before a device must re-authenticate (1-60):

save

## Enable Client Rules Forwarding Blocks

This is a transport rule to help stop data exfiltration with client created rules that auto-forwards email from user's mailboxes to external email address. This is an increasingly common data leakage method in more organizations.

```
IF The Sender is located 'Inside the organization'  
AND IF The Recipient is located 'Outside the organization'  
AND IF The message type is 'Auto-Forward'  
THEN Reject the message with the explanation 'External Email Forwarding via Client Rules is not permitted'.
```

To enable:

1. Click Learn More in the Secure Score Portal

## 2. Click Apply

×
**Enable Client Rules Forwarding Block**

**What am I about to change?**

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

1. Client created external mail forwarding Rules, such as the Outlook desktop client.
2. Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
3. Admins can create external transport rules to forward messages.
4. Client created ForwardingSmtpAddress via Outlook Web Access interface.

This Security Control action will help mitigate Client created external mail forwarding rules.

A simple mitigation is to, on each Remote Domain, including the Default to disallow Auto-Forwarding. This is a global setting and applies to every email sent from within a Tenant, as a result it is a very broad approach, which does not allow white listing. More details can be found [here](#). RBAC roles can be used to achieve a similar result.

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

1. Clients will receive a custom NDR message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
3. Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.

This Security Control will create a transport rule that 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.

1. If The Sender is located 'Inside the organization'
2. If The Recipient is located 'Outside the organization'
3. If The message type is 'Auto-Forward'
4. Reject the message with the explanation 'External Mail Forwarding via Client Rules is not permitted'

We found that you had 0 Rules out of 0 that did have blocks enabled.

Apply
More ▾
Cancel

## 3. This auto-creates a Transport rule in EAC under Mail Flow>Rules. This is where you would come to modify/delete

[rules](#) [message trace](#) [url trace](#) [accepted domains](#) [remote domains](#) [connectors](#)

ON	RULE	PRIORITY
<input checked="" type="checkbox"/>	Client Rules To External Block - Secure Score 6/6/2018	0

## Enable Audit Log Search

You should enable audit data recording for your Office 365 service to ensure that you have a record of every user and administrator's interaction with the service, including Azure AD, Exchange Online, and SharePoint Online/OneDrive for Business. This data will make it possible to investigate and scope a

security breach, should it ever occur. You (or another admin) must turn on audit logging before you can start searching the Office 365 audit log.

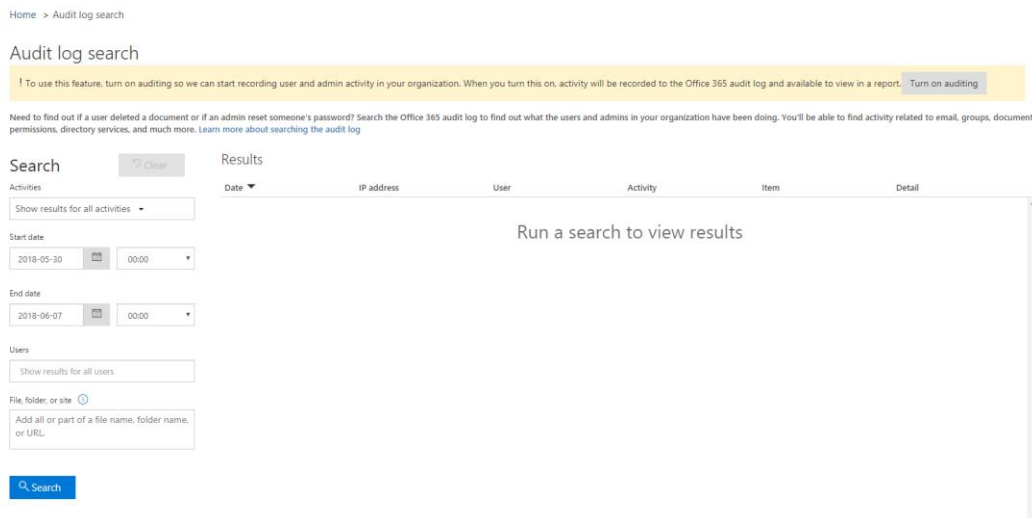
Questions to Ask:

1. How often do I want to get reports on audit log data? (Recommended bi-weekly)
2. Is there a certain environment I need to more closely monitor? (Exchange, SharePoint, OneDrive, etc)

### [How to Turn the Audit Log On](#)

### [How to Search the Audit Log](#)

1. Go to Admin Centers>Security and Compliance Center>Search & Investigation>Audit Log search



## Audit log search

! We're preparing the Office 365 audit log. You'll be able to search for user and admin activity in a couple of hours.

2. Create a custom search based off of:
  - a. Activity
  - b. Date Range
  - c. Users
  - d. File/Folder/Site

**Search** Clear

Activities

Show results for all activities ▾

Start date

2018-05-30 📅 00:00 ▾

End date

2018-06-07 📅 00:00 ▾

Users

Show results for all users

File, folder, or site ⓘ

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

🔍 Search

+ New alert policy

## Create a New Alert Policy based off a certain event

New alert policy
✕

**Name \***

**Description**

**Alert type**

Custom
▾

**Send this alert when... \*** ▾

**Activities \***

Choose activities for alert
▾

**Users:**

Show results for all users

---

**Send this alert to... \*** ▴

**Recipients \***

Show results for all users

Feedback

## Export Entries CSV

anization have been doing. You'll be able to find activity related to email, groups, documents,

▾ Filter results
 

↓ Export results ▾

	Item	Detail
um	Unknown	
din	Unknown	

## Enable Mailbox Auditing for All Users

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.

1. [Powershell Script to Enable](#)

**\*NOTE\*** Use the Office 365 audit log to search for mailbox activity that have been logged. You can search for activity for a specific user mailbox.

2. Go to Admin>Security and Compliance Center>Search & Investigation>Audit Log search

Home > Audit log search

## Audit log search

### Search

Activities

Show results for all activities ▾

× Clear all to show results for all activities

Search

#### Exchange mailbox activities

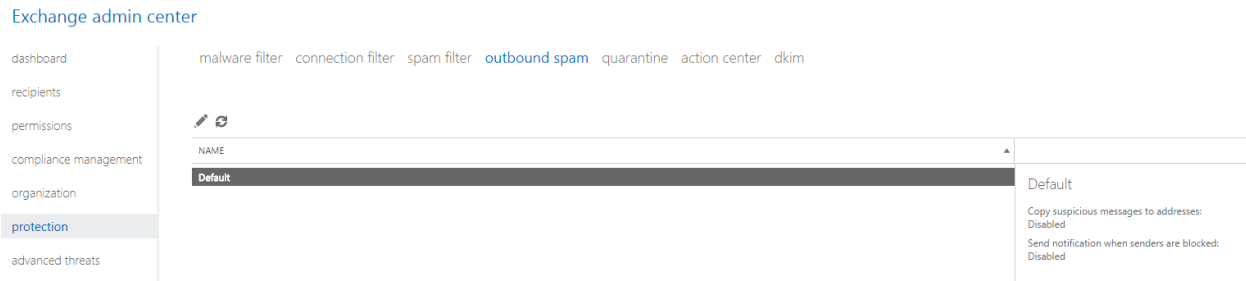
Created mailbox item	Copied messages to another folder
User signed in to mailbox	Sent message using Send On Behalf permissions
Purged messages from mailbox	Moved messages to Deleted Items folder
Moved messages to another folder	Sent message using Send As permissions
Updated message	Deleted messages from Deleted Items folder
Added delegate mailbox permissions	Removed delegate mailbox permissions

[List of Mailbox Auditing Actions](#)

[Set Up Outbound Spam Notifications](#)

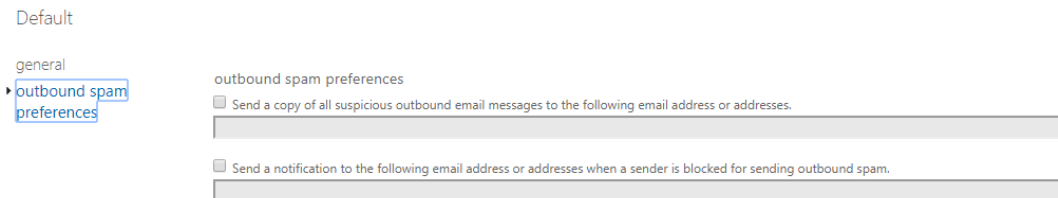
You should set your Exchange Online Outbound Spam notifications to copy and notify someone when a sender in your tenant has been blocked for sending excessive or spam emails. A blocked account is a good indication that the account in question has been breached and that an attacker is using it to send spam emails to other people.

