



# Hardening 365: Enterprise Edition

*Prepared by*  
**Nick Ross**  
*Sales Engineer*  
([nross@pax8.com](mailto:nross@pax8.com))



**pax8**



## 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 Enterprise market who primarily work with the Enterprise skus available from Microsoft.

## Versioning

Version	Date	Author	Notes
1.0	June 2018	Pax8	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>
<a href="#">Enable Encryption</a>		<a href="#">Create DLP Policies</a>
<a href="#">Enable and User Information Rights Management on Document Data</a>		<a href="#">Enable Advanced Threat Protection safe attachments policy</a>
<a href="#">Enable ATP Safe Links</a>		<a href="#">Implement Cloud App Security</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

Using Office 365 Secure Score .....	6
Enable MFA .....	7
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
Enable Encryption .....	48
Create DLP Policies.....	53
Enable and User Information Rights Management on Document Data .....	65
Enable Advanced Threat Protection safe attachments policy .....	69
Enable ATP Safe Links .....	74
Implement Cloud App Security .....	83



Exchange Online Protection/Antispam Policies.....	92
Connection Filtering:.....	92
Spam Filtering: .....	95
Outbound filtering: .....	100
Mail Flow Rules: .....	100
Malware: .....	102
DNS Settings.....	104



## Using Office 365 Secure Score

---

Microsoft Secure Score

---

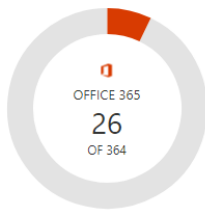
Your Secure Score Summary

26

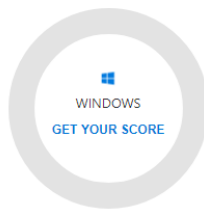
Jun 6, 2018 6:00 PM

Of 364

---



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

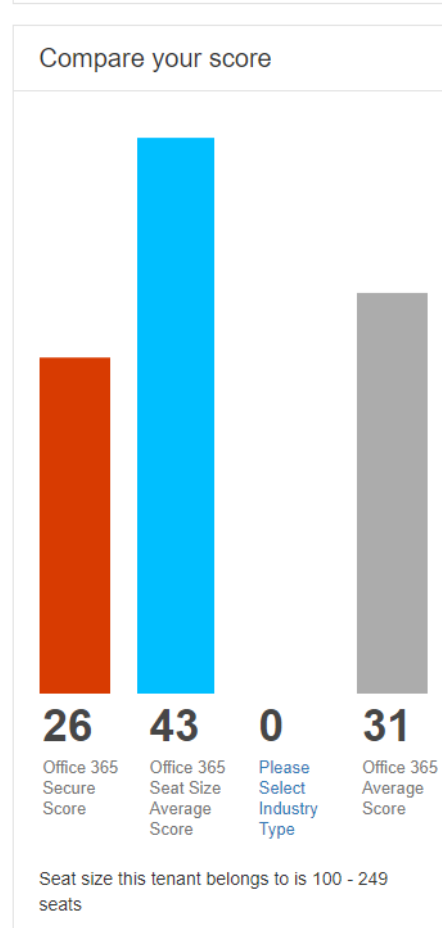


Get the full security story with a [free Windows Defender ATP trial](#)

---

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.



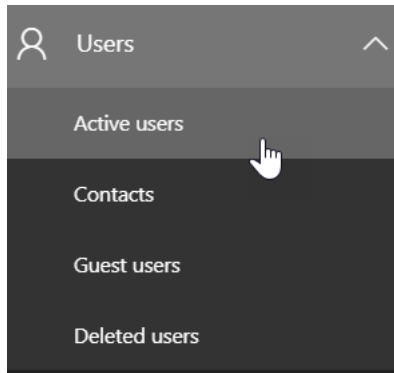
Below is a checklist to help boost your score:

### Enable MFA

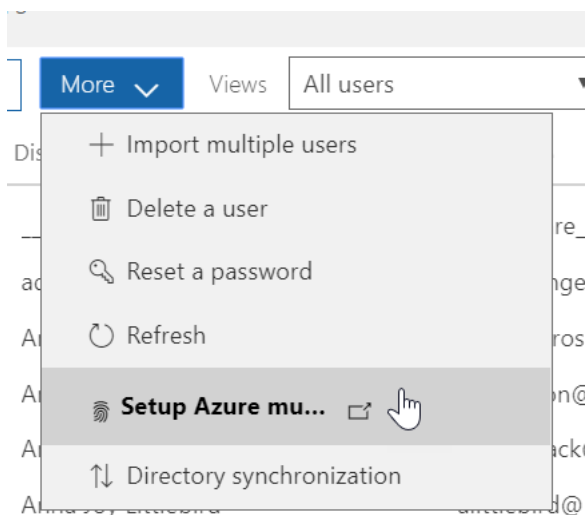
You should enable MFA for all of your user accounts because a breach of any of those accounts can lead to a breach of any data that user has access to.



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: [Sign-in allowed users](#) Multi-Factor Auth status: [Any](#)

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	John Doe	john.doe@contoso.com	Enabled
<input type="checkbox"/>	Jane Smith	jane.smith@contoso.com	Disabled
<input checked="" type="checkbox"/>	Bob Johnson	bob.johnson@contoso.com	Disabled
<input checked="" type="checkbox"/>	Alice Brown	alice.brown@contoso.com	Disabled
<input checked="" type="checkbox"/>	David Wilson	david.wilson@contoso.com	Disabled
<input checked="" type="checkbox"/>	Emily White	emily.white@contoso.com	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



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

<div><div>+ -</div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>		
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

Home > Audit log search

### Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report. [Turn on auditing](#)

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

#### Search

Activities Clear

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](#)

#### Results

Date	IP address	User	Activity	Item	Detail
Run a search to view results					

### 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
umt	Unknown	
dln	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

### Exchange admin center

dashboard	malware filter	connection filter	spam filter	outbound spam	quarantine	action center	dkim
recipients							
permissions							
compliance management							
organization							
protection							
advanced threats							

NAME	
Default	Default
	Copy suspicious messages to addresses: Disabled
	Send notification when senders are blocked: Disabled

## 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

### Default

general	outbound spam preferences
outbound spam preferences	<input type="checkbox"/> Send a copy of all suspicious outbound email messages to the following email address or addresses.
	<input type="checkbox"/> Send a notification to the following email address or addresses when a sender is blocked for sending outbound spam.

## 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”



Search Clear Results 0 results found

Activities	Date	IP address	User	Activity	Item
Added member to Role, ... (2)					
Removed delegation entry					
Role administration activities					
Added member to Role		✓	Removed a user from a directory role		✓
Directory administration activities			Set company contact information		

## 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

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

recipients

permissions

compliance management

organization

protection

advanced threats

mail flow

mobile

public folders

unified messaging

Help

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](#)

### Run an administrator role group report...

Search the admin audit log for changes made to role groups, which are used to assign administrative permissions to users. [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](#)

### 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](#)

### 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 admin audit log report...

View entries from the admin audit log about configuration changes made by administrators in your organization. [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 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:

select mailboxes...

Search for access by:

All non-owners

search

clear

Search results

Mailbox

LAST ACCESSED:

There are no items to show in this view.



Close

## Review the Malware Detections Report Weekly

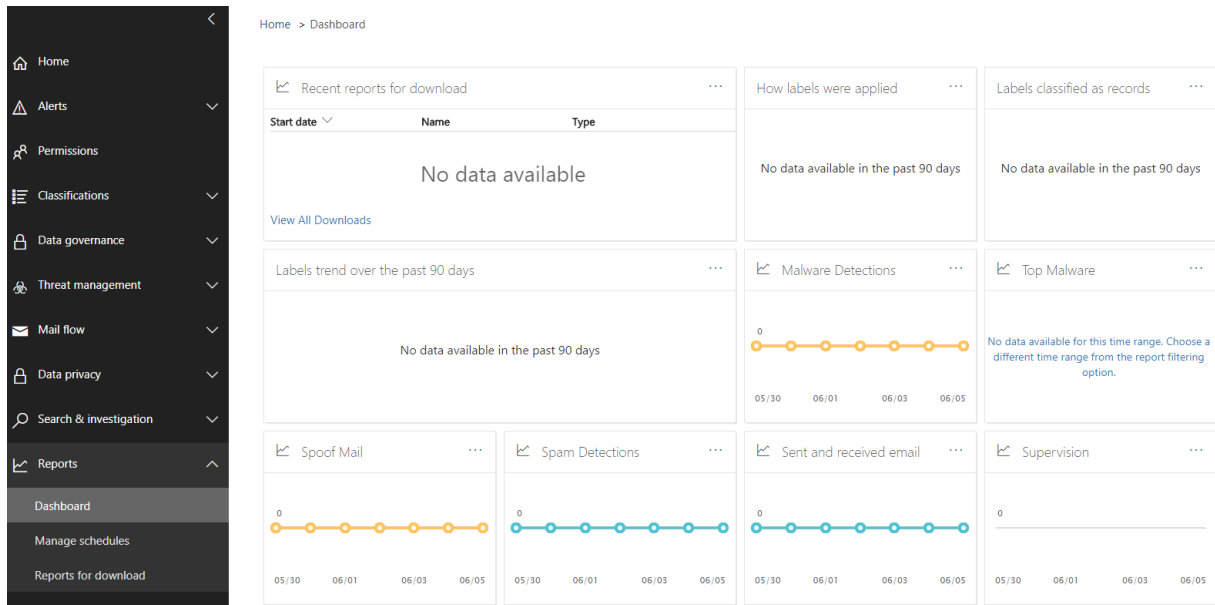
This report shows specific instances of Microsoft blocking a malware attachment from reaching your users. While this report isn't strictly actionable, reviewing it will give you a sense of the overall volume of



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

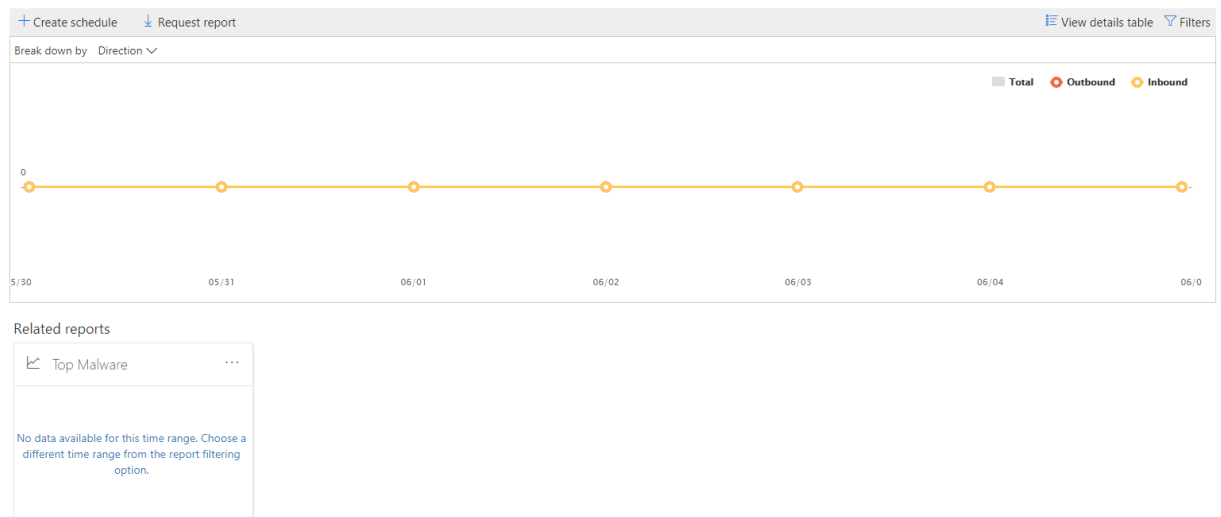


## 2. Click on Malware Detections

## 3. View the Detection Report

Home > Dashboard > Report Viewer - Security & Compliance

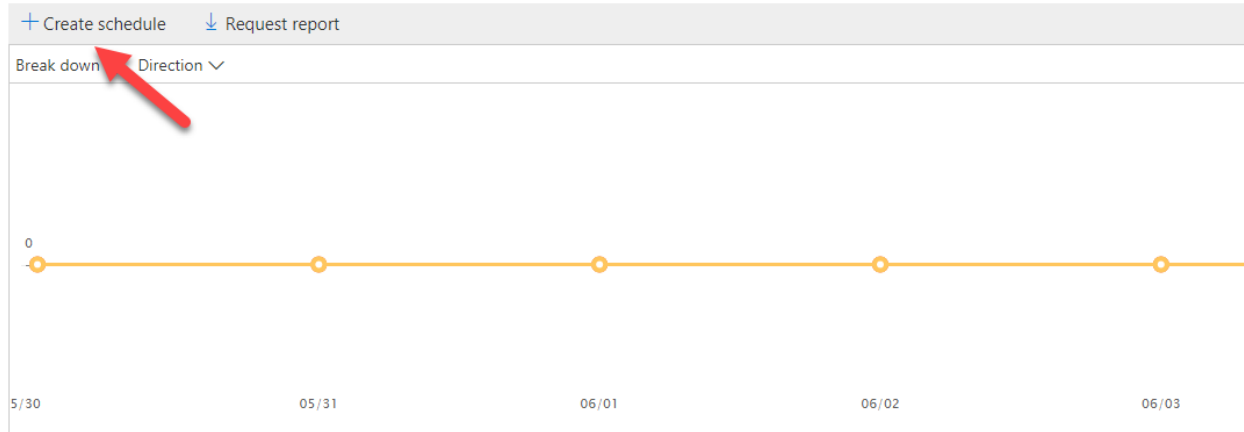
### Malware Detections Report





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

Home > My records > Audit logs

Azure Active Directory

Audit logs

Search (Ctrl+F)

Columns Refresh Download Troubleshoot

Category: All Activity Resource Type: All Activity: Assign external user to application

Date Range: 7 Days Target: Enter target name or upn Initiated By (Actor): Enter actor name or upn

Apply

Search to filter items...

