



Welcome to the “New features to help secure external collaboration using MIP” Webinar

We will start at 2-3 minutes after the scheduled time to accommodate those still connecting.

Questions? Feel free to type them in the instant message window at any time. Note that any questions you post will be **public**. You have the option to post questions anonymously.

This webinar is being **recorded** and is available later for viewing using the same event link.

Join our Community: <https://www.yammer.com/askipteam/>



M365
SECURITY,
COMPLIANCE &
MANAGEMENT

New features to help secure external collaboration using MIP

Samson Chan –Program Manager, Microsoft Information Protection

Adam Bell – Program Manager, Microsoft Information Protection Customer Acceleration Team (CAT)



Today's Agenda

- Overview MIP Ecosystem
- Protection sharing options
- SharePoint Online
 - External Sharing flow
 - Default Sharing Link
 - Sensitive by Default
- Email
 - Email sharing flow
 - Best practices



Microsoft Information Protection (MIP)

Key customer benefits



BUILT-IN

Built-in labeling and protection experience in Microsoft 365 apps, Microsoft 365 services, other MS services like Power BI, Edge and Windows



INTELLIGENT

Accuracy in classification via ML based trainable classifiers and exact data match



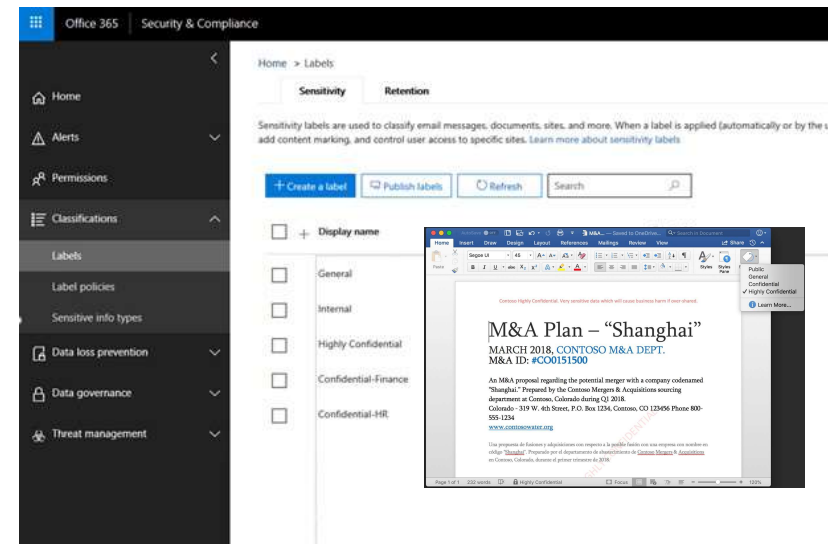
UNIFIED

Single admin console to configure and manage your policies and view analytics across on-premises, Microsoft 365 apps, Microsoft 365 services, 3rd party services and Windows devices