1. In EAC go to Protection>Outbound Spam



2. Click on the Pencil Icon to Edit the default Policy

3. Click on “Outbound Spam Preferences” and choose to send a copy and notification to someone within the organization

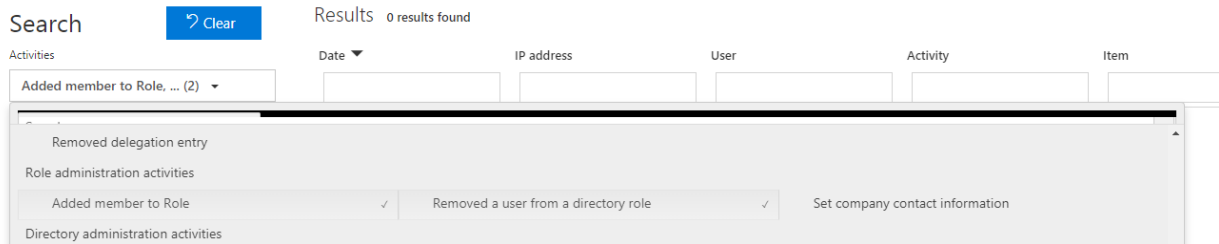


## Review Role Changes Weekly

You should do this because you should watch for illicit role group changes, which could give an attacker elevated privileges to perform more dangerous and impactful things in your tenancy.

1. Go to Admin>Security and Compliance Center>Search & Investigation>Audit Log search
2. Filter the search by going to Role Administration Activities and select “Added Member to Role” and “Removed a user from a Directory Role”





## Review Mailbox Forwarding Rules Weekly

You should review mailbox forwarding rules to external domains at least every week. There are several ways you can do this, including simply reviewing the list of mail forwarding rules to external domains on all of your mailboxes using a PowerShell script, or by reviewing mail forwarding rule creation activity in the last week from the Audit Log Search. While there are lots of legitimate uses of mail forwarding rules to other locations, it is also a very popular data exfiltration tactic for attackers. You should review them regularly to ensure your users' email is not being exfiltrated. Running the PowerShell script linked below will generate two csv files, "MailboxDelegatePermissions" and "MailForwardingRulesToExternalDomains", in your System32 folder.

### [Powershell Script](#)

## Review the Mailbox Access by Non-Owners Report Bi-Weekly

This report shows which mailboxes have been accessed by someone other than the mailbox owner. While there are many legitimate uses of delegate permissions, regularly reviewing that access can help prevent an external attacker from maintaining access for a long time and can help discover malicious insider activity sooner.

1. In EAC, go to Compliance Management>Auditing

Exchange admin center

in-place eDiscovery & hold auditing data loss prevention retention policies retention tags journal rules

Use these reports and audit logs to view information about mailboxes accessed by someone other than the owner and changes made by administrators to your Exchange organization. You can also export search results to a file that is sent to you or other users. [Learn more](#)

- Run a non-owner mailbox access report...**  
 Search mailbox audit logs for mailboxes that have been opened by someone other than the owner. You have to enable mailbox audit logging for each mailbox that you want to run a non-owner mailbox access report for. If mailbox audit logging isn't enabled for a mailbox, you won't get any results for it when you run this report. [Learn more](#)
- Export mailbox audit logs...**  
 Export entries from mailbox audit logs about non-owner access to user mailboxes. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. [Learn more](#)
- Run the administrator role group report...**  
 View entries from the admin audit log about configuration changes made by administrators in your organization. [Learn more](#)
- Run an in-Place eDiscovery & Hold report...**  
 Search the admin audit log for changes made to In-Place eDiscovery searches and In-Place Holds. [Learn more](#)
- Export the admin audit log...**  
 Export entries from the admin audit log for any configuration change made to your organization. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. [Learn more](#)
- Run a per-mailbox Litigation Hold report...**  
 Search the admin audit log to determine if a Litigation Hold was enabled or disabled for a user's mailbox. [Learn more](#)
- Run the external admin audit log report...**  
 View entries from the admin audit log about configuration changes made to your Exchange Online services by Microsoft or by a delegated admin. [Learn more](#)

2. Click on “Run a non-owner mailbox access report...”

3. Specify a data range and run a search

search for mailboxes accessed by non-owners

Specify a date range and select the mailboxes to search for. Then select to search for non-owner access by anyone or by users inside or outside your organization. [Learn more](#)

\*Start date: 2018 May 22

\*End date: 2018 June 6

Search these mailboxes or leave blank to find all mailboxes accessed by non-owners:

Search for access by: All non-owners

Search results	
Mailbox	LAST ACCESSED:
There are no items to show in this view.	

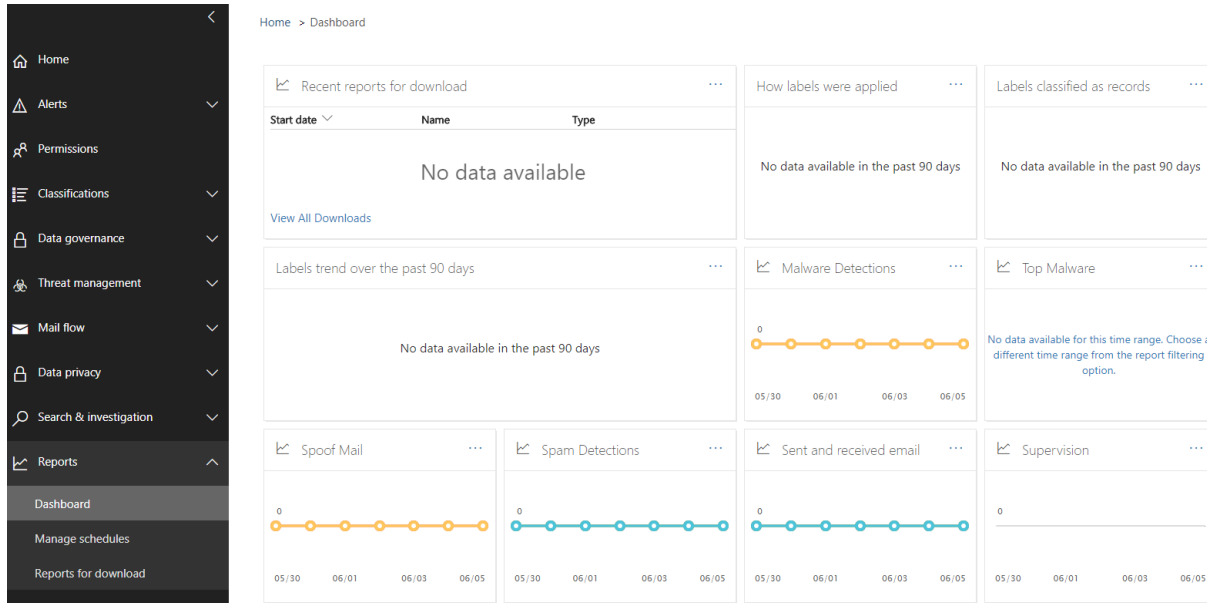
## Review the Malware Detections Report Weekly

This report shows specific instances of Microsoft blocking a malware attachment from reaching your users. While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of



malware being targeted at your users, which may prompt you to adopt more aggressive malware mitigations

### 1. Go to Admin>Security and Compliance Center>Reports>Dashboard

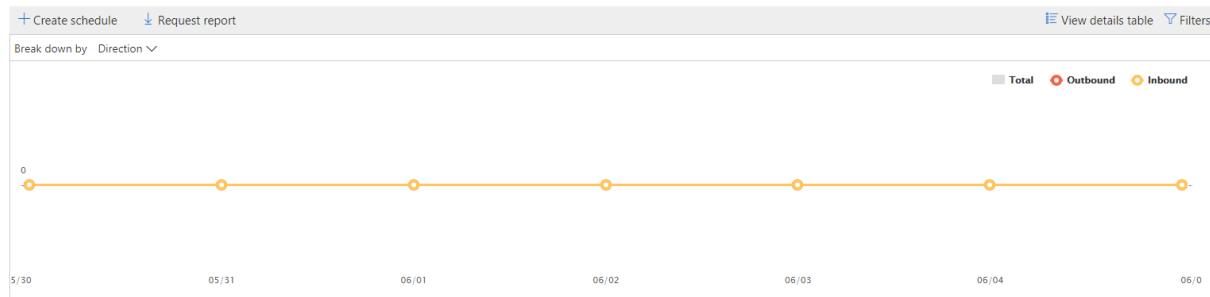


### 2. Click on Malware Detections

### 3. View the Detection Report

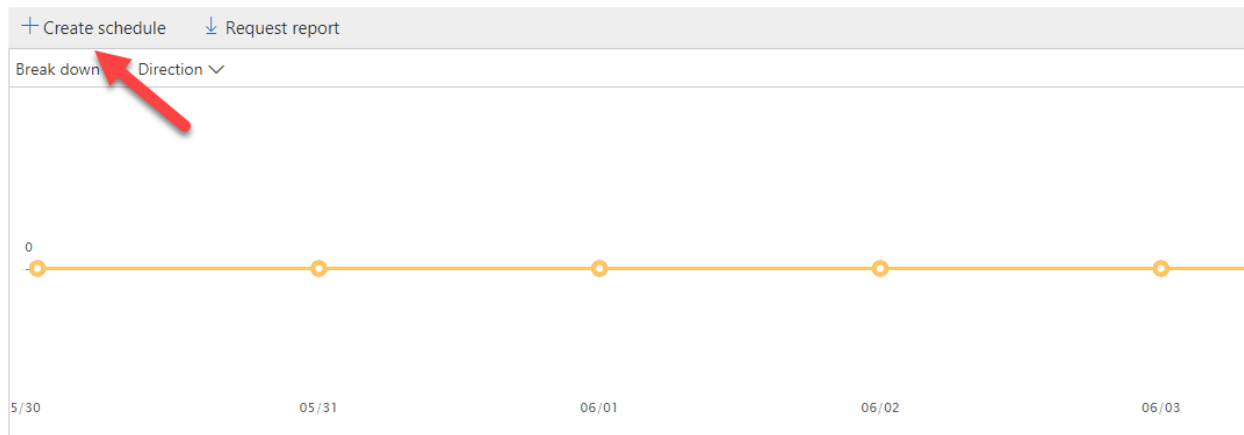
Home > Dashboard > Report Viewer - Security & Compliance

#### Malware Detections Report



4. Click "+ Create Schedule"

### Malware Detections Report



5. Create a weekly report schedule and send it to the appropriate email address

## Create schedule



You are about to create a schedule for this report. You will receive a weekly email once the report is ready. You can also download the report from the Manage schedules and Manage downloads page. For more options in scheduling, visit the Customize schedules page.