DATE	TARGET(S)	INITIATED BY (ACTOR)
No audit logs found		

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

Category: All Activity Resource Type: All Activity: Assign external user to application

Date Range: 7 Days Target: Enter target name or upn Initiated By (Actor): Enter actor name or upn

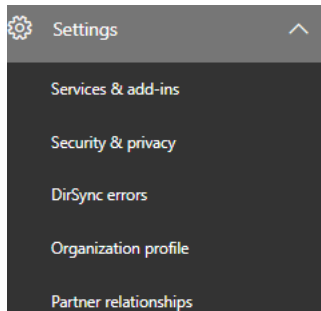
Apply

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



### 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

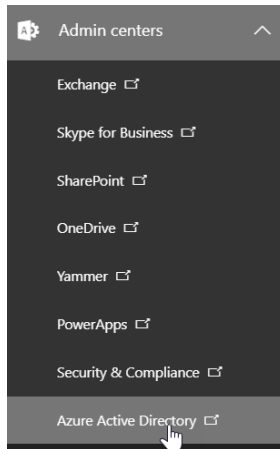
Cancel

## Review Sign-Ins after Multiple Failures report weekly

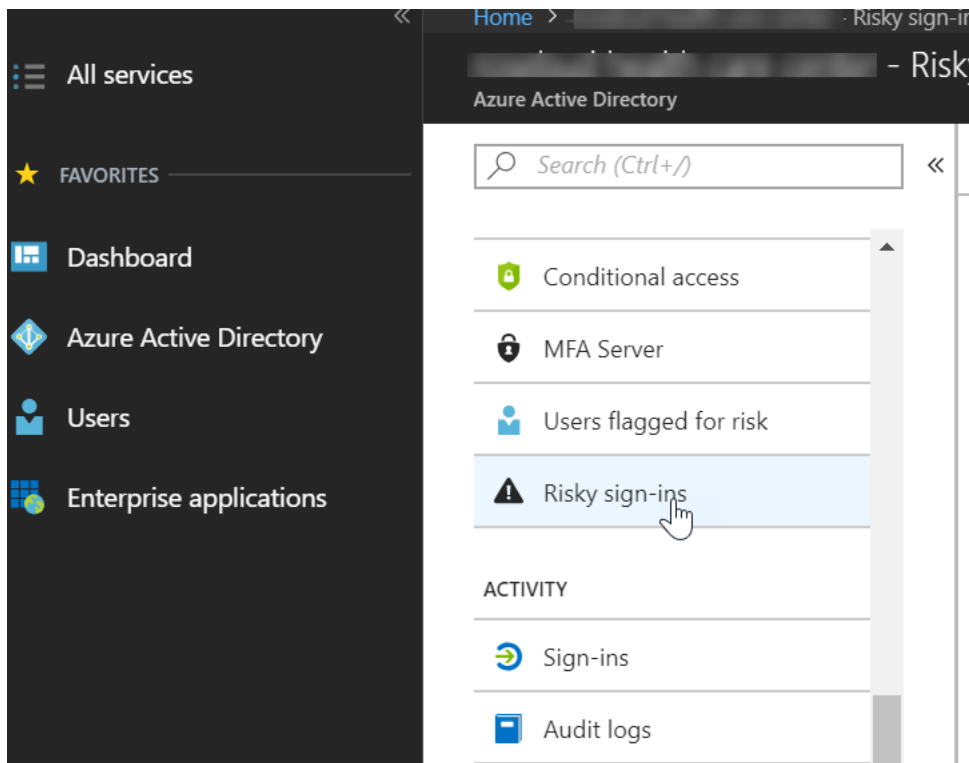
These reports contains records of accounts that have successfully signed-in after multiple risk events, such as locations, IP addresses which could be an indication that the account could be compromised.



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

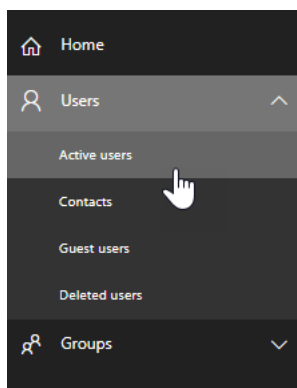
Left sidebar menu:

- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings
- SECURITY
  - Conditional access
  - MFA Server
  - Users flagged for risk
  - Risky sign-ins

## 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

Admin 2

×

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

Off

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

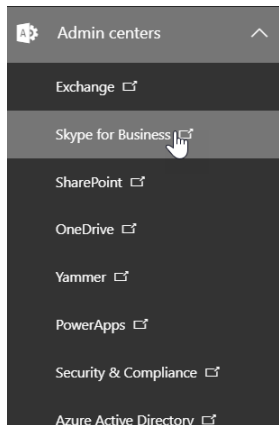
Global admini  
are the only  
Make sure a  
a mobile ph  
in their cont  
passwords a

## 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

dashboard

users

organization

audio conferencing

online meetings

tools

reports

general

external communications

external access

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

On except for blocked domains

public IM connectivity

☒ Let people use Skype for Business to communicate with Skype users outside your organization.

blocked or allowed domains

+

DOMAIN	STATUS
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

+

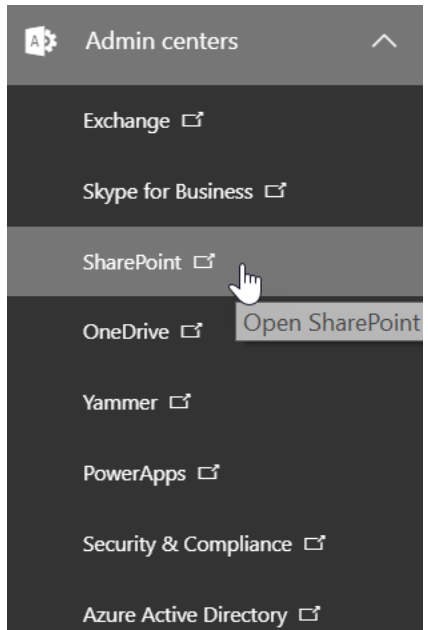
DOMAIN	STATUS
There are no results to display.	

## 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:

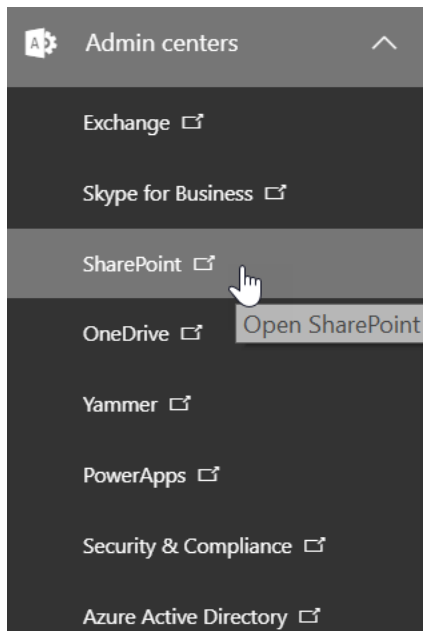


### Enable Versioning on all SharePoint Online Document Libraries

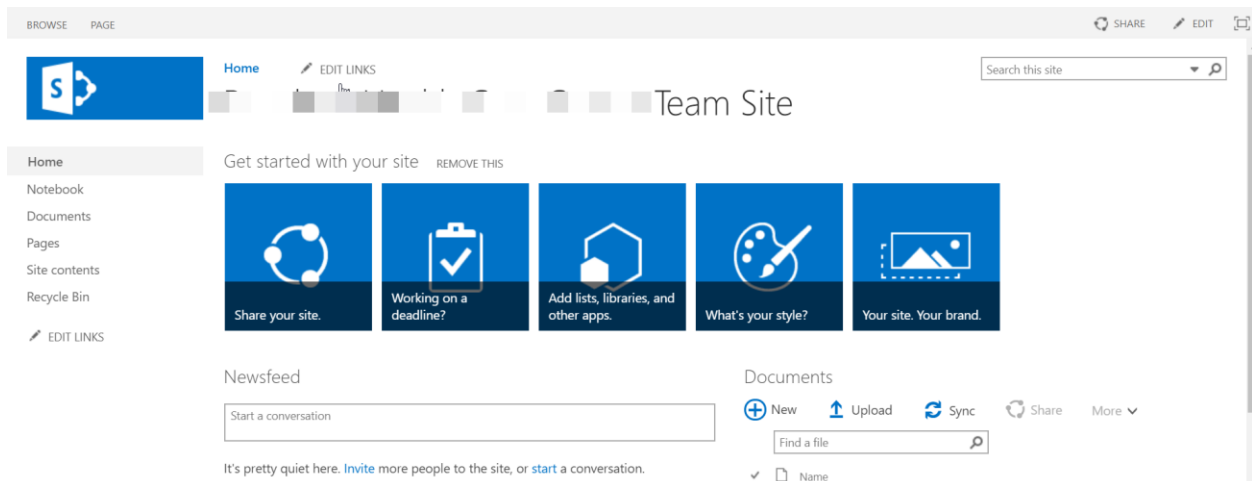
You should enable versioning on all of your SharePoint online site collection document libraries. This will ensure that accidental or malicious changes to document content can be recovered.



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



Office 365

BROWSEPAGE

Home

Notebook

Documents

Pages

Site contents

Recycle Bin

EDIT LINKS

Home

EDIT LINKS

Team Site

Get started with your site REMOVE THIS

Share your site.

Working on a deadline?

Add lists, libraries, and other apps.

What's your style?

Your site. Your brand.

Newsfeed

Documents

NewUploadSyncShareMore

Office 365 settings

Shared with...

Edit page

Add a page

Add an app

Site contents

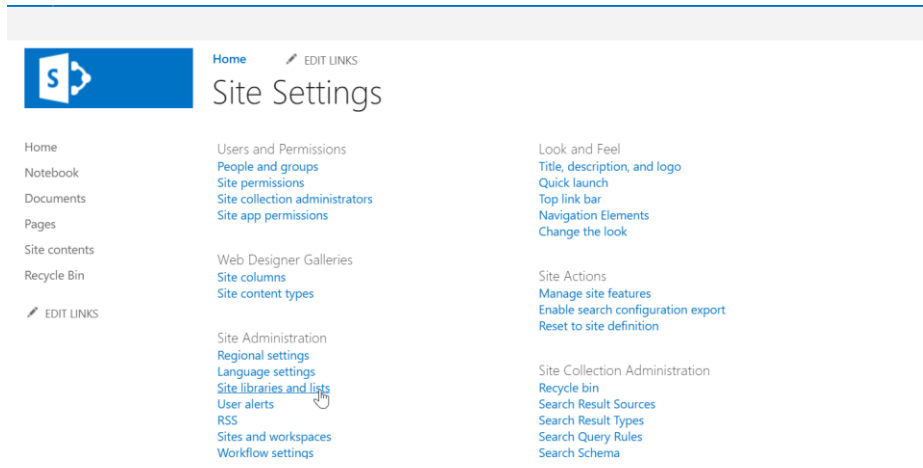
Change the look

Site settings

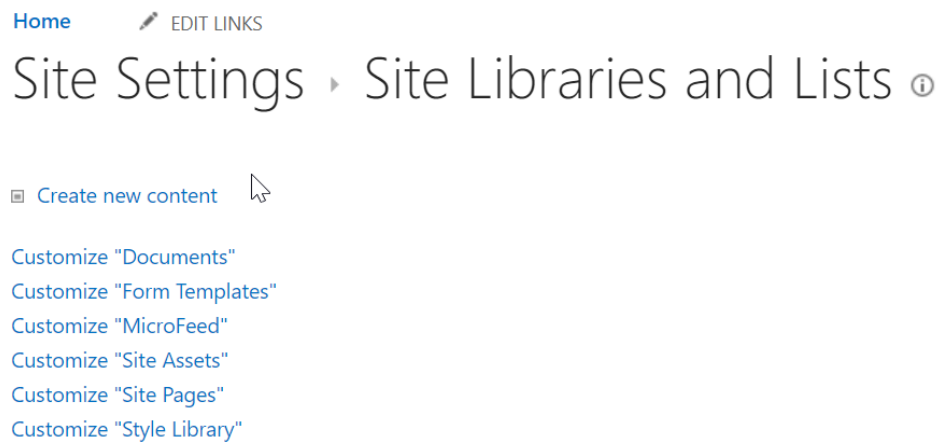
Getting started



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



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





## 6. Click on Versioning Settings

The screenshot shows the SharePoint 'Documents > Settings' page. On the left is a navigation pane with links: Home, Notebook, Documents, Pages, Site contents, Recycle Bin, and EDIT LINKS. The main area is titled 'Documents > Settings' and contains three sections: 'List Information', 'General Settings', and 'Permissions and Management'. Under 'List Information', there are fields for Name, Web Address, and Description. Under 'General Settings', there is a list of links: List name, description and navigation; Versioning settings (highlighted with a mouse cursor); Advanced settings; Validation settings; Column default value settings; and Audience targeting settings. Under 'Permissions and Management', there are links: 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; and Generate file plan report. On the far right, there is a 'Communications' section with a link for RSS settings.