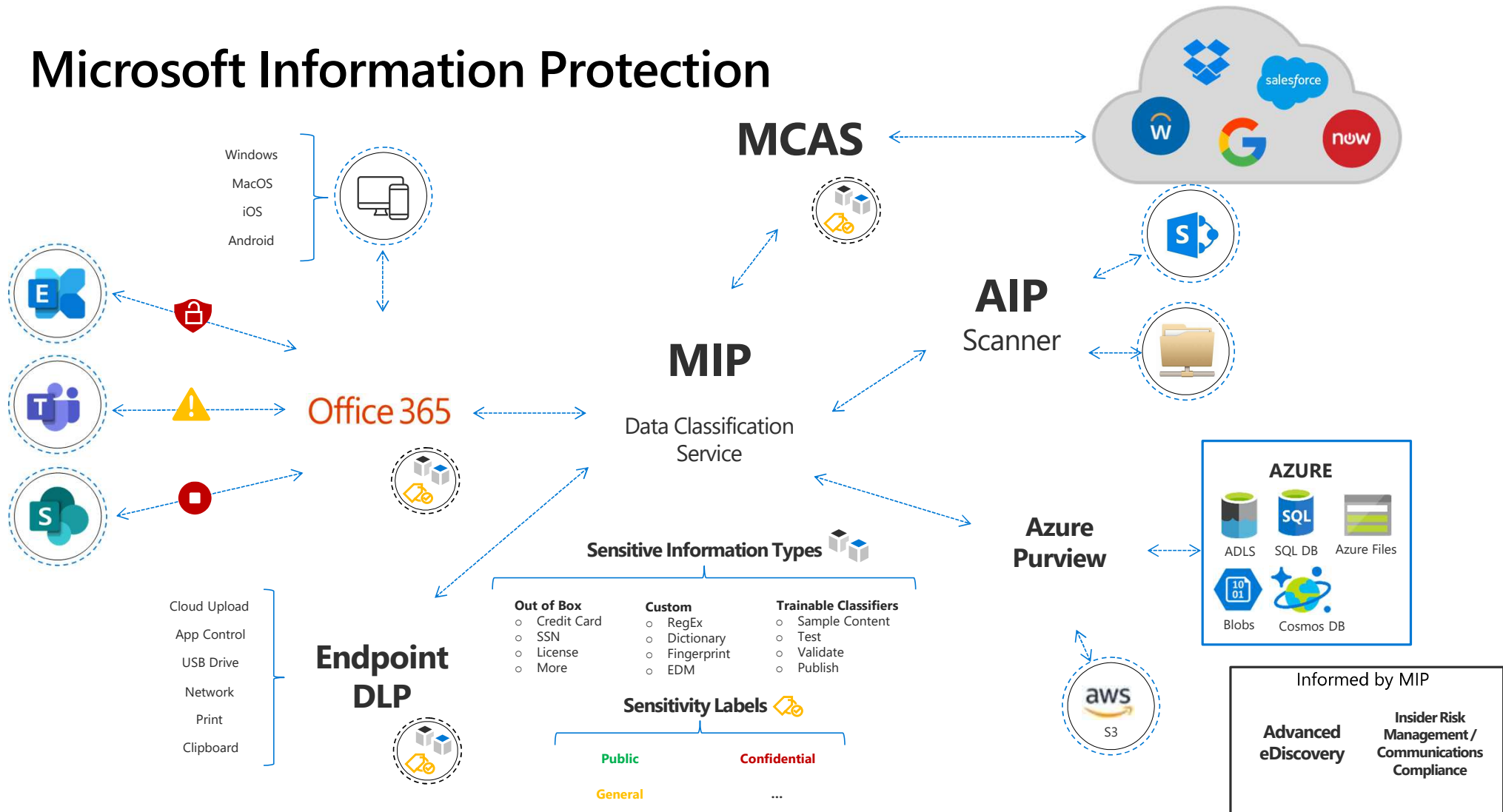
EXTENSIBLE

MIP platform extends the protection experience, in a consistent way, to popular non-Microsoft apps and services