Start date:

2018-06-06



Frequency  
Weekly

Send email to  
admin@rosebudhealthcare.onmicrosoft.com

Schedule Name  
Schedule-Weekly-MalwareDetection

Create schedule

Cancel

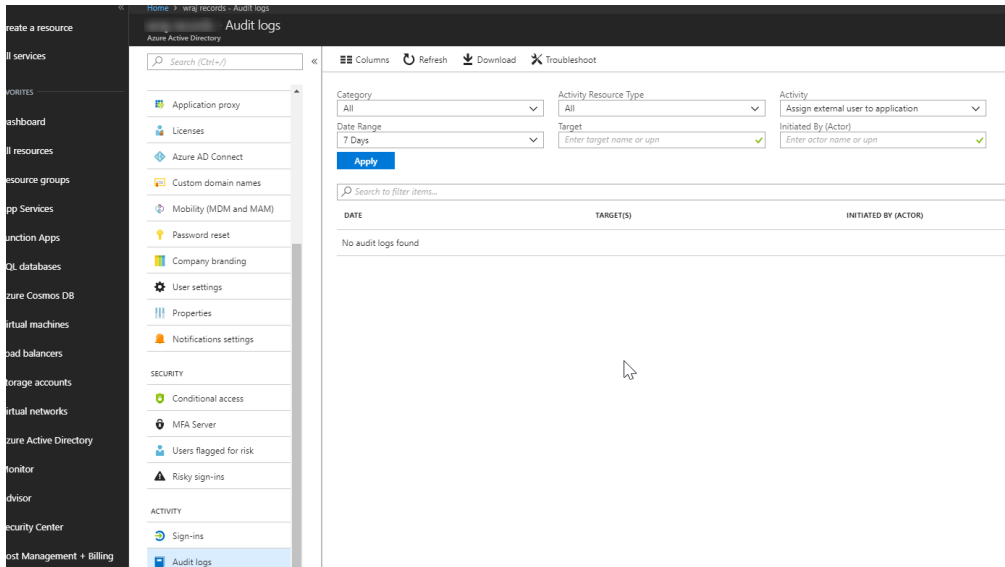
### Options

[Customize schedule](#)

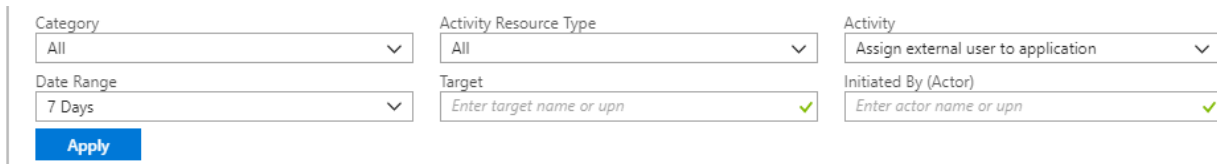
## Review your Account Provisioning Activity Report Weekly

This report includes a history of attempts to provision accounts to external applications. If you don't usually use a third-party provider to manage accounts, any entry on the list is likely illicit. But, if you do, this is a great way to monitor transaction volumes, and look for new or unusual third-party applications that are managing users.

1. Go to Admin Centers>Azure Active Directory>Audit Logs



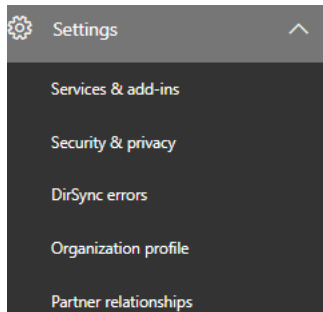
2. In the “Activity” section, search for “external” and select “Assign external user to application”











Do not Allow Calendar Details Sharing

You should not allow your users to share calendar details with external users. This feature allows your users to share the full details of their calendars with external users. Attackers will very commonly spend time learning about your organization (performing reconnaissance) before launching an attack. Publicly available calendars can help attackers understand organizational relationships, and determine when specific users may be more vulnerable to an attack, such as when they are traveling

## 1. Go to Settings>Services & Add-ins



## 2. Click on Calendar

name	Host Apps	Status
 Azure multi-factor authentication Manage your settings for Azure multi-factor authentication		
 Bing Turn Bing for business access on or off for your company employees		
 Bookings Turn Bookings on or off for your organization and learn how to get licenses for your users		
 Business center Control which business apps people in your company can use		
 Calendar Let people share their calendars with external users		
 Cortana Turn Cortana access on or off for your entire organization		
 Directory Synchronization Sync users to the cloud using Active Directory		
 Dynamics Customer Insights Preview Manage and update your Dynamics Customer Insights Preview settings		



### 3. Change the settings to “Calendar free/busy information with time only”

**Calendar**

**External sharing**

Let your users share their calendars with external users who have Office 365 or Exchange  On

Allow anonymous users to access calendars with an email invitation  On

Calendar free/busy information with time only

Calendar free/busy information with time, subject and location

All calendar appointment information

**Don't see what you're looking for?**

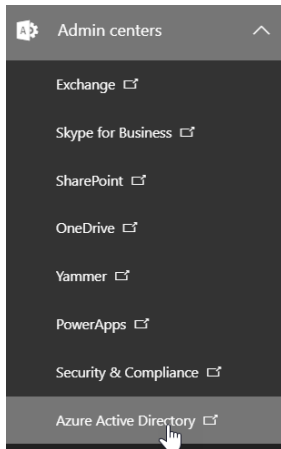
[Go to the Exchange admin center to manage additional settings](#)

**Save** **Cancel**

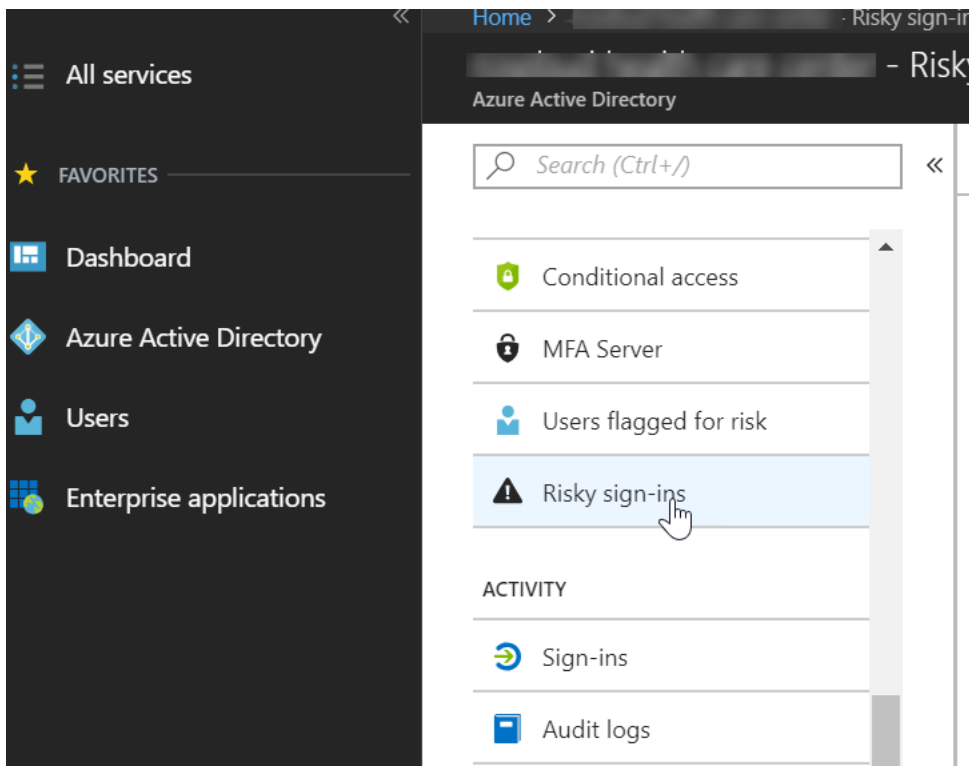
### Review Sign-Ins after Multiple Failures report weekly

These reports contains records of accounts that have successfully signed-in after multiple risk events, such as locations, IP addresses which could be an indication that the account could be compromised.