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

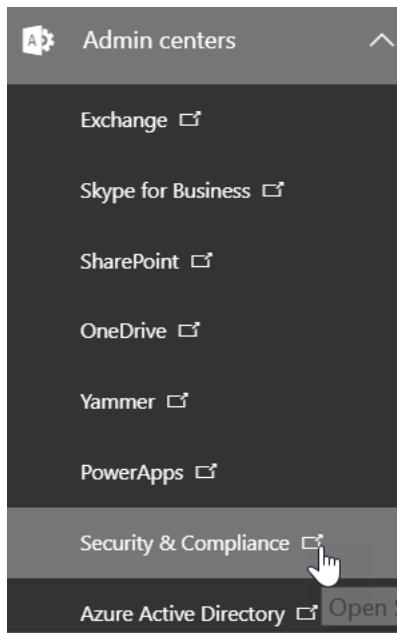
The screenshot shows the 'Settings > Versioning Settings' page. It has a left sidebar with 'Content Approval' and 'Document Version History' sections. The main area is titled 'Settings > Versioning Settings' and contains three sections: 'Content Approval', 'Document Version History', and 'Versioning Settings'. The 'Content Approval' section has a heading 'Content Approval' and a description: 'Specify whether new items or changes to existing items should remain in a draft state until they have been approved. [Learn about requiring approval.](#)'. The 'Document Version History' section has a heading 'Document Version History' and a description: 'Specify whether a version is created each time you edit a file in this document library. [Learn about versions.](#)'. The 'Versioning Settings' section has a heading 'Versioning Settings' and a description: 'Specify whether a version is created each time you edit a file in this document library. [Learn about versions.](#)'. Below the description are three sections: 'Require content approval for submitted items?' with radio buttons for 'Yes' and 'No' (selected); 'Create a version each time you edit a file in this document library?' with radio buttons for 'No versioning', 'Create major versions' (selected), and 'Create major and minor (draft) versions' (indicated by a red arrow); and 'Optionally limit the number of versions to retain:' with a checkbox for 'Keep the following number of major versions:' (checked) and a text box containing '500', and a checkbox for 'Keep drafts for the following number of major versions:' (unchecked).



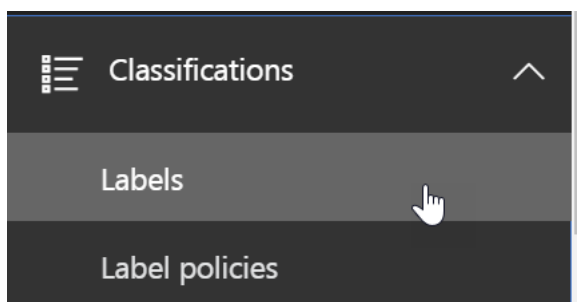
## Tag Documents in SharePoint

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](#)

[+ Create a label](#) [Publish labels](#) [Auto-apply a label](#) [Refresh](#)

<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 ⓘ

[Next](#) [Cancel](#) [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 were ready to "Publish the Label"

# HIPPA Tag

Edit label

Publish label

Auto-apply a label

Delete label

**Name**  
HIPPA Tag

**Description for admins**  
All Documents containing PII

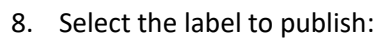
Edit

**Description for users**  
This is a tag for sensitive data

Edit

Close

Feedback



## 9. Choose your locations

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.

✓ Choose labels to publish

✓ Publish to these locations

✓ Name your policy

● Review your settings

Review your settings

⚠ 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

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

HIPPA Tag 7 years keep

Publish to these locations

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

Edit label

Publish label

Auto-apply a label

Delete label

Name

HIPPA Tag

Description for admins

All Documents containing PII

Edit

Description for users

This is a tag for sensitive data

Edit

Close

Feedback

44



### 13. Choose your Conditions:

Automatically apply a label to content

☒ Choose label to auto-apply

☐ Choose conditions

☐ Settings

☐ Name your policy

☐ Locations

☐ Review your settings

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

Feedback

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

Automatically apply a label to content

☒ Choose label to auto-apply

☐ Choose conditions

☐ Settings

☐ Name your policy

☐ Locations

☐ Review your settings

Select from a template

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

Search

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



### 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

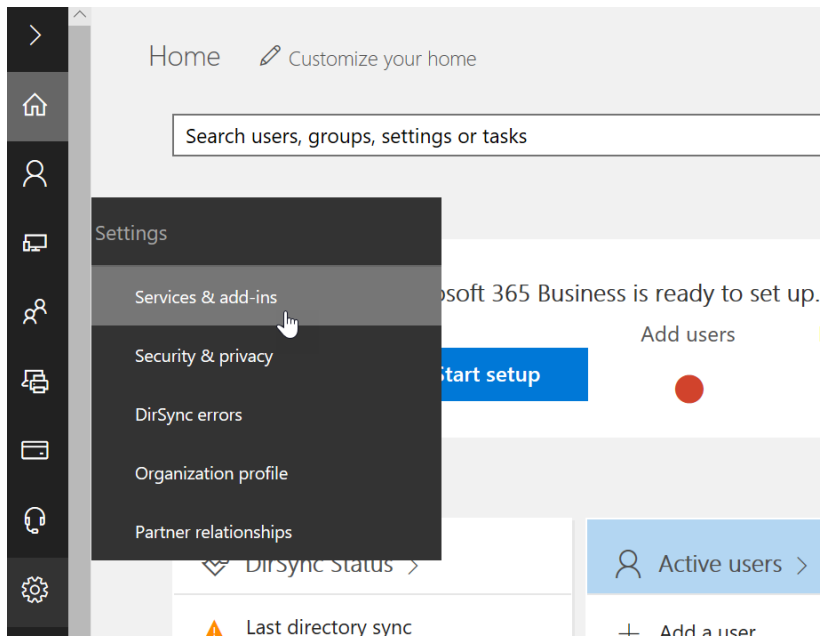
Cancel

Feedback









## Enable Encryption

1. In the Admin Center, go to Settings>Services&Add-Ins;





## 2. Find “Microsoft Azure Information Protection”

Name ▾	Host App
	Dynamics Customer Insights Preview Manage and update your Dynamics Customer Insights Preview settings
	Integrated Apps Manage your Integrated Apps settings
	Mail Set up auditing, track messages, and protect email from spam and malware
	Microsoft Azure Information Protection Update your settings for Microsoft Azure Information Protection
	Microsoft Forms Manage and update your Microsoft Forms settings
	Microsoft Teams Manage and update your Microsoft Teams settings



3. Select "Manage Microsoft Azure Information Protection settings"



## Microsoft Azure Information Protection

### Keep your information safe, online or offline

With Microsoft Azure Information Protection you can add another layer of protection to the data you store in Office 365. The rules you set protect your files whether they're viewed using Office online or downloaded to a user's device. Policies and encryption let you safely share files in email or OneDrive and safeguard confidential information.

[Manage Microsoft Azure Information Protection settings](#) 

Close



#### 4. Make sure Rights Management is activated

## rights management



### Rights management is activated

Rights Management safeguards your email and documents, and helps you securely share this data with your colleagues.

To disable Rights Management, click deactivate.

deactivate

### resources

- [What is Rights Management?](#)
- [Rights Management Deployment roadmap](#)
- [Using Rights Management](#)
- [FAQs For Rights Management](#)

## additional configuration

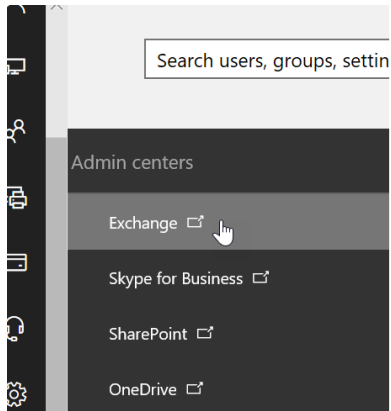
You can configure advanced features for Rights Management using Microsoft Azure.

This requires a one-time sign up for a free Azure subscription to access Azure Active Directory.

advanced features

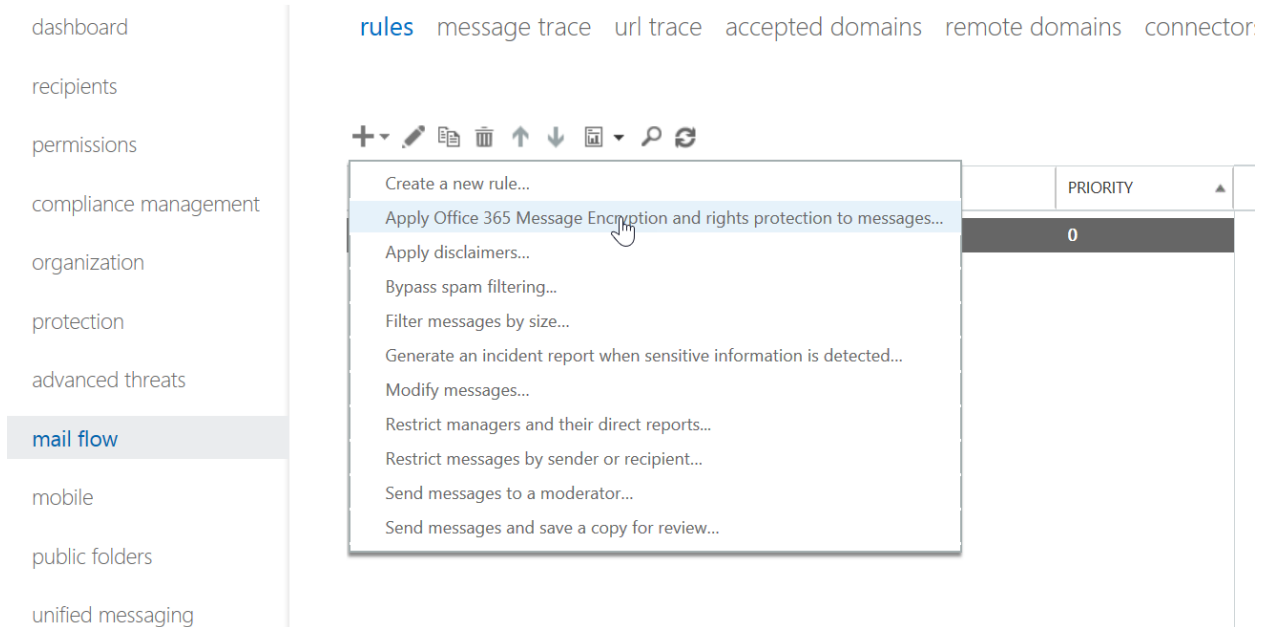


5. After this is active, go to the Exchange Admin Center



6. Go to Mail Flow>Rules and click the + icon to add a new rule. From here you will be able to configure a rule to automatically encrypt messages based off of certain parameters

## Exchange admin center





## 7. Apply Rules Particular to Your Organization

new rule

Name:

\*Apply this rule if...  
 ['U.S. Social Security Number \(SSN\)' or 'ABA Routing Number' or 'U.S. Bank Account Number'](#)

\*Do the following...  
 [\\*Select one...](#)

Except if...

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

8. From here this rule will automatically encrypt messages that define these parameters. Additionally, users will be able to encrypt messages at will via OWA

## Create DLP Policies

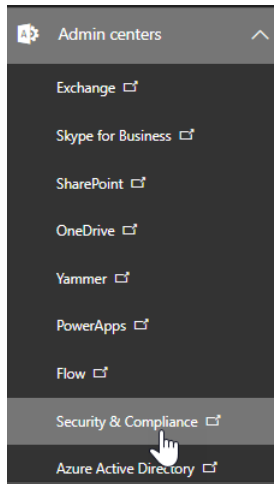
To comply with business standards and industry regulations, organizations need to protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy in the Office 365 Security & Compliance Center, you can identify, monitor, and automatically protect sensitive information across Office 365.