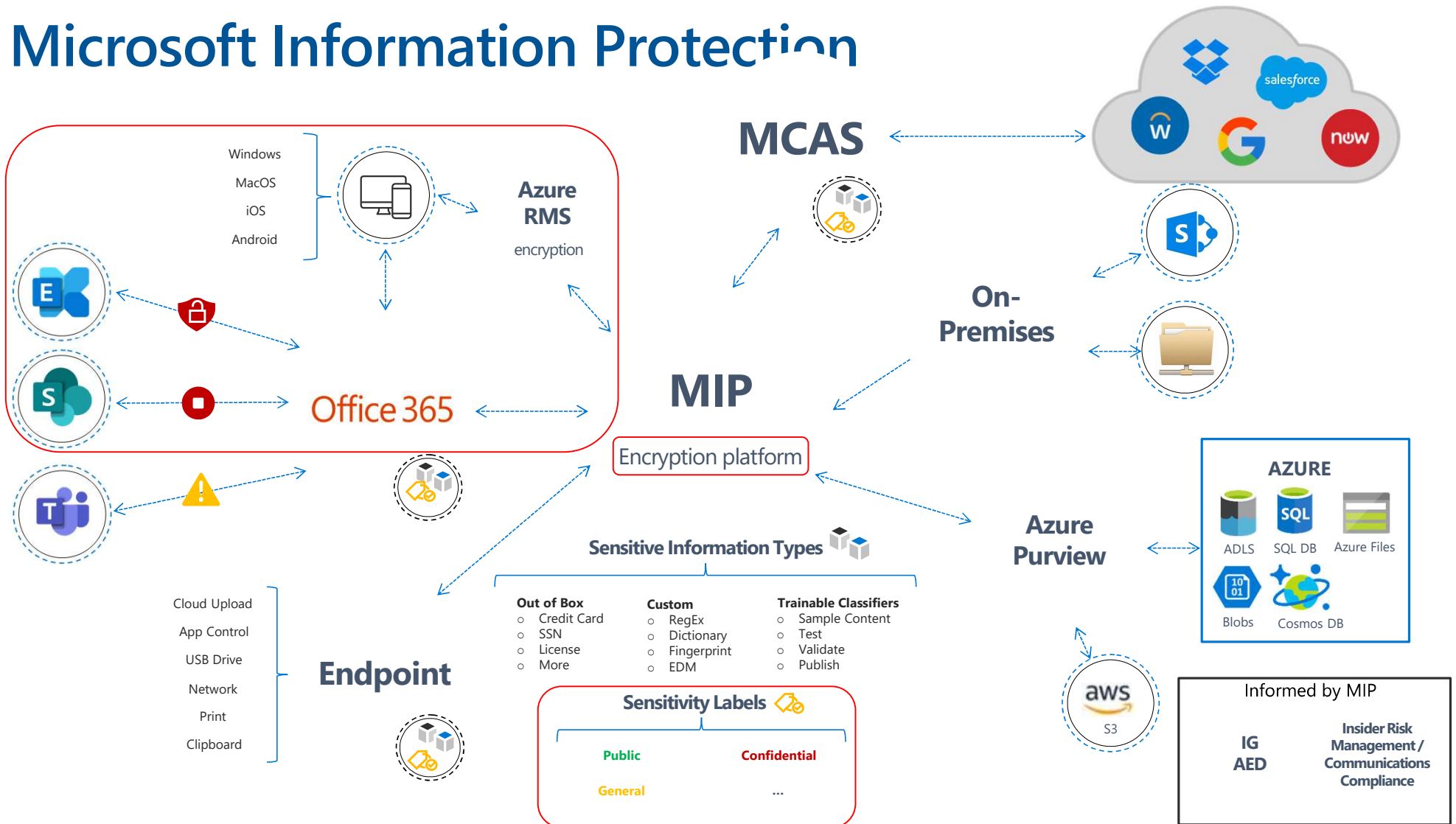


Microsoft Information Protection is a **built-in, intelligent, unified** and **extensible** platform and solution to protect sensitive data.

Microsoft Information Protection



Microsoft Information Protection





Sensitivity Labels are the foundation

1. All built on top of labels – these features are driven by label actions
2. It provides the capability to control access wherever the file travels
3. Balance of security versus collaboration



External Collaboration: Requires two parts

1. How do you get the file to the recipient?



2. How does the recipient work with the protected content?

Recipient Identity - Software used to consume - Permissions



Recap on usage rights

- **Admin-Defined Permission** - *Assign permissions now*
 - Admins define a list of users with usage rights (in a label)
 - 4 default logical groupings of usage rights are provided to simplify label creation (Viewer, Reviewer, Co-Author, Co-owner)
 - Admins can also customize/choose from the list of usage rights for different users
- **User-Defined Permission (UDP)** - *Let users assign*
 - User inputs a list of users in the application
 - UDP labels have fixed usage rights and only the user who applied the label can can change/remove label
 - Do Not Forward/Encrypt-only are built-in UDP (label) protection in Outlook and Exchange
 - Prompt User are built-in UDP (label) protection in Word, Excel, and PowerPoint

Encryption

Control who can access files and email messages that have this label applied.

☐ Remove encryption if the file is encrypted

☒ Configure encryption settings

① Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. reasons, performance will be slow when the files are opened or saved, and some SharePoint and [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

Assign permissions now

Let users assign permissions when they apply the label



External Collaboration: Options with protected content

1. Sharing with SharePoint Online
 - “Today” this is only available for Admin-Defined permissions

2. Sharing with email
 - Available for Admin-Defined permissions and UDP



Sharing with SharePoint Online

Integration with AAD B2B

Default sharing link

Sensitive by default



SPO: External Sharing

Sharing

Use these settings to control sharing at the organization level in SharePoint and OneDrive. [Learn more](#)

External sharing

Content can be shared with:

SharePoint

OneDrive

<div><div></div><div>Most permissive</div></div>	<div><div></div><div>Anyone</div><div>Users can share files and folders using links that don't require sign-in.</div></div>
	<div><div></div><div>New and existing guests</div><div>Guests must sign in or provide a verification code.</div></div>
	<div><div></div><div>Existing guests</div><div>Only guests already in your organization's directory.</div></div>
<div><div></div><div>Least permissive</div></div>	<div><div></div><div>Only people in your organization</div><div>No external sharing allowed.</div></div>

You can further restrict sharing for each individual site and OneDrive. [Learn how](#)

More external sharing settings

Container label properties

Define external sharing and device access settings

Control who can share SharePoint content with people outside your organization and decide whether users can access labeled sites from unmanaged devices.

- ☒ **Control external sharing from labeled SharePoint sites**
When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site.

Content can be shared with

☐ Anyone

Users can share files and folders using links that don't require sign-in.

☒ New and existing guests

Guests must sign in or provide a verification code.

☐ Existing guests

Only guests in your organization's directory.

☐ Only people in your organization

No external sharing allowed.

- ☐ **Use Azure AD Conditional Access to protect labeled SharePoint sites**
You can either control the level of access users have from unmanaged devices or select an existing authentication context to enforce restrictions.

SPO: External Sharing flow

Documents

Documents

Name	Modified
Created inside SPO.docx	
Lorem - External 2.docx	
Protected outside - uploaded to SPO.docx	

Share



Documents

Send link

People in MIPDemo