1. Go into Admin Centers>Azure Active Directory



2. Go to Azure Active Directory>Risky Sign-ins



### 3. View Users with Risky Sign-Ins

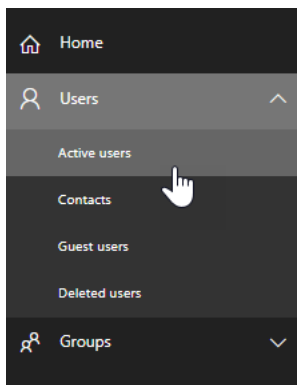
Search (Ctrl+/) << Download + Add known IP address ranges

USER	IP	LOCATION	SIGN-IN TIME (UTC)	STATUS
[Redacted]	[Redacted]	US	5/24/2018 12:12 PM	Active

### Designate More than 1 Global Admin

You should designate more than one global tenant administrator because that one admin can perform malicious activity without the possibility of being discovered by another admin. You could also set this second admin up with a mailbox in which all of the reports discussed in this playbook are filtered into.

1. Log In to the 365 Admin Center>Go to Users>Active Users



## 2. Click +Add a User>Add User Details

A2 Armin ?

First name: Admin  
Last name: 2  
Display name \*: Admin 2  
Username \*: admin2  
Location: United States

▼ Contact information

▼ Password: Auto-generated

▼ Roles: User (no administrator access)

▲ Product licenses \* Decision required

▼ Office 365 Business Premium Off  
You don't have any licenses available. To purchase additional licenses, please contact your partner(s).

▼ Office 365 Business 5 of 5 licenses available  
Not Recommended:  
Create user without product license Off  
They may have limited or no access to Office 365 until you assign a product license.

Add Cancel

### 3. Click “Roles”> Change to Global Administrator

Contact information  


---

 Password Auto-generated  


---

 Roles Global administrator  


---

You can assign different roles to people in your organization. [Learn more about admin roles](#)

User (no administrator access)  
 This user won't have permissions to the Office 365 admin center or any admin tasks.

Global administrator  
 This user will have access to all features in the admin center and can perform all tasks in the Office 365 admin center.

Customized administrator  
 You can assign this user one or many roles so they can manage specific areas of Office 365.

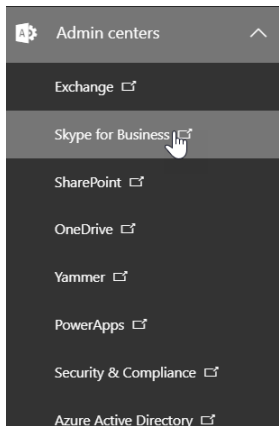
Alternative email address

Global administrators are the only ones who can manage the admin center. Make sure a user has a mobile phone number in their contact information and a strong password.

## Do Not Allow External Domain Skype Communications

You should not allow your users to communicate with Skype users outside your organization. While there are legitimate, productivity-improving scenarios for this, it also represents a potential security threat in that those external users will now be able to interact with your users over Skype for Business. Attackers may be able to pretend to be someone your user knows, and then send malicious links or attachments, resulting in an account breach, or leaked information

1. Go into Admin Centers>Skype for Business Admin Center



2. Go to Organization>External Communications

### Skype for Business admin center

A screenshot of the 'Skype for Business admin center' showing the 'external communications' settings page. The left sidebar contains navigation options: dashboard, users, organization (selected), audio conferencing, online meetings, tools, and reports. The main content area has tabs for 'general' and 'external communications'. Under 'external access', there is a dropdown menu set to 'On except for blocked domains'. Below that, under 'public IM connectivity', there is a checked checkbox 'Let people use Skype for Business to communicate with Skype users outside your organization.' At the bottom, there is a section for 'blocked or allowed domains' with a table header containing 'DOMAIN' and 'STATUS', and a message 'There are no results to display.'

### 3. Change to “Off Completely”

external access

You can control access to Skype for Business users in other organizations in two ways: 1) block specific domains, but allow access to everyone else, or 2) allow specific domains, but block access to everyone else. [Learn more](#)

Off completely

Off completely

On except for blocked domains

On only for allowed domains

organization.

blocked or allowed domains

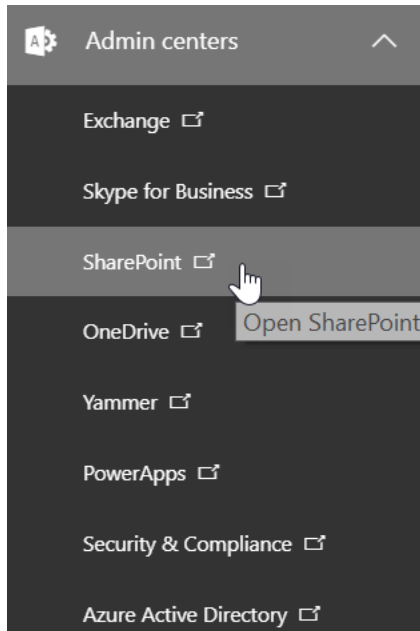
+ ✎ 🗑️ 🔍

DOMAIN ▲	STATUS
There are no results to display.	

### Configure Expiration Time for External Sharing Links

You should restrict the length of time that anonymous access links are valid. An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared.

1. Go to Admin Centers>SharePoint



2. Click on the “Sharing Tab”

SharePoint admin center

- site collections
- infopath
- user profiles
- bcs
- term store
- records management
- search
- secure store
- apps
- sharing**
- settings
- configure hybrid

We're working on a new SharePoint admin center. [Try the preview](#)

**Sharing outside your organization**

Control how users share content with people outside your organization.

- Don't allow sharing outside your organization
- Allow sharing only with the external users that already exist in your organization's directory
- Allow users to invite and share with authenticated external users
- Allow sharing to authenticated external users and using anonymous access links

Anonymous access links expire in this many days:

Anonymous access links allow recipients to:

Files:

Folders:

**Who can share outside your organization**

- Let only users in selected security groups share with authenticated external users
- Let only users in selected security groups share with authenticated external users and using anonymous links

Feedback



3. Checkmark the box next to “Anonymous access links expire in this many days” and select # of days:

#### Sharing outside your organization

Control how users share content with people outside your organization.

- Don't allow sharing outside your organization
- Allow sharing only with the external users that already exist in your organization's directory
- Allow users to invite and share with authenticated external users
- Allow sharing to authenticated external users and using anonymous access links

Anonymous access links expire in this many days:

Anonymous access links allow recipients to:

Files:

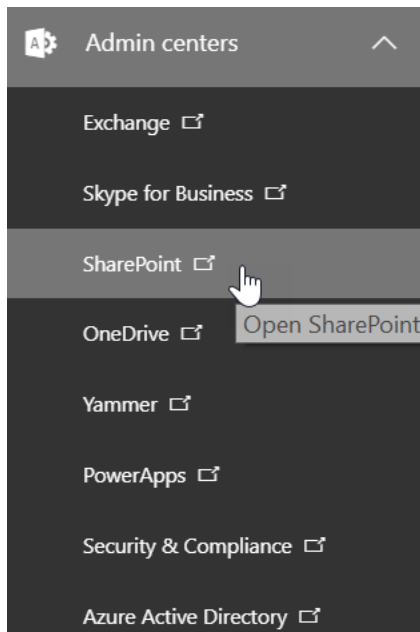
Folders:



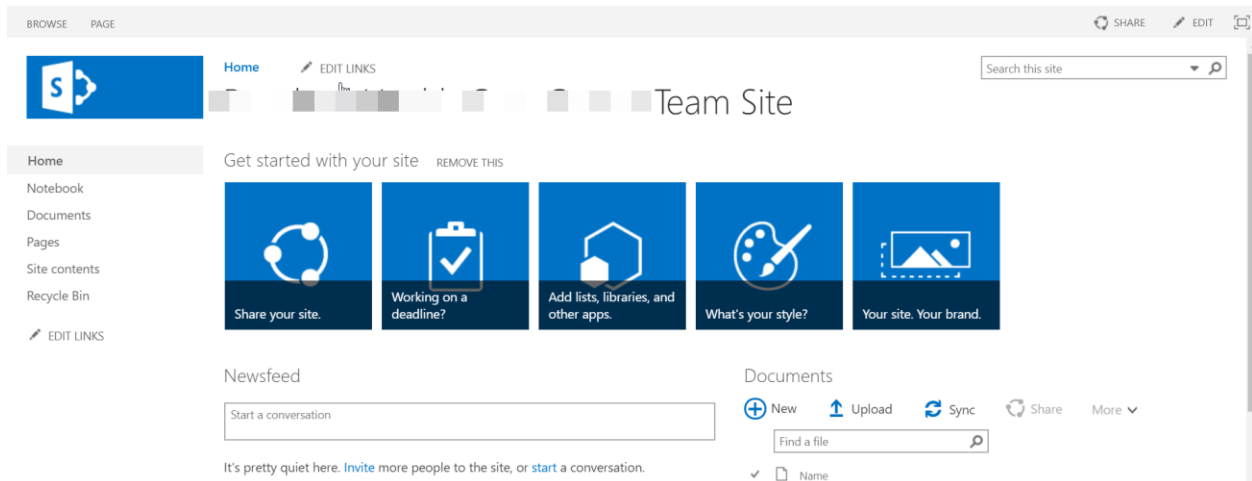
## Enable Versioning on all SharePoint Online Document Libraries

You should enable versioning on all of your SharePoint online site collection document libraries. This will ensure that accidental or malicious changes to document content can be recovered.