For a detailed support article containing everything on DLP, Click [this link](#)

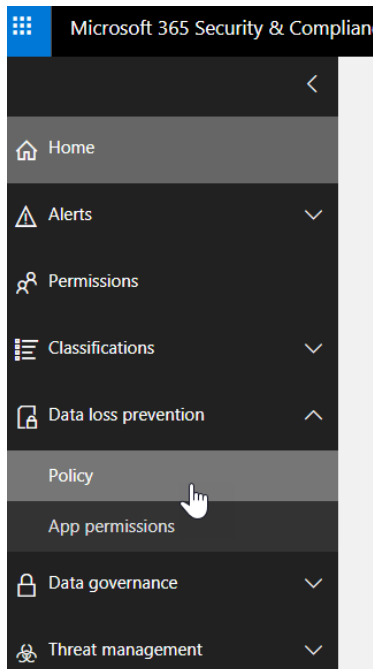
Here are the steps:



1. Go to Admin Centers>Security and Compliance Center



2. Click the Data Loss Prevention Tab and then click Policy

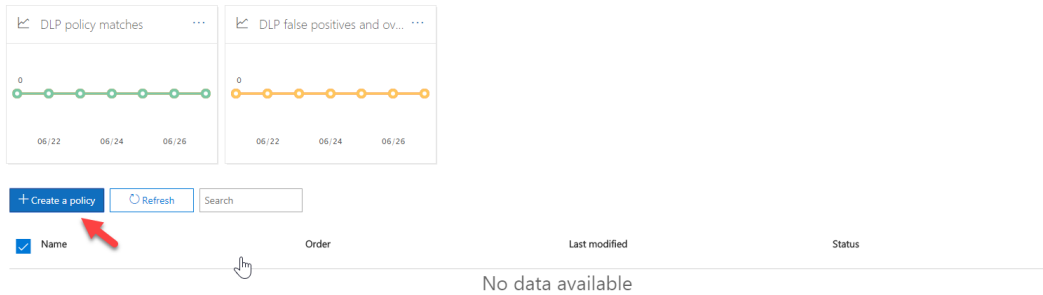


3. On the new screen that pops up, click +Create a policy



Home > Data loss prevention

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more](#)



4. From here you can select from a list of predesigned policy templates or customize your own. For this example, I am going to create a policy for HIPAA compliance:

New DLP policy

● Choose the information to protect

● Name your policy

● Choose locations

● Policy settings

● Review your settings

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.  
[Learn more about DLP policy templates](#)

Search

Show options for All countries or regions ▼

Financial

Medical and health

Privacy

Custom

Custom policy

Custom policy

Description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Next

Cancel

5. Go to Medical and Health> US Health Insurance Act>Click Next

55



New DLP policy

● Choose the information to protect

● Name your policy

● Choose locations

● Policy settings

● Review your settings

## Start with a template or create a custom policy



Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

[Learn more about DLP policy templates](#)

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.K. Access to Medical Reports Act

U.S. Health Insurance Act (HIPAA)

### 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

Next

Cancel



6. Here you can give a name and description for your policy

New DLP policy

☒ Choose the information to protect

☐ Name your policy

☐ Choose locations

☐ Policy settings

☐ Review your settings

### Name your policy

Name \*

Description

7. Next, you can chose the locations you want this policy to be active whether that be Exchange Online, OneDrive, or Sharepoint

New DLP policy

☒ Choose the information to protect

☒ Name your policy

☐ Choose locations

☐ Policy settings

☐ Review your settings

### Choose locations

We'll protect content that's stored in the locations you choose. \*

☒ All locations in Office 365. Includes content in Exchange email and OneDrive and SharePoint documents.

☐ Let me choose specific locations.



- From here we can get even more granular with our settings. I can choose to add more content to my filter and choose whether to detect content that is shared inside or outside more organization

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

● Policy settings

● Review your settings

Customize the type of content you want to protect

Select 'Find content that contains' if you want to quickly set up a policy that protects only sensitive information or labeled content. Use advanced settings for more options, such as protecting content in email messages sent to specific domains, attachments with specific file extensions, and more.

☒ Find content that contains: ⓘ  
PII Identifiers  
Medical Terms  
[Edit](#)

☒ Detect when this content is shared:  
with people outside my organization ▼

☐ Use advanced settings ⓘ

Back

Next

Cancel

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

● Policy settings

● Review your settings

Customize the type of content you want to protect

Select 'Find content that contains' if you want to quickly set up a policy that protects only sensitive information or labeled content. Use advanced settings for more options, such as protecting content in email messages sent to specific domains, attachments with specific file extensions, and more.

☒ Find content that contains: ⓘ  
PII Identifiers  
Medical Terms  
[Edit](#)

☒ Detect when this content is shared:  
with people outside my organization ▼  
with people outside my organization  
only with people inside my organization

☐ Use advanced settings ⓘ

Back

Next

Cancel

58



9. If I click on the “User Advanced Settings” icon, I can create a new rule to apply more granular conditions to my policies. These rules include exceptions, actions to take when condition are met, user notifications, user overrides, and incident reports that are sent to admins when a rule match occurs

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations

Policy settings

Review your settings

Customize the type of content you want to protect

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones. [Learn more about DLP rules](#)

+ New rule

Name	Status	Priority
Content matches U.S. HIPAA	<input checked="" type="checkbox"/>	1

Back Next Cancel



#### ^ Actions

Use actions to protect content when the conditions are met.

[+ Add an action ▾](#)

#### ^ User notifications

Use Notifications to inform your users and help educate them on the proper use of sensitive information.



#### ^ User overrides

Let people who see the tip override the policy and share the content.



ⓘ You must turn on user notifications to let users override the policy.

#### ^ Incident reports

Use this severity level in admin alerts and reports:

Low ▾

Send an alert to admins when a rule match occurs.



Use email incident reports to notify you when a policy match occurs.



Save

Cancel



10. From here you can customize what to do if sensitive info is protected. You can use notifications and overrides to educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

● Policy settings

● Review your settings

What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

☒ Show policy tips to users and send them an email notification.  
Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)  
[Customize the tip and email](#)

☐ Send incident reports in email  
By default, you and your global admin will automatically receive the email.

☐ Restrict who can access the content and override the policy  
People outside your org can't access the content.

Back

Next

Cancel



## 11. Lastly, you can choose to test the policy before going into full production:

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

● Policy settings

● Review your settings

What do you want to do if we detect sensitive info?

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

☒ Show policy tips to users and send them an email notification.  
Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)  
[Customize the tip and email](#)

☐ Send incident reports in email  
By default, you and your global admin will automatically receive the email.

☐ Restrict who can access the content and override the policy  
People outside your org can't access the content.

Back

Next

Cancel



## 12. Once you review your settings, you can click Create

New DLP policy

✓ Choose the information to protect

✓ Name your policy

✓ Choose locations

✓ Policy settings

● Review your settings

Review your settings

Template name

U.S. Health Insurance Act (HIPAA)

Edit

Policy name

U.S. Health Insurance Act (HIPAA)

Edit

Description

Edit

Applies to content in these locations

Exchange email  
SharePoint sites  
OneDrive accounts

Edit

Policy settings

If the content has these types of sensitive information: PII Identifiers, Medical Terms then notify people with a policy tip and email message. .

Edit

Turn policy on after it's created?

Test it out first. Don't apply actions or show policy tips to users.

Edit

Back

Create

Cancel

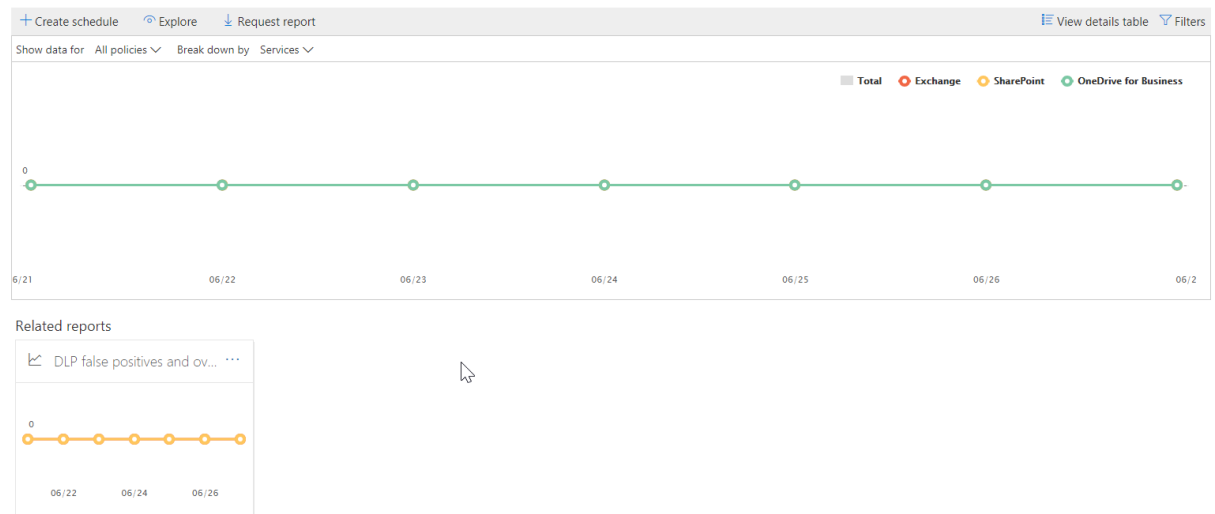


13. After you create and turn on your DLP policies, you'll want to verify that they're working as you intended and helping you stay compliant. With DLP reports, you can quickly view the number of DLP policy and rule matches over time, and the number of false positives and overrides. For each report, you can filter those matches by location, time frame, and even narrow it down to a specific policy, rule, or action.

Home > Dashboard > Report Viewer - Security & Compliance

### DLP policy matches

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive information. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people.





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:

2018-06-28

Frequency

Weekly

Send email to

-----@-----

Schedule Name

Schedule-Weekly-UnifiedPolicyDLP

Create schedule

Cancel

Options

[Customize schedule](#)

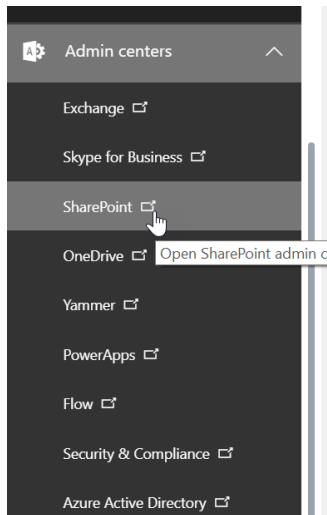
## Enable and User Information Rights Management on Document Data

You should enable and use Information Rights Management protections on email and document data. This will help prevent accidental or malicious exposure of your data outside of your organizational boundaries. Attackers targeting specific, high value data assets will be prevented from opening them without a user credential in your tenancy.



Steps:

1. Go to Admin Center>Sharepoint



2. Select the site you want to edit from Site Collections

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](#)

Site Collections

New Delete Properties Owners Sharing Buy Storage Server Resource Quota Upgrade Recycle Bin

Contribute Manage Restore

Search by URL...

1.09 TB available of 1.09 TB 2400 resources available

URL	STORAGE USED (GB)	SERVER RESOURCE QUOTA
	0.00	300
	0.00	0
	0.03	0
	0.13	200
	0.00	0



### 3. Click on the Gear icon and go to Site Settings

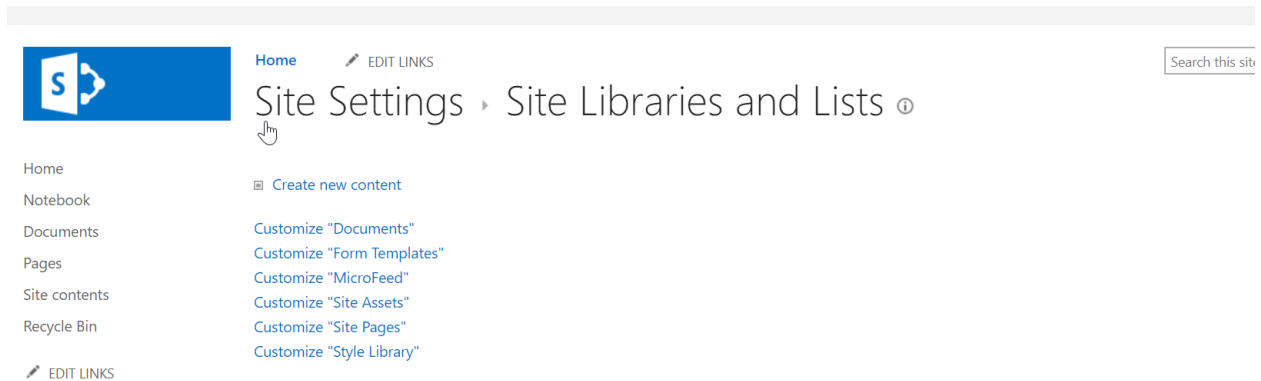
The screenshot shows the SharePoint 'Team Site' home page. On the left is a navigation pane with links like Home, Notebook, Documents, Pages, Site contents, and Recycle Bin. The main area has a 'Get started with your site' section with five tiles: 'Share your site', 'Working on a deadline?', 'Add lists, libraries, and other apps', 'What's your style?', and 'Your site. Your brand.'. Below this is a 'Newsfeed' section with a text input and a 'Documents' section with buttons for New, Upload, Sync, Share, and More. A gear icon in the top right corner is open, showing a menu with options like Office 365 settings, SharePoint settings, and Site settings. A red arrow points to the 'Site settings' option.