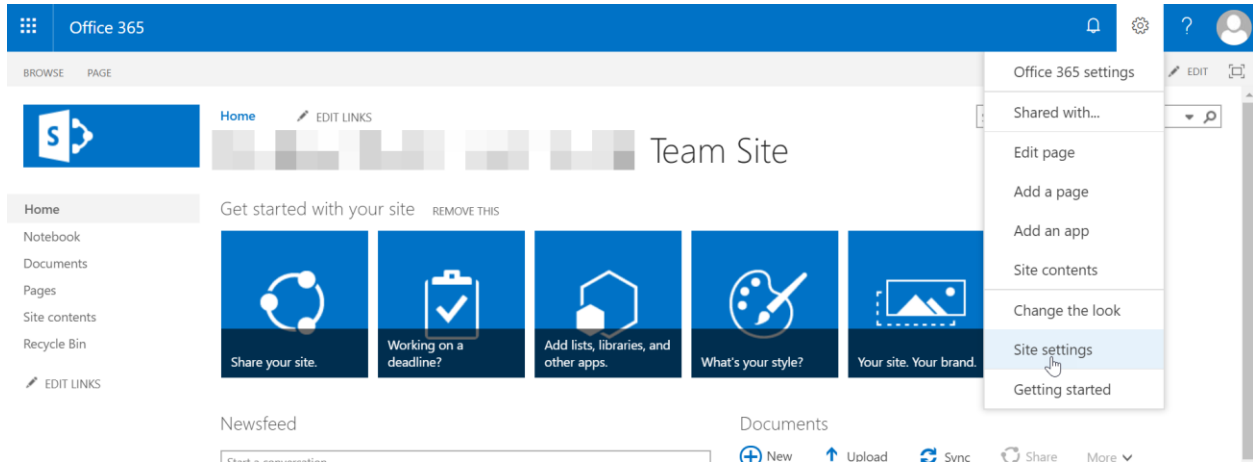
1. Go to Admin Centers>SharePoint



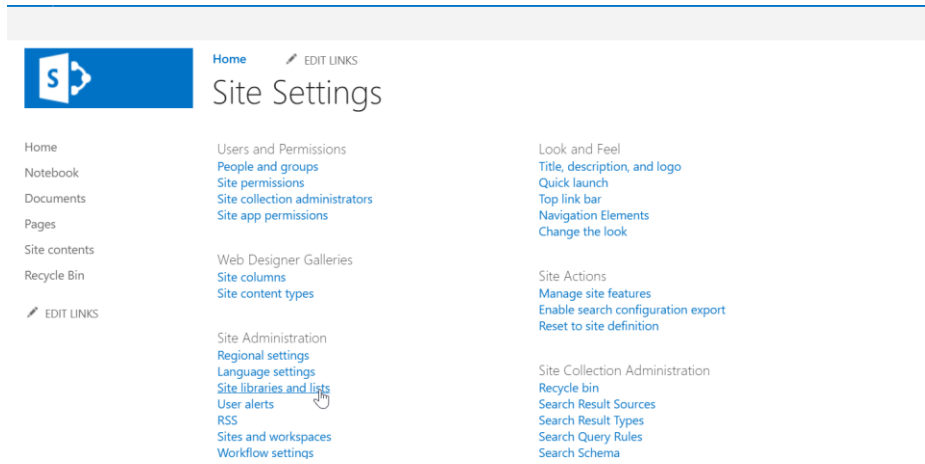
2. Go to one of you sites you want to configure versioning on:



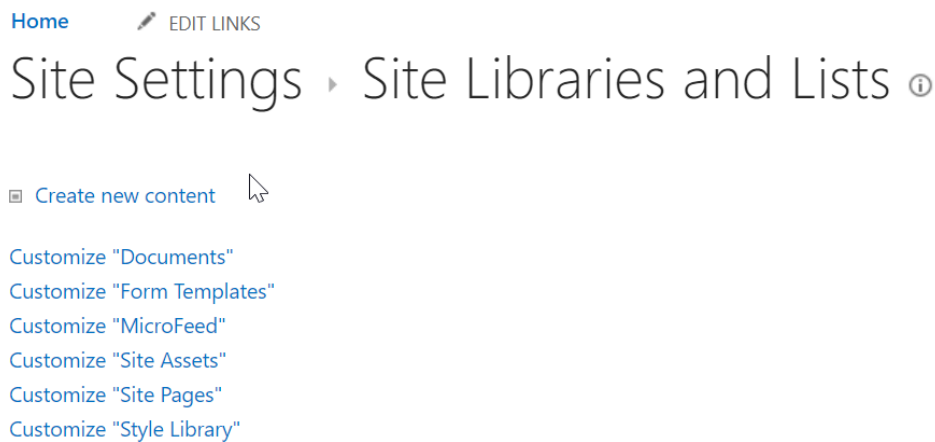
### 3. Go to Settings>Site Settings



#### 4. Go to Site Administration>Site Libraries and Lists



#### 5. Select on of your document libraries



## 6. Click on Versioning Settings

Home EDIT LINKS

# Documents Settings

Home  
Notebook  
Documents  
Pages  
Site contents  
Recycle Bin  
EDIT LINKS

List Information  
Name: Documents  
Web Address:  
Description:

General Settings Permissions and Management Communications

- List name, description and navigation
- Versioning settings**
- Advanced settings
- Validation settings
- Column default value settings
- Audience targeting settings
- Delete this document library
- Permissions for this document library
- Manage files which have no checked in version
- Workflow Settings
- Apply label to items in this list or library
- Generate file plan report
- RSS settings

## 7. Customize the settings to create version preferences:

# Settings Versioning Settings

Content Approval  
Specify whether new items or changes to existing items should remain in a draft state until they have been approved. [Learn about requiring approval.](#)

Document Version History I  
Specify whether a version is created each time you edit a file in this document library. [Learn about versions.](#)

Require content approval for submitted items?  
 Yes  No

Create a version each time you edit a file in this document library?  
 No versioning  
 Create major versions  
 Example: 1, 2, 3, 4  
 Create major and minor (draft) versions  
 Example: 1.0, 1.1, 1.2, 2.0

Optionally limit the number of versions to retain:

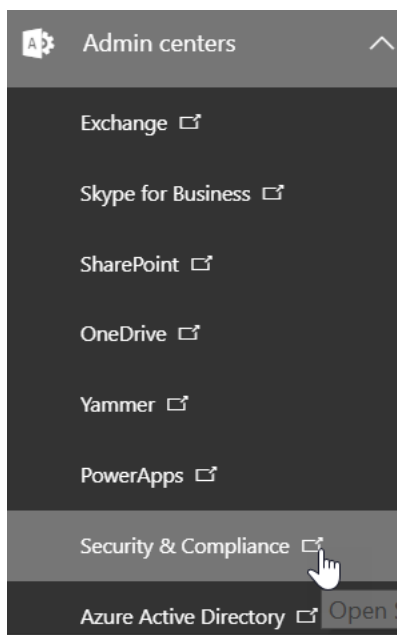
Keep the following number of major versions:

Keep drafts for the following number of major versions:

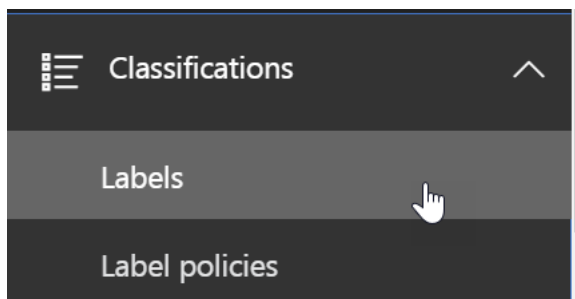
## Tag Documents in SharePoint

You should apply labels to documents in SharePoint Online. If you use document classification tags, you can author rules that leverage the label to implement specific retention/deletion policies using data loss protection (DLP) in the Security and Compliance Center.

1. Go to Admin Centers>Security and Compliance



2. Click Classifications>Labels



### 3. Click Create Label

Home > Labels

When published, labels appear in your users' apps, such as Outlook, SharePoint, and OneDrive. When a label is applied to email or docs (automatically or by the user), the content is retained based on the settings you chose. For example, you can create labels that retain content for a certain time or ones that simply delete content when it reaches a certain age. [Learn more about labels](#)

<input checked="" type="checkbox"/>	Name	Created by	Retention period	Last modified
No data available				

0 item(s) loaded. Feedback

### 4. Create a name for your label and create a description to help admins and users, then click Next

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

## Name your label

**Name \*** ⓘ

**Description for admins** ⓘ

**Description for users** ⓘ

Feedback

### 5. Create a custom retention policy for the Label

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

## Label settings

Retention [?](#)

On

When this label is applied to content...

Retain the content [?](#)

For this long...  years

What do you want to do after this time?

Delete the content automatically. [?](#)

Trigger a disposition review. [?](#)

[Back](#) [Next](#) [Cancel](#) [Feedback](#)

### 6. Review your Settings and click, Create this Label

Create a label to help users classify their content.

- Name your label
- Label settings
- Review your settings

## Review your settings

**Description for admins** [Edit](#)

All Documents containing PII

**Description for users** [Edit](#)

This is a tag for sensitive data

**Retention** [Edit](#)

7 years  
Retain only  
Based on when it was created

[Back](#) [Create this label](#) [Cancel](#)



7. Now we're ready to "Publish the Label"

## HIPPA Tag ✕

[✎ Edit label](#) [🗨️ Publish label](#) [🔄 Auto-apply a label](#)

[🗑️ Delete label](#)

**Name**  
HIPPA Tag

**Description for admins** [Edit](#)  
All Documents containing PII

**Description for users** [Edit](#)  
This is a tag for sensitive data

[Close](#) [Feedback](#)

## 8. Select the label to publish:

Publish labels so users can apply them to their content.

- Choose labels to publish
- Publish to these locations
- Name your policy
- Review your settings

### Choose labels to publish

Choose the labels you want to publish to your organization's apps so users can apply them to their content. If you don't see the labels you want, you'll be able to create one from scratch.

**Publish these labels (1 label(s))**

HIPPA Tag 7 years keep

[Edit](#)

[Next](#) [Cancel](#)

[Feedback](#)

## 9. Choose your locations

Publish labels so users can apply them to their content.

- Choose labels to publish
- Publish to these locations
- Name your policy
- Review your settings

### Choose locations

We'll publish the labels to the locations you choose.

- All locations. Includes content in Exchange email, Office 365 groups, OneDrive and SharePoint documents.
- Let me choose specific locations.

[Back](#) [Next](#) [Cancel](#)

[Feedback](#)

## 10. Name the Policy

Publish labels so users can apply them to their content.

Choose labels to publish

Publish to these locations

Name your policy

Review your settings

### Name your policy

Name \* ⓘ

HIPPA Info

Description

Enter a friendly description for your policy

Back

Next

Cancel

Feedback

### 11. Review your settings and click “Publish Labels”

Publish labels so users can apply them to their content.

**Review your settings** [Close]

⚠ It will take up to 1 day for labels to appear to your users. Labels will appear in Outlook and Outlook web app only for mailboxes that have at least 10 MB of data.

**Choose labels to publish** [Edit]

1 label(s) will be published (made available) so your users can classify their content

HIPPA Tag 7 years keep

**Publish to these locations** [Edit]

Exchange email  
OneDrive accounts  
SharePoint sites  
Office 365 groups

[Back] [Publish labels] [Cancel] [Feedback]

### 12. You can also Auto-apply the tag based on certain parameters:

**HIPPA Tag** [Close]

[Edit label] [Publish label] [Auto-apply a label] [Delete label]

**Name**  
HIPPA Tag

**Description for admins** [Edit]  
All Documents containing PII

**Description for users** [Edit]  
This is a tag for sensitive data

[Close] [Feedback]

### 13. Choose your Conditions:

Automatically apply a label to content

×

Choose label to auto-apply

Choose the type of content you want to apply this label to

Apply label to content that contains sensitive information ⓘ  
 Apply label to content that contains specific words or phrases ⓘ

Back
Next
Cancel

Choose conditions

Settings

Name your policy

Locations

Review your settings

Feedback

### 14. Drill down into certain templates or create your own:

Automatically apply a label to content

×

Choose label to auto-apply

Select from a template

Just tell us what kind of information you want to detect.

Show options for All countries or regions ▼

Financial

Medical and health

Privacy

Custom

Australia Health Records Act (HRIP Act)

Canada Health Information Act (HIA)

Canada Personal Health Information Act (PHIA) - Manitoba

Canada Personal Health Act (PHIPA) - Ontario

U.S. Health Insurance Act (HIPAA)

**Description**

Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA).

**Protects this information:**

- PII Identifiers
- Medical Terms

Feedback

45

15. Click “edit” if you want to add more content:

Automatically apply a label to content

- Choose label to auto-apply
- Choose conditions
- Settings
- Name your policy
- Locations
- Review your settings

### What kind of content do you want to detect ?

Select which types of data you want to detect so that the system can apply a label

**Select the types you want to detect**

Detect content that contains these information types:

- PII Identifiers
- Medical Terms

[Edit](#)

**Apply this label**

We'll apply "HIPPA Tag" to content that matches the settings above.

[Back](#) [Next](#) [Cancel](#)

[Feedback](#)

16. Name your policy

Automatically apply a label to content

- Choose label to auto-apply
- Choose conditions
- Settings
- Name your policy
- Locations
- Review your settings

### Name your policy

**Name \*** ⓘ

**Description**

[Back](#) [Next](#) [Cancel](#)

[Feedback](#)

### 17. Choose Locations:

Automatically apply a label to content

- ✔ Choose label to auto-apply
- ✔ Choose conditions
- ✔ Settings
- ✔ Name your policy
- Locations
- Review your settings

## Choose locations

We'll apply the label to content that's stored in the locations you choose.

All locations. Includes content in Exchange email, OneDrive and SharePoint documents.
   
 Let me choose specific locations.

Back
Next
Cancel

✕

Feedback

### 18. Review Settings and click "Auto-apply"

- ✔ Choose conditions
- ✔ Settings
- ✔ Name your policy
- ✔ Locations
- Review your settings

HIPPA Info

**Description** Edit

**Applies to content in these locations** Edit

Exchange email

OneDrive accounts

SharePoint sites

**Settings** Edit

Detect content that contains sensitive information

Auto-apply label "HIPPA Tag" to content in the locations you chose

Back
Auto-apply
Cancel

Feedback

## Exchange Online Protection/Antispam Policies

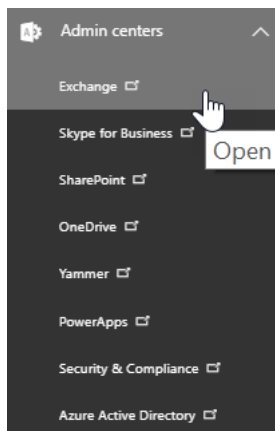
Checklist:

Connection Filtering:

Questions to Ask:

- Do I need to create an allowed list from a specific IP range?
- Do I need to create a block list?

1. Go into Admin Centers>Exchange Admin Center





## 2. Select the “Protection” tab

### Exchange admin center

malware filter connection filter spam filter outbound spam quarantine action center dkim

[+](#)
[✎](#)
[🗑️](#)
[↑](#)
[↓](#)
[🔄](#)

ENABLED	NAME	PRIORITY	
<input checked="" type="checkbox"/>	Default	Lowest	<p>Default</p> <p>Enabled</p> <p>Relative priority: Lowest</p> <p>Summary</p> <p>Malware detection response: Don't notify recipients</p> <p>Sender notifications: None</p> <p>Administrator notifications: None</p> <p>Customized notification text: Not configured</p>

dashboard  
 recipients  
 permissions  
 compliance management  
 organization  
**protection**  
 mail flow  
 mobile  
 public folders  
 unified messaging  
 hybrid

## 3. Click on “Connection Filter”

### Exchange admin center

malware filter **connection filter** spam filter outbound spam quarantine action center dkim

[✎](#)
[🗑️](#)
[🔄](#)

NAME	
Default	<p>Default</p> <p>Scoped to: All domains</p> <p>Summary</p> <p>IP Allow list: Not configured</p> <p>IP Block list: Not configured</p> <p>Safe list: Disabled</p>

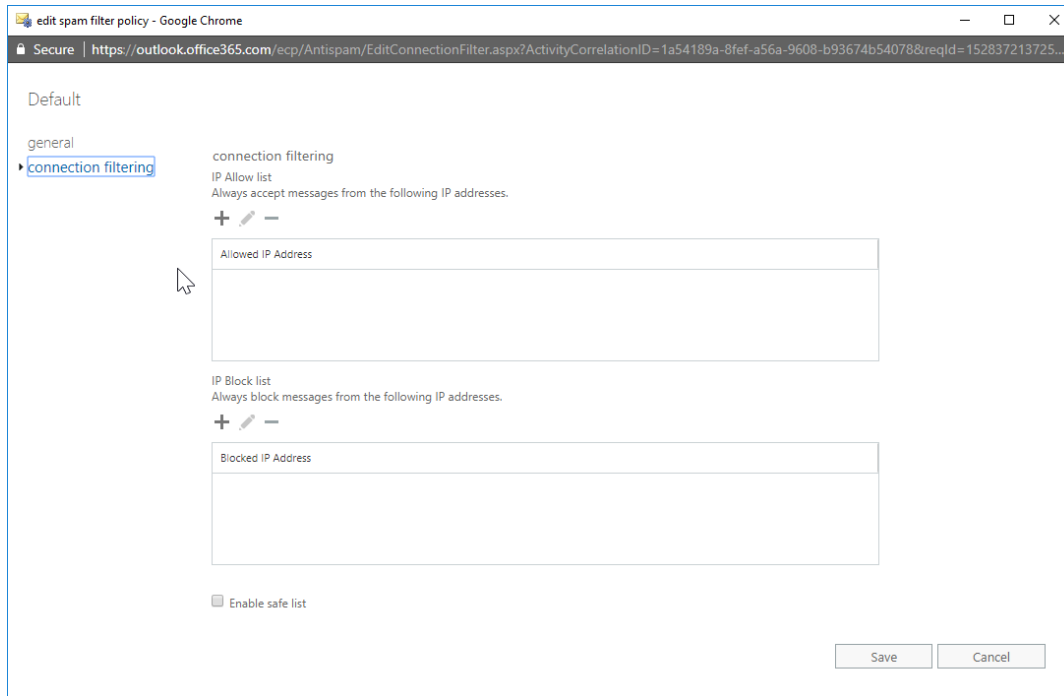
dashboard  
 recipients  
 permissions  
 compliance management  
 organization  
**protection**  
 mail flow  
 mobile  
 public folders  
 unified messaging  
 hybrid