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

The screenshot shows the 'Site Settings' page. The left navigation pane is expanded to 'Site Administration'. Under 'Site Administration', there is a list of links: Regional settings, Language settings, Site libraries and lists, User alerts, RSS, Sites and workspaces, Workflow settings, Site Closure and Deletion, and Popularity Trends. A red arrow points to the 'Site libraries and lists' link. The main area is divided into three columns: 'Users and Permissions', 'Web Designer Galleries', and 'Site Administration'. The 'Site Administration' column contains the link 'Site libraries and lists'.

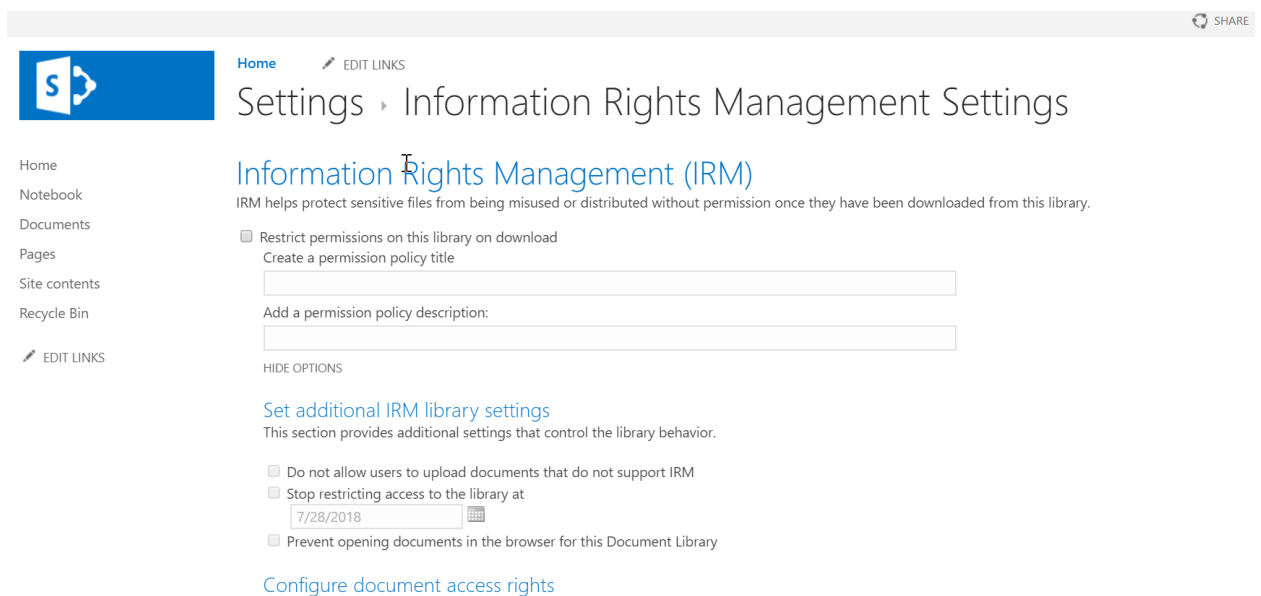


5. Click on the Library/List that you want to apply IRM



The screenshot shows the SharePoint 'Site Settings' page. The left sidebar contains a navigation menu with links: Home, Notebook, Documents, Pages, Site contents, Recycle Bin, and an 'EDIT LINKS' button. The main content area has a breadcrumb trail 'Home > Site Settings > Site Libraries and Lists' with an information icon. Below the breadcrumb, there is a 'Create new content' button and a list of customization options: 'Customize "Documents"', 'Customize "Form Templates"', 'Customize "MicroFeed"', 'Customize "Site Assets"', 'Customize "Site Pages"', and 'Customize "Style Library"'. A search bar in the top right corner is labeled 'Search this site'.

6. From here you can customize the settings you want to apply



The screenshot shows the 'Information Rights Management (IRM) Settings' page. The left sidebar is identical to the previous screenshot. The main content area has a breadcrumb trail 'Home > Settings > Information Rights Management Settings'. The title 'Information Rights Management (IRM)' is displayed in blue. Below the title, a description states: 'IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this library.' There is a checkbox labeled 'Restrict permissions on this library on download' which is currently unchecked. Below this checkbox, there is a text input field for 'Create a permission policy title' and another for 'Add a permission policy description:'. A 'HIDE OPTIONS' link is present. Further down, there is a section titled 'Set additional IRM library settings' with the text 'This section provides additional settings that control the library behavior.' Below this, there are three checkboxes: 'Do not allow users to upload documents that do not support IRM', 'Stop restricting access to the library at' (with a date input field showing '7/28/2018'), and 'Prevent opening documents in the browser for this Document Library'. At the bottom, there is a link 'Configure document access rights'.



#### [Set additional IRM library settings](#)

This section provides additional settings that control the library behavior.

- ☐ Do not allow users to upload documents that do not support IRM
- ☐ Stop restricting access to the library at
- ☐ Prevent opening documents in the browser for this Document Library

#### [Configure document access rights](#)

This section control the document access rights (for viewers) after the document is downloaded from the library; read only viewing right is the default. Granting the rights below is reducing the bar for accessing the content by unauthorized users.

- ☐ Allow viewers to print
- ☐ Allow viewers to run script and screen reader to function on downloaded documents
- ☐ Allow viewers to write on a copy of the downloaded document
- ☐ After download, document access rights will expire after these number of days (1-365)

#### [Set group protection and credentials interval](#)

Use the settings in this section to control the caching policy of the license the application that opens the document will use and to allow sharing the downloaded document with users that belong to a specified group

- ☐ Users must verify their credentials using this interval (days)
- ☐ Allow group protection. Default group:

## Enable Advanced Threat Protection safe attachments policy

This will extend the malware protections in the service to include routing all messages and attachments that don't have a known virus/malware signature to a special hypervisor environment where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. This will extend the malware protections in the service to include routing all messages and attachments that don't have a known virus/malware signature to a special hypervisor environment where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent.

### \*Licensing Note\*

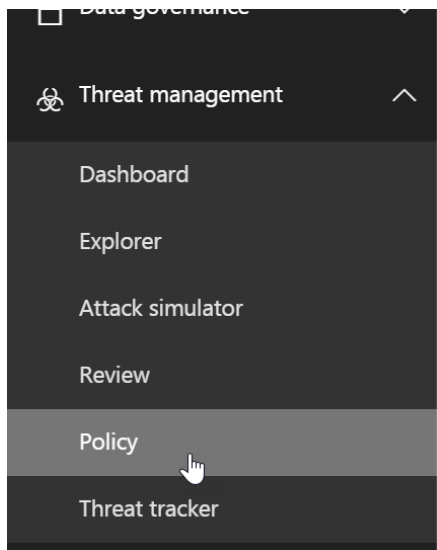
The ATP Safe Links features are only available in Advanced Threat Protection. Office 365 ATP is included in subscriptions, such as:

- Office 365 Enterprise E5
- Office 365 Education A5
- Microsoft 365 Business
- Add-On

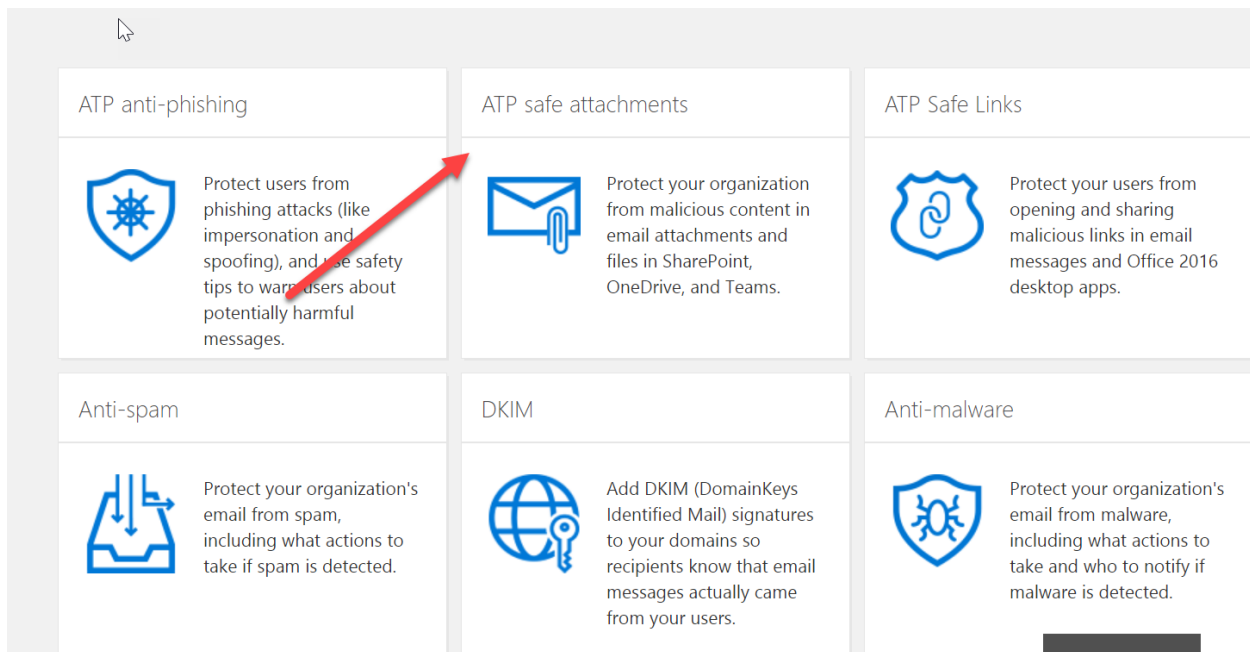
Steps:



1. In the Security and Compliance Center, go to Threat Management>Policy



2. Click on the ATP Safe Attachments Icon



3. Checkmark the box next to “Turn on ATP for SharePoint, OneDrive, and Microsoft Teams”



Home > Safe attachments

## 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](#)

Reports for this feature just got better. Check out the new [report](#) in the Security and Compliance Center for an enhanced reporting experience.



ENABLED	NAME	PRIORITY	
There are no items to show in this view.			

0 selected of 0 total

Save

Feedback



#### 4. Click the + icon to set up a new policy

Home > Safe attachments

## 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](#)

Reports for this feature just got better. Check out the new [report](#) in the Security and Compliance Center for an enhanced reporting experience.



ENABLED	NAME	PRIORITY
There are no items to show in this view.		

0 selected of 0 total

Save

Feedback



5. Here you have some setting that you can adjust. First you will name your policy. Then you will have the option to select what action to take when malware is detected. The options to choose from are Off, Monitor, Block, Replace, and Dynamic Delivery. All of these options will slow mail flow except for Dynamic Delivery. The Dynamic Delivery option sends the mail immediately and replaces the attachment with a placeholder file until the scan is complete. For a more detailed explanation of these options, please follow [this support article](#).

### new safe attachments policy

\*Name:

Description:

#### Safe attachments unknown malware response

Select the action for unknown malware in attachments. [Learn more](#)

##### Warning

Monitor, Replace and Block actions may cause significant delay to email delivery. [Learn more](#)

Dynamic Delivery is only available for recipients with hosted mailboxes. [Learn more](#)

If you choose the Block, Replace or Dynamic Delivery options and malware is detected in attachment, the message containing the attachment will be quarantined and can be released only by an admin.

- ☒ Off - Attachment will not be scanned for malware.
- ☐ Monitor - Continue delivering the message after malware is detected; track scan results.
- ☐ Block - Block the current and future emails and attachments with detected malware.
- ☐ Replace - Block the attachments with detected malware, continue to deliver the message.
- ☐ Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

#### Redirect attachment on detection

Send the blocked, monitored, or replaced attachment to an email address.

☐ Enable redirect

You can also choose to redirect the attachment to another email such as an admin or quarantine mailbox.



Redirect attachment on detection

Send the blocked, monitored, or replaced attachment to an email address.

☐ Enable redirect

Send the attachment to the following email address

☒ Apply the above selection if malware scanning for attachments times out or error occurs.

### Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

\*If...

Except if...

Lastly, you will notice above, you can specify this policy to specific groups or domains.