#### 4. Click on the Pencil icon to modify the default policy



NAME	
Default	Default Scoped to: All domains  Summary IP Allow list: Not configured IP Block list: Not configured Safe list: Disabled

5. Click “connection filtering”, add Allowed/Block List



Spam Filtering:

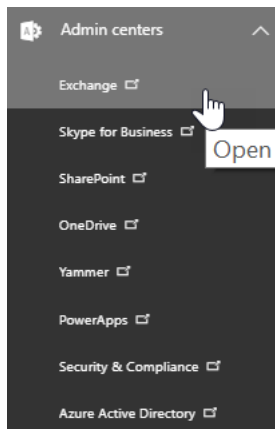
Questions to Ask:

1. What actions do we want to take when a message is identified as spam?
  - a. Move Message to Junk Folder (Default)
  - b. Add X Header (Sends the message to the specified recipients, but adds X-header text to the message header to identify it as spam)
  - c. Prepend Subject line with text (Sends the message to the intended recipients but prepends the subject line with the text that you specify in the Prefix subject line with this text input box. Using this text as an identifier, you can optionally create rules to filter or route the messages as necessary.)
  - d. Redirect message to email address (Sends the message to a designated email address instead of to the intended recipients.)

2. Do we need to add allowed senders/domains or block senders/domains?
3. Do we need to filter messages written in specific language?
4. Do we need to filter message coming from specific countries/regions?
5. Do we want to configure any end-user spam notifications to inform users when messages intended for them were sent to quarantine instead? (From these notifications, end users can release false positives and report them to Microsoft for analysis.)

Steps:

1. Go to Admin Centers>Exchange Online Admin Center



## 2. Click on "Protection"

### Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection**
- mail flow
- mobile
- public folders
- unified messaging
- hybrid

**malware filter** connection filter spam filter outbound spam quarantine action center dkim



ENABLED	NAME	PRIORITY	
<input checked="" type="checkbox"/>	Default	Lowest	<b>Default</b> Enabled Relative priority: Lowest  <b>Summary</b> Malware detection response: Don't notify recipients Sender notifications: None Administrator notifications: None Customized notification text: Not configured

### 3. Click on “Spam Filter” and click on the pencil icon to modify the default policy

malware filter connection filter **spam filter** outbound spam quarantine action center dkim

ENABLED	NAME	PRIORITY	
<input checked="" type="checkbox"/>	Default	Lowest	<p>Default</p> <p>Enabled</p> <p>Relative priority: Lowest</p> <p>Summary</p> <p>Detection response for spam: Move message to Junk Email folder</p> <p>Detection response for high confidence : Move message to Junk Email folder</p>

### 4. Navigate through the tabs to configure any of the questions asked previously

Secure | <https://outlook.office365.com/ecp/Antispam/EditSpamContentFilter.aspx?ActivityCorrelationID=145c7311-053e-3e8c-38d0-501fc950f851&reqId=1528372513319&pwmcid...>

Default

- general
- spam and bulk actions**
- block lists
- allow lists
- international spam
- advanced options

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:

Move message to Junk Email folder

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

\*Add this X-header text:

\*Prepend subject line with this text:

\*Redirect to this email address:

Save Cancel

5. The “advanced options” tab allows you to get more granular with your policy and tighten the settings on the spam filter:

Default

- general
- spam and bulk actions
- block lists
- allow lists
- international spam
- ▶ advanced options

**advanced options**

Increase Spam Score  
Specify whether to increase the spam score for messages that include these types of links or URLs.

Image links to remote sites:  ▼

Numeric IP address in URL:  ▼

URL redirect to other port:  ▼

URL to .biz or .info websites:  ▼

Mark as Spam  
Specify whether to mark messages that include these properties as spam.

Empty messages:  ▼

JavaScript or VBScript in HTML:  ▼

Frame or IFrame tags in HTML:  ▼

Object tags in HTML:  ▼

Embed tags in HTML:  ▼

Form tags in HTML:  ▼

Save Cancel

6. You can configure end user spam notifications on the right-hand side of the page:

malware filter connection filter **spam filter** outbound spam quarantine action center dkim

ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	Default	Lowest

Default

Enabled

Relative priority: Lowest

Summary

Detection response for spam:  
Move message to Junk Email folder

Detection response for high confidence spam:  
Move message to Junk Email folder

Mark bulk email as spam:  
Enabled

Threshold:  
7 (Default)

Sender block list:  
Not configured

Domain block list:  
Not configured

Sender allow list:  
Not configured

Domain allow list:  
Not configured

International spam - languages:  
Disabled

International spam - regions:  
Disabled

End-user spam notifications:  
Disabled

Configure end-user spam notifications...

Test mode options:  
None

Configure end-user spam notifications...

## [Powershell Commands to Configure](#)

### Outbound filtering:

#### Questions to Ask:

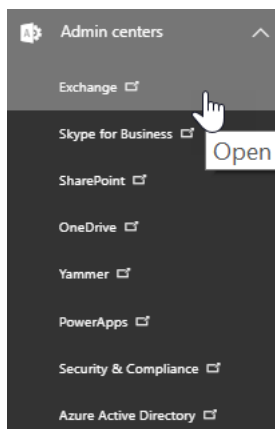
1. Do I want to receive notifications when someone is flagged for sending outbound spam?
  - This is a check to make sure users don't send spam
  - Can turn on settings to send copies/notifications of all suspicious outbound mail to certain email address
  - Refer to "[Set Up Outbound Spam Notifications](#)" of Secure Score section for implementation

### Mail Flow Rules:

#### Questions to Ask:

1. Do I need to create custom mail flow rules based on business policies?
  - Create Rules based on If/Then statements
  - For example, you could have a moderator for a group/individual that approves messages before they are sent out

1. Go to Admin Centers>Exchange





## 2. Go to Mail Flow>Rules

### Exchange admin center

Exchange admin center navigation menu:

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection
- mail flow**
- mobile
- public folders
- unified messaging
- hybrid

Top navigation bar:

- rules**
- message trace
- accepted domains
- remote domains
- connectors

Table headers:

ON	RULE	PRIORITY
There are no items to show in this view.		

## 3. There are a variety of templates available to you through the Business Plan. I crossed out the ones that requires RMS licensing:

### Exchange admin center

Exchange admin center navigation menu:

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection
- mail flow**
- mobile
- public folders
- unified messaging
- hybrid

Top navigation bar:

- rules**
- message trace
- accepted domains
- remote domains
- connectors

Dropdown menu items:

- Create a new rule...
- ~~Apply disclaimers...~~
- Bypass spam filtering...
- Filter messages by size...
- ~~Send messages to a moderator...~~
- Modify messages...
- Restrict managers and their direct reports...
- Restrict messages by sender or recipient...
- Send messages to a moderator...
- Send messages and save a copy for review...

Table headers:

ON	RULE	PRIORITY
There are no items to show in this view.		

4. You can customize the fields appropriately. You can choose the severity level and choose whether to force it right away or not:

new rule

Name:

\*Apply this rule if...  
 [\\*Select people...](#)

\*Do the following...

Properties of this rule:  
 Audit this rule with severity level:

Choose a mode for this rule:  
 Enforce  
 Test with Policy Tips  
 Test without Policy Tips

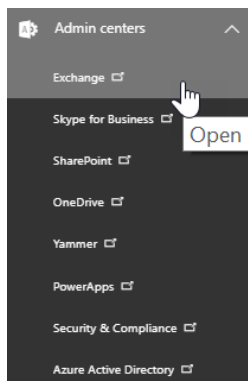
[More options...](#)

Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

## Malware:

- This is already set up company-wide via default anti-malware policy
- Do you need to create more granular policies for a certain group of users such as additional notifications via text or heightened filtering based on file extensions?

1. Go to Admin Centers>Exchange



## 2. Go to Protection>Malware Filter>Click on Pencil Icon to Modify default policy

### Exchange admin center

- dashboard
- recipients
- permissions
- compliance management
- organization
- protection**
- mail flow
- mobile
- public folders
- unified messaging
- hybrid

malware filter connection filter spam filter outbound spam quarantine action center dkim



ENABLED	NAME	PRIORITY	
<input checked="" type="checkbox"/>	Default	Lowest	<p>Default</p> <p>Enabled</p> <p>Relative priority: Lowest</p> <p>Summary</p> <p>Malware detection response: Don't notify recipients</p> <p>Sender notifications: None</p> <p>Administrator notifications: None</p> <p>Customized notification text: Not configured</p>

### 3. Modify Accordingly

Default

general

▶ settings

#### Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

- No  
 Yes and use the default notification text  
 Yes and use custom notification text

\*Custom notification text:

If the message body is detected to contain malware, the message and all of its associated attachments are deleted regardless of which option you select.

#### Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

- Off  
 On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

+ -

FILE TYPES
.ace
.ani

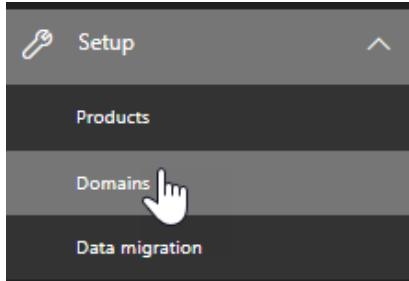
Save

Cancel

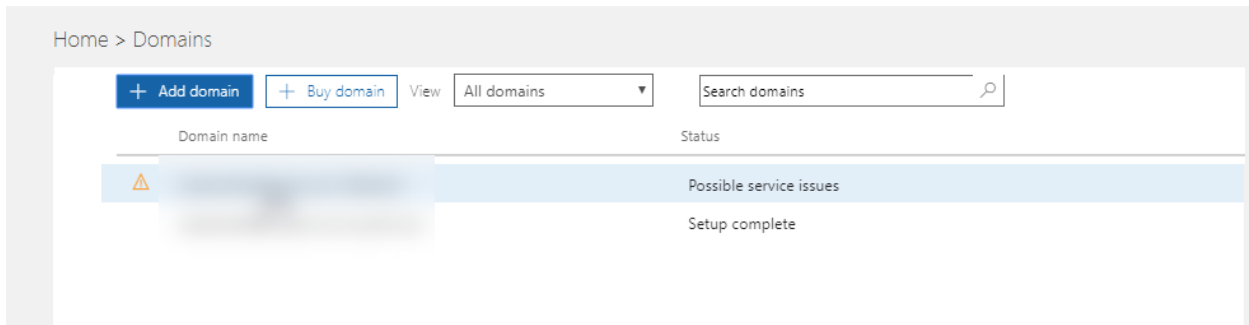
## DNS Settings

- Do you have SPF records/DKIM records/DMARC in place?
- SPF validates the origin of email messages by verifying the IP address of the sender against the alleged owner of the sending domain which helps prevent spoofing
- DKIM lets you attach a digital signature to email messages in the message header of emails you send. Email systems that receive email from your domain use this digital signature to determine if incoming email that they receive is legitimate.
- DMARC helps receiving mail systems determine what to do with messages that fail SPF or DKIM checks and provides another level of trust for your email partners.

1. Go to Admin Center>Setup>Domains



2. Click on the domain you want to add records to:



### 3. Take Note of the MX and TXT record listed under the Exchange Online

rosebudhealthcare.com (Default)  
Domain managed outside Office 365

DNS management | Check DNS | Remove

⚠ DNS errors detected, [click here to view](#)

^ Required DNS settings  
Your DNS records must be set up for Exchange Online.  
You can also download or import DNS records from a file.

Export options

^ Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	1	rosebudhealthcare.com	mail.protection.outlook.com	1 Hour
TXT		rosebudhealthcare.com	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME		rosebudhealthcare.com	autodiscover.outlook.com	1 Hour

^ Skype for Business

Type	Host name	Points to address or value	TTL
CNAME	rosebudhealthcare.com	skypeforbusiness.outlook.com	1 Hour
CNAME	rosebudhealthcare.com	skypeforbusiness.outlook.com	1 Hour

^ Mobile Device Management for Office 365

Type	Priority	Host name	Points to address or value	TTL
SRV		rosebudhealthcare.com	_sip sipdir.online.lync.com	1 Hour
SRV		rosebudhealthcare.com	_sipfederationts sipfed.online.lync.com	1 Hour
CNAME	-	enterpriseregistration	enterpriseregistration.windows.net	1 Hour
CNAME	-	enterpriseenrollment	enterpriseenrollment.manage.microsoft.com	1 Hour

Close

4. Add the TXT record of v=spf1 include:spf.protection.outlook.com -all to your DNS settings for our SPF record
5. For our DKIM records we need to publish two CNAME records in DNS

Use the following format for the CNAME Record:

```
Host name: selector1._domainkey.<domain>
Points to address or value: selector1-<domainGUID>._domainkey.<initialDomain>
TTL: 3600

Host name: selector2._domainkey.<domain>
Points to address or value: selector2-<domainGUID>._domainkey.<initialDomain>
TTL: 3600
```

Where:

**<domain>** = our primary domain

**<domainGUID>** = The prefix of our MX record (ex. **domain-com**.mail.protection.outlook.com)

**<initialDomain>** = domain.onmicrosoft.com

Example: DOMAIN = tminus365.com

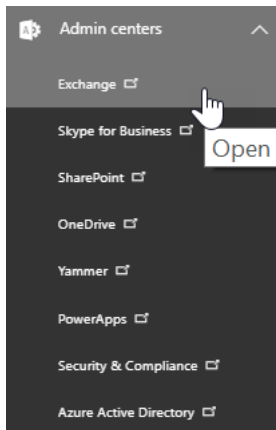
**CNAME Record #1:**

```
Host Name: selector1._domainkey.tminus365.com
Points to address or value: selector1-pax8-com._domainkey.tminus365.onmicrosoft.com
TTL: 3600
```

**CNAME Record #2:**

```
Host Name: selector2._domainkey.tminus365.com
Points to address or value: selector2-pax8-com._domainkey.tminus365.onmicrosoft.com
TTL: 3600
```

6. After Publishing the records, go to Admin Centers>Exchange



7. Go to Protection>DKIM

Exchange admin center

malware filter connection filter spam filter outbound spam quarantine action center [dkim](#)

DKIM (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organization. [Learn more about DKIM](#)

NAME	ACCEPTED DOMAIN	DOMAIN TYPE	
		<b>Authoritative</b>	
		Authoritative	Sign messages for this domain with DKIM signatures: Disabled
		Authoritative	<a href="#">Enable</a>

Status:  
Not signing DKIM signatures for this domain.

Last checked on:  
5/30/2018 8:09 PM




## 8. Select the Domain for which you want to enable DKIM and click “Enable” on the right hand side

### Exchange admin center

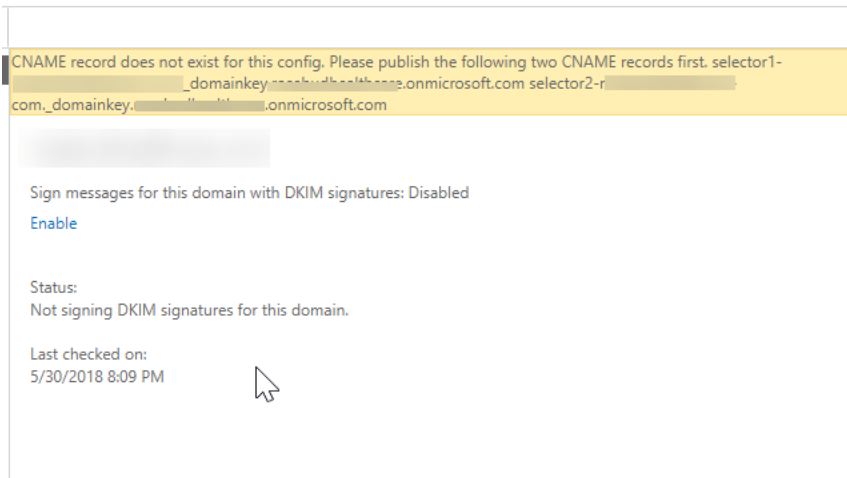
malware filter connection filter spam filter outbound spam quarantine action center [dkim](#)

DKIM (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in your organization. [Learn more about DKIM](#)

NAME	ACCEPTED DOMAIN	DOMAIN TYPE	
		<b>Authoritative</b>	
		Authoritative	
		Authoritative	Sign messages for this domain with DKIM signatures: Disabled <a href="#">Enable</a>
			Status: Not signing DKIM signatures for this domain.
			Last checked on: 5/30/2018 8:09 PM



9. If you have improperly added the CNAME records you will get an error message:



10. With the SPF and DKIM records in place, we can now set up DMARC, the format for the TXT record we want to add is as follows:

```
_dmarc.domain TTL IN TXT "v=DMARC1; pct=100; p=policy"
```

Where:

**<domain>** = domain we want to protect

**<TTL>** = 3600

**<pct=100>** = indicates that this rule should be used for 100% of email

**<policy>** = specifies what policy you want the receiving server to follow if DMARC Fails.

\*NOTE\* You can set <policy> to none, quarantine, or reject

Example:

1. `_dmarc.tminus365.com 3600 IN TXT "v=DMARC1; p=none"`
2. `_dmarc.tminus365.com 3600 IN TXT "v=DMARC1; p=quarantine"`
3. `_dmarc.tminus365.com 3600 IN TXT "v=DMARC1; p=reject"`