## Enable ATP Safe Links

This will extend the phishing protection in the service to include redirecting all email hyperlinks through a forwarding service which will block malicious ones even after it has been delivered to the end user. Beginning in late October 2017, ATP Safe Links protection is extended to apply to URLs in email as well as URLs in Office 365 ProPlus documents, such as Word, Excel, PowerPoint, and Visio on Windows, as well as Office apps on iOS and Android devices



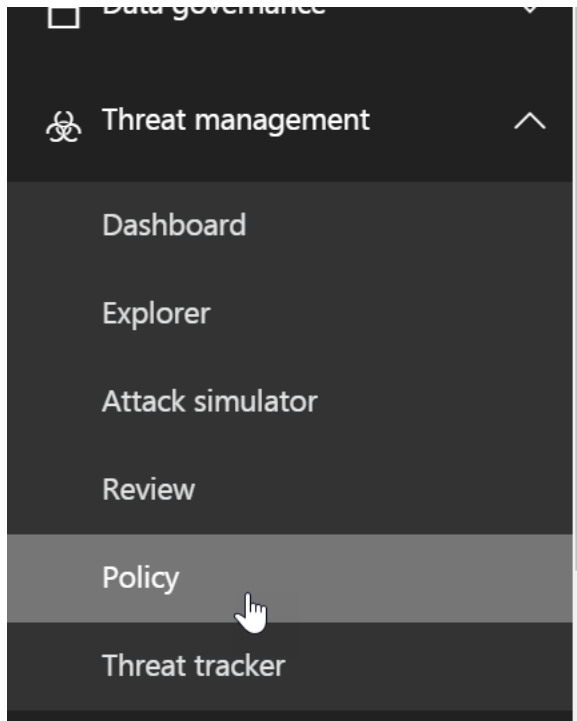
**\*Licensing Note\***

The ATP Safe Links features are only available in Advanced Threat Protection. Office 365 ATP is included in subscriptions, such as:

- Office 365 Enterprise E5
- Office 365 Education A5
- Microsoft 365 Business
- Add-On

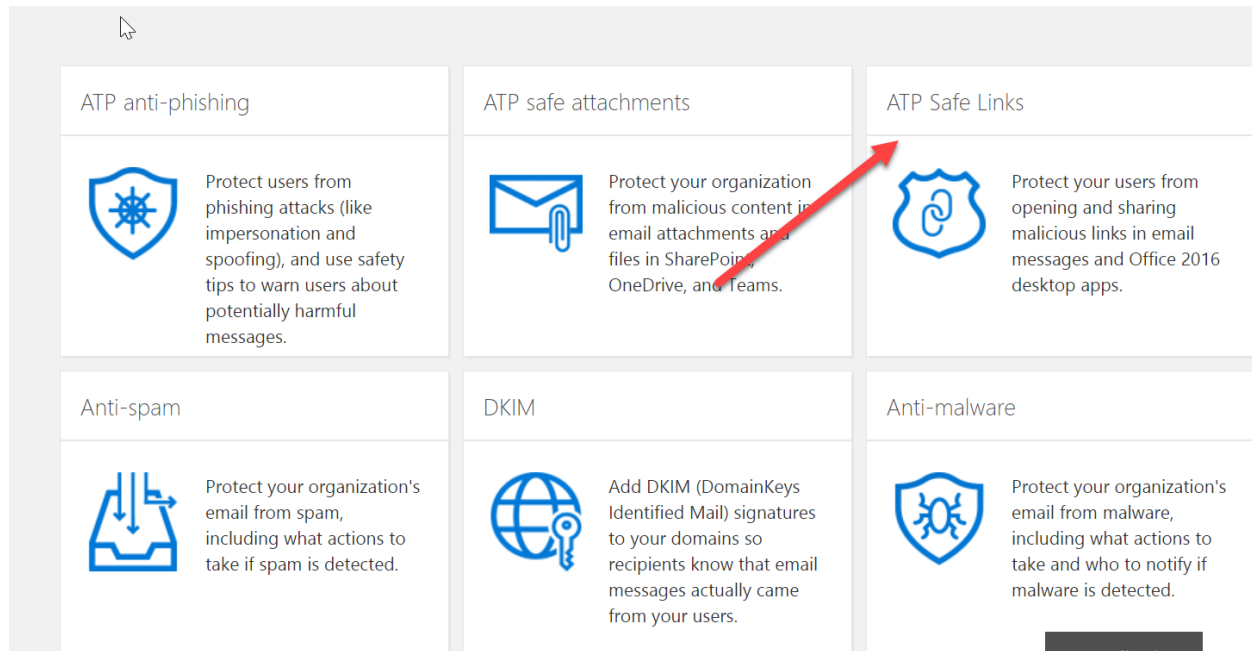
**Steps:**

1. In the Security and Compliance Center, go to Threat Management>Policy

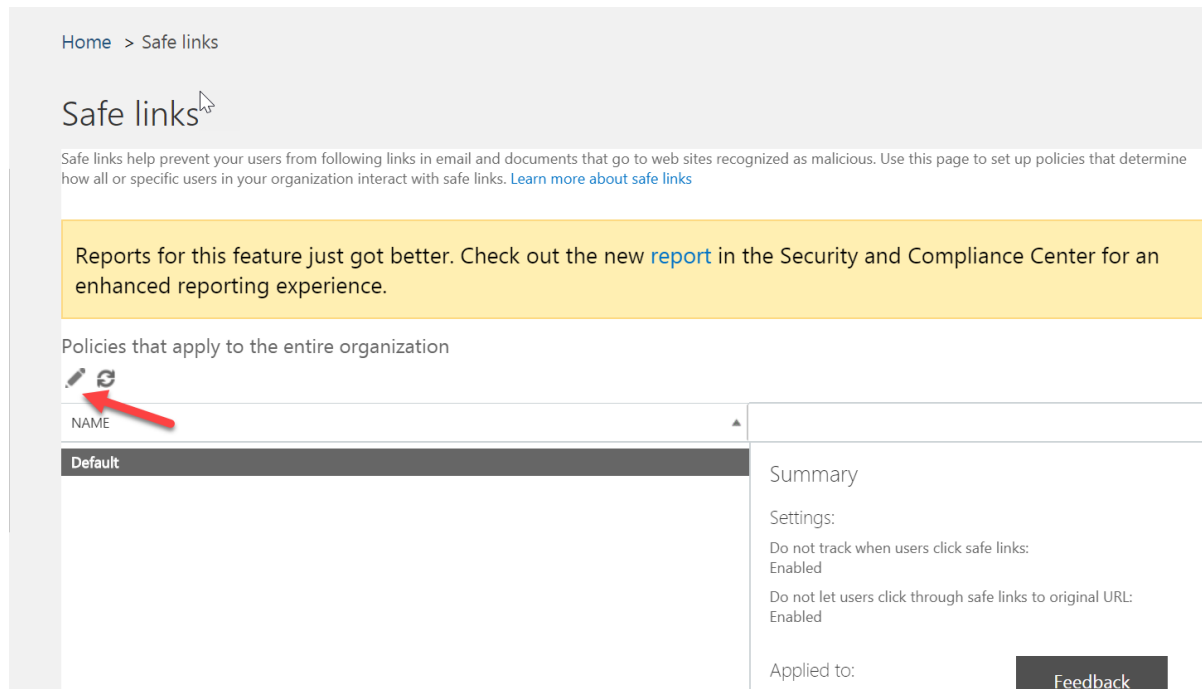




## 2. Click on the ATP Safe Attachments Icon



## 3. Here you can click on the Default Policy to see its settings. You will notice that by default, nothing is turned on:





## Safe links policy for your organization

### Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.

Block the following URLs:



### Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☐ Office 365 ProPlus, Office for iOS and Android

For the locations selected above:

- ☒ Do not track when users click safe links
- ☒ Do not let users click through safe links to original URL

#### Safe Links will be used in:

Office 365 ProPlus (Word, Excel, PowerPoint, and Visio on Windows; and Word, Excel, and PowerPoint on Mac)  
Office Online (Word Online, Excel Online, PowerPoint Online, and OneNote Online)  
Word, Excel, and PowerPoint for iOS and Android

#### Apps not currently supported:



OneNote (desktop version)  
Non Office 365 ProPlus products (such as Office 2016, Office 365 Home, Office 365 Personal, and the consumer version of Office Online)  
Office apps for iOS and Android not listed above


When a user clicks a URL in one of the supported apps, Office 365 will first



4. The first things we can do here is add an asterisk as a wildcard so that URLs start getting scanned for malicious content

Block the following URLs:



\*

These URLs will be blocked in email messages and in Office 365 ProPlus, Office Online, and Office for iOS and Android files.

You can use three wildcard asterisks (\*) per URL entered.

[Get help with this](#)

We can also checkmark the box for using Safe Links in Office 365 ProPlus and Office for IOS/Andriod

**Settings that apply to content except email**

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

☒ Office 365 ProPlus, Office for iOS and Android

For the locations selected above:








☒ Do not track when users click safe links

☒ Do not let users click through safe links to original URL



5. The other option is to scroll down and create a new safe link policy

Policies that apply to specific recipients

ENABLED	NAME	PRIORITY
There are no items to show in this view.		

0 selected of 0 total

Feedback

6. Here we can give a new name to the policy and I recommend checkmarking all of the fields but you can customize to fit your organizational needs:

new safe links policy

\*Name:

New Policy

Description:

Select the action for unknown potentially malicious URLs in messages.

☐ Off

☒ On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.

☒ Use safe attachments to scan downloadable content.

☒ Apply safe links to messages sent within the organization.

☒ Do not track when users click safe links.

☒ Do not let users click through safe links to original URL.

Do not allow users through to the orig from the warning p

7. Additionally you can whitelist certain URLs and define certain domain/groups/users to apply this policy to:



## new safe links policy

Do not rewrite the following URLs:



+

## Applied To

Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

\*If...

Select one ▼

add condition

Except if...

add exception



8. After you click save, you can see a summary on the right hand side:

Policies that apply to specific recipients

+ ✎ 🗑️ ⬆️ ⬇️ 📄 ⌵ ↺

ENABLED	NAME	PRIORITY
<input checked="" type="checkbox"/>	New Policy	0

Summary

Safe attachments URL Scanning:  
Enabled

Apply safe links to messages sent within the organization.  
Enabled


Do not track when users click safe links:  
Enabled

Do not let users click through safe links to original URL:  
Enabled

1 selected of 1 total

Feedback

9. After the policy is in place, the ATP Safe Links feature immediately checks the URL a user clicks on before opening the website. The URL is identified as blocked, malicious, or safe.



This link is being scanned.

We're scanning this link to see if it is malicious.

`www.unsafe_url/login.php`

We're scanning this link to see if it's malicious. The scan should be completed soon, so try opening the link in a few minutes.


[X Close this page](#)

[Continue anyway \(not recommended\)](#)

Powered by Office 365 Advanced Threat Protection



- If the URL is to a website that is included in the whitelisted URLs list for a policy that applies to the user, the website opens.
- If the URL is to a website that is included in the organization's custom blocked URLs list or a URL is to a website determined to be malicious, a warning page opens.



A link was clicked from a suspicious message.

This link was clicked from a message that has similarities to other suspicious messages.


We recommend that, before opening the website, go back and review the email message to determine the content of this email. Please be cautious when replying to the sender, even if it looks like someone you know.

[Tips for identifying phishing attacks](#)

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

[Learn more about Office 365 anti-phishing](#)



This link was clicked from a phishing message.

This link was clicked from a message that has been identified as a phishing attack.

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.


[Tips for identifying phishing attacks](#)

[X Close this page](#)

[Continue anyway \(not recommended\)](#)

[Learn more about Office 365 anti-phishing](#)





This website is classified as malicious.

Opening this website might not be safe.


`www.unsafe_url/login.php`

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

X Close this page

[Continue anyway \(not recommended\)](#)

Powered by Office 365 Advanced Threat Protection



This website was blocked by your Office 365 administrator.

Opening this website might not be safe.

`www.unsafe_url/login.php`

You can't access this website because it might not be safe. If you want to know why it was blocked, contact your administrator.

X Close this page

[Continue anyway \(not recommended\)](#)

Powered by Office 365 Advanced Threat Protection

- If the URL goes to a downloadable file and your organization's ATP Safe Links policies are configured to scan such content, the downloadable file is checked
- If the URL is determined to be safe, the website opens.

Implement Cloud App Security

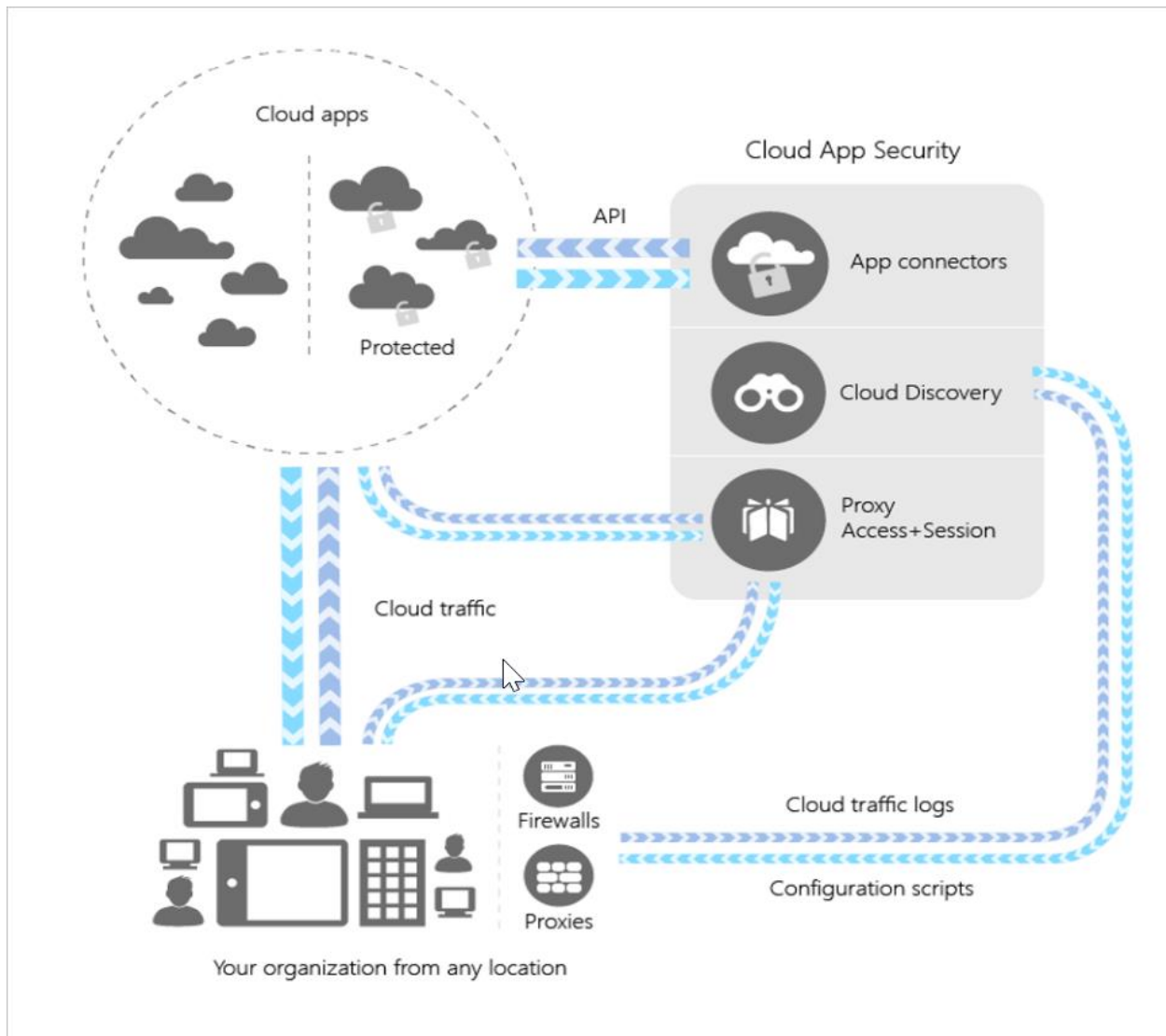


Cloud App Security is a critical component of the Microsoft Cloud Security stack. It's a comprehensive solution that can help your organization as you move to take full advantage of the promise of cloud applications, but keep you in control, through improved visibility into activity. It also helps increase the protection of critical data across cloud applications. With tools that help uncover shadow IT, assess risk, enforce policies, investigate activities, and stop threats, your organization can more safely move to the cloud while maintaining control of critical data.

**\*Licensing Considerations\***

Currently Cloud App Security comes with the following Plans:

- Office 365 E5
- EMS+E5
- Microsoft E3 and E5



#### Key Terms:

- **Cloud Discovery**-uses your traffic logs to dynamically discover and analyze the cloud apps that your organization is using. To create a snapshot report of your organization's cloud use, you can manually upload log files from your firewalls or proxies for analysis. To set up continuous reports, use Cloud App Security log collectors to periodically forward your logs.
- **Sanctioning and unsanctioning an app**- You can use Cloud App Security to sanction or unsanction apps in your organization by using the Cloud app catalog. The Microsoft team of



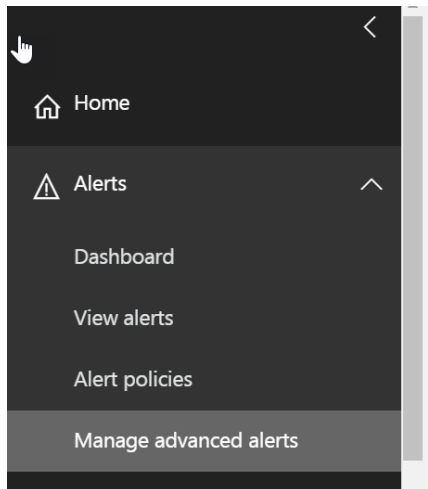
analysts has an extensive and continuously growing catalog of over 16,000 cloud apps that are ranked and scored based on industry standards. You can use the Cloud app catalog to rate the risk for your cloud apps based on regulatory certifications, industry standards, and best practices. Then, customize the scores and weights of various parameters to your organization's needs. Based on these scores, Cloud App Security lets you know how risky an app is based on over 70 risk factors that might affect your environment.

- **App Connectors-** use APIs from cloud app providers to integrate the Cloud App Security cloud with other cloud apps. App connectors extend control and protection. They also give you access to information directly from cloud apps, for Cloud App Security analysis.
- **Conditional Access App Control Protection-** utilizes reverse proxy architecture to give you the tools you need to have real-time visibility and control over access to and activities performed within your cloud environment. With Conditional Access App Control, you can protect your organization:
  - Avoid data leaks by blocking downloads before they happen
  - Set rules that force data stored in and downloaded from the cloud to be protected with encryption
  - Gain visibility into unprotected endpoints so you can monitor what's being done on unmanaged devices
  - Control access from non-corporate networks or risky IP addresses
- **Policy Control-** you can use policies to define your users' behavior in the cloud. Use policies to detect risky behavior, violations, or suspicious data points and activities in your cloud environment. If needed, you can use policies to integrate remediation processes to achieve complete risk mitigation.

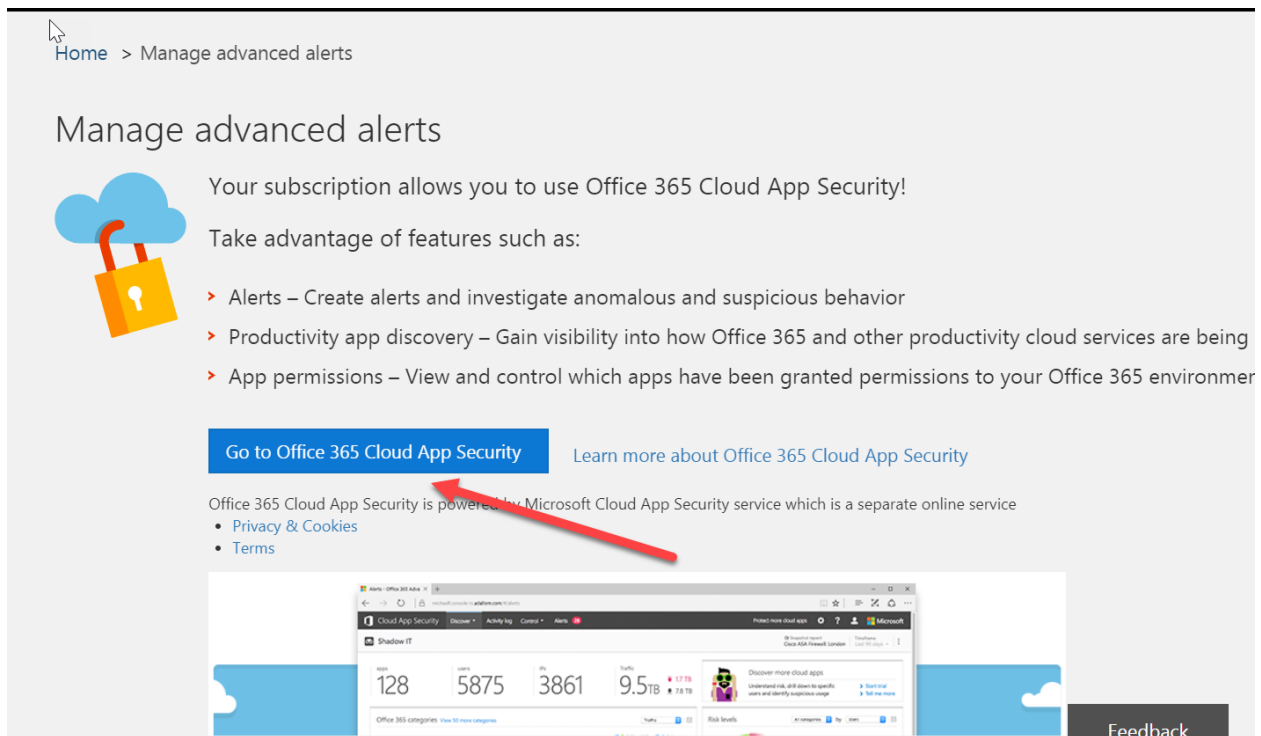


Steps:

1. Go to Security and Compliance Admin Center>Alerts>Manage Advanced Alerts

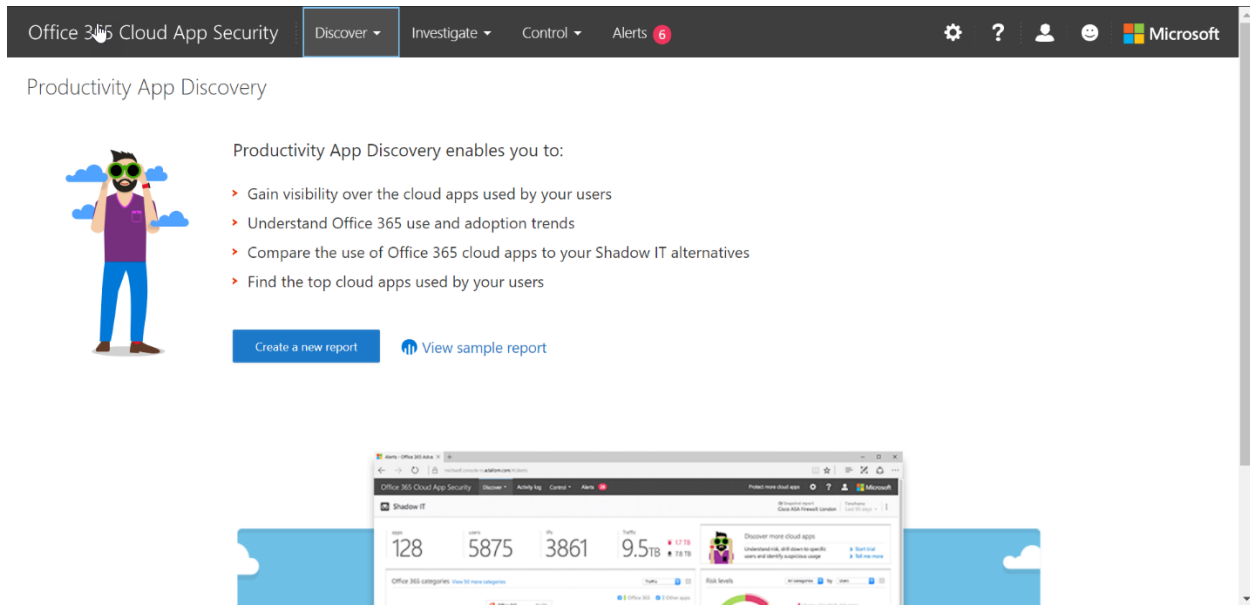


2. Click the link to enter the Cloud App Security Portal





3. From here we can go to Discover>Discovery Dashboard>Click Create New Report



4. Now we can add a log from our Firewall provider

Create new Productivity App Discovery snapshot report

Upload logs to discover cloud app activity and use.

Productivity App Discovery is powered by Microsoft Cloud App Security which is a separate online service. [Terms](#) | [Privacy statement](#)

#### Report name

#### Description

#### Data source

#### Choose traffic logs

1 GB maximum size per log, from the last 90 days

#### Report creation process

⌚ Analysis takes up to 24 hours | [Track status](#)

● Upload

■ Parse

■ Data analysis

● Generate report



[View sample report](#)

There is a list of providers from the dropdown. For the complete list, Follow [this link](#)



## Create new Productivity App Discovery snapshot report



Upload logs to discover cloud app activity and use.

**Barracuda**  
Barracuda - F-Series Firewall  
**Barracuda - F-Series Firewall Web Log Streaming**  
Barracuda - Web App Firewall (W3C)  
**Blue Coat**  
Blue Coat ProxySG - Access log (W3C)  
**Check Point**  
Check Point - Web App Firewall (W3C)  
Choose appliance...

Choose traffic logs

Choose up to 20 files

Browse

1 GB maximum size per log, from the last 90 days

Cancel

Create

### Report creation process

⌚ Analysis takes up to 24 hours | [Track status](#)

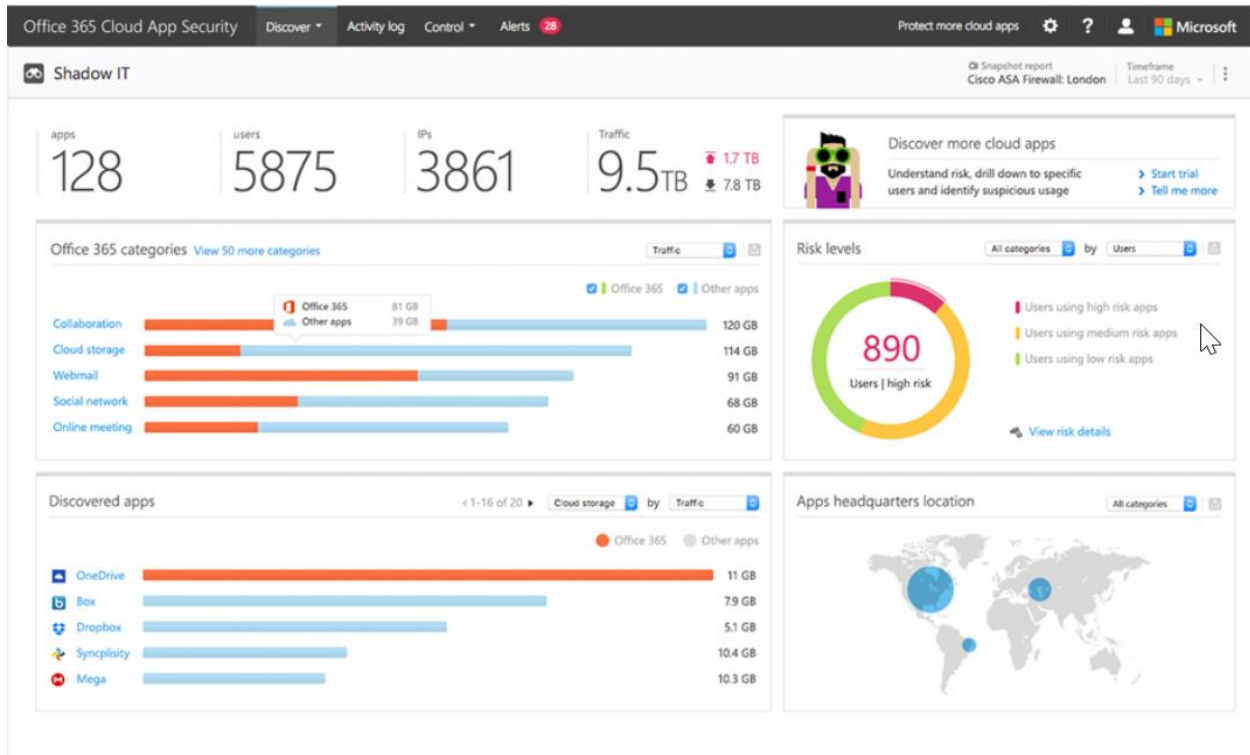
- Upload
- Parse
- Data analysis
- Generate report



[View sample report](#)



5. After the log is imported, your dashboard will contain info on discovered users, apps, IPs, and traffic



6. You can create new policies and customize them based on priority level

## Policies

NAME	TYPE	STATUS	SEVERITY	CATEGORY	Advanced		
Policy name...	Select type...	ACTIVE DISABLED		Select risk category...			

1 - 13 of 13 Policies							Create policy	
Policy	Count	Severity	Category	Action	Modified			
Multiple failed login attempts This policy profiles your environment and triggers alerts when us...	0 open alerts		Threat detection		Mar 28, 2018			
Activity from suspicious IP addresses This policy profiles your environment and triggers alerts when act...	0 open alerts		Threat detection		Mar 28, 2018			
Unusual impersonated activity (by user) This policy profiles your environment and triggers alerts when us...	0 open alerts		Threat detection		Mar 28, 2018			
...	...		...		...			



7. Additionally, you can see all of your apps in one location, including sanctioned and unsanctioned apps

**Cloud Discovery** Continuous report: Global Timeframe: Last 90 days

Dashboard | Discovered apps | IP addresses | Users Updated on Sep 15, 2016

518 all apps

22 sanctioned apps

20 unsanctioned apps

476 other apps

Filter by

Name

Activity timeframe

Risk factor

Score

Name	Traffic	Upload	Transactions	Score	Users	IP addresses	Last seen
Office 365 Collaboration	5.2 GB	838 MB	5K	6	668	595	Sep 15, 2016
Google Apps Admin Console Collaboration	66 KB	10 KB	126	5	120	86	Sep 15, 2016
Google Apps Collaboration	16 MB	3 MB	251	6	227	161	Sep 15, 2016
Google Docs Collaboration	24 MB	4 MB	247	7	225	162	Sep 15, 2016
Citrix Podio Collaboration	6 MB	1 MB	262	5	234	164	Sep 15, 2016
Syncplicity Collaboration	13 MB	5 MB	224	5	202	153	Sep 15, 2016
Atlassian Confluence Collaboration	83 KB	17 KB	204	7	192	132	Sep 15, 2016
Smartsheet	59 KB	7 KB	198	7	177	131	Sep 15, 2016

8. Lastly, alerts allow you to address security risk based off your policies

#### Alerts

**Alerts** Advanced

RESOLUTION STATUS: OPEN | DISMISSED | RESOLVED

CATEGORY: Select risk category...

SEVERITY: Low Medium High

APP: Select apps...

USER NAME: Select users...

POLICY: Select policy...

1 - 6 of 6 alerts

Alert	App	Resolution	Severity	Date
Activity from infrequent country Q RO	Office 365	OPEN	Medium	16 days ago
Activity from infrequent country Q RO	Microsoft ...	OPEN	Medium	17 days ago
System alert: Mail server is changing	Microsoft ...	OPEN	High	18 days ago
Activity from infrequent country Q US	Microsoft ...	OPEN	Medium	23 days ago



## Exchange Online Protection/Antispam Policies

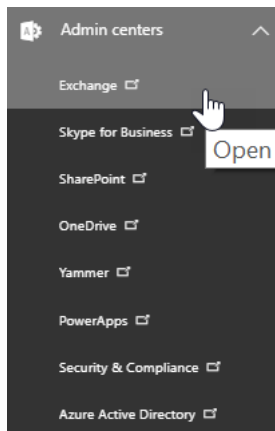
Checklist:

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	<div>Default</div> <div>Enabled</div> <div>Relative priority: Lowest</div> <div>Summary</div> <div>Malware detection response: Don't notify recipients</div> <div>Sender notifications: None</div> <div>Administrator notifications: None</div> <div>Customized notification text: Not configured</div>

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

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



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

The screenshot shows the 'edit spam filter policy' window in Google Chrome. The browser address bar shows the URL: <https://outlook.office365.com/ecp/Antispam/EditConnectionFilter.aspx?ActivityCorrelationID=1a54189a-8fef-a56a-9608-b93674b54078&reqId=152837213725...>. The page title is 'edit spam filter policy - Google Chrome'. The main content area is titled 'Default' and has a sidebar with 'general' and 'connection filtering' (selected). The 'connection filtering' section has two sub-sections: 'IP Allow list' and 'IP Block list'. The 'IP Allow list' section has a heading 'Always accept messages from the following IP addresses.' and a table with one column 'Allowed IP Address'. The 'IP Block list' section has a heading 'Always block messages from the following IP addresses.' and a table with one column 'Blocked IP Address'. There are '+', '-', and edit icons for each list. At the bottom, there is a checkbox 'Enable safe list' and 'Save' and 'Cancel' buttons.

## Spam Filtering:

### Questions to Ask:

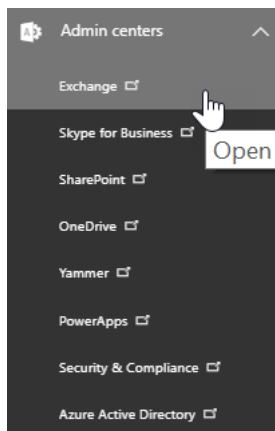
1. What actions do we want to take when a message is identified as spam?
  - a. Move Message to Junk Folder (Default)
  - b. Add X Header (Sends the message to the specified recipients, but adds X-header text to the message header to identify it as spam)
  - c. Prepend Subject line with text (Sends the 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

Default

Enabled

Relative priority: Lowest

Summary

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

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

### 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

98



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:

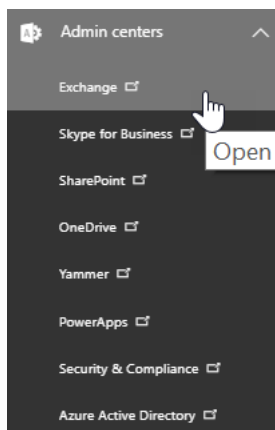
1. Do I want to receive notifications when someone is flagged for sending outbound spam?
  - This is a check to make sure users don't send spam
  - Can turn on settings to send copies/notifications of all suspicious outbound mail to certain email address
  - Refer to "[Set Up Outbound Spam Notifications](#)"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

dashboard rules message trace accepted domains remote domains connectors

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

hybrid

+ - ✎ 📧 🗑️ ⬆️ ⬇️ 📅 🔍 ↺

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

dashboard rules message trace accepted domains remote domains connectors

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

hybrid

+ - ✎ 📧 🗑️ ⬆️ ⬇️ 📅 🔍 ↺

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...

		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](#)

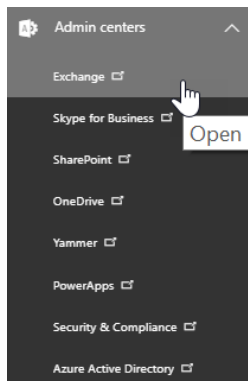
Save

Cancel

## 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

Default

Enabled

Relative priority: Lowest

Summary

Malware detection response:  
Don't notify recipients

Sender notifications:  
None

Administrator notifications:  
None

Customized notification text:  
Not configured



### 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

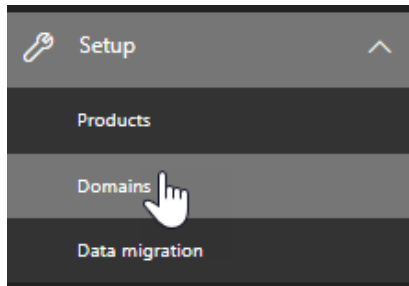
Save

Cancel

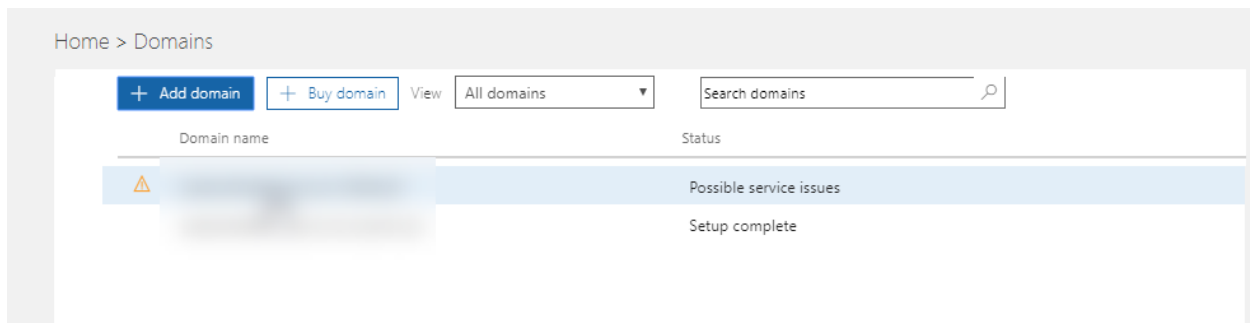
## DNS Settings

- 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 to the following values.  
You can also download or import a DNS file.

[Export options](#)

^ Exchange Online

Type	Priority	Host name	Points to address or value	TTL
MX	0	rosebudhealthcare-com.mail.protection.outlook.com		1 Hour
TXT	-	v=spf1 include:spf.protection.outlook.com -all		1 Hour
CNAME	-	autodiscover.outlook.com		1 Hour

^ Skype for Business

Type	Points to address or value	TTL
CNAME	skypeforbusiness.rosebudhealthcare-com	1 Hour
CNAME	skypeforbusiness.rosebudhealthcare-com	1 Hour

^ Mobile Device Management for Office 365

Type	Priority	Host name	Points to address or value	TTL
SRV	-	_sip	sipdir.online.lync.com	1 Hour
SRV	-	_sipfederationtls	sipfed.online.lync.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:**

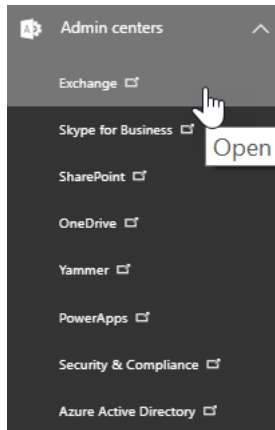
```
Host Name: selector1._domainkey. tminus365.com
Points to address or value: selector1-pax8-com._domainkey. tminus365.onmicrosoft.com
TTL: 3600
```

#### **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
		Authoritative

Sign messages for this domain with DKIM signatures: Disabled  
[Enable](#)

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

CNAME record does not exist for this config. Please publish the following two CNAME records first: selector1-  
\_domainkey.██████████.onmicrosoft.com selector2-r-  
com.\_domainkey.██████████.onmicrosoft.com

Sign messages for this domain with DKIM signatures: Disabled  
[Enable](#)

Status:  
Not signing DKIM signatures for this domain.

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



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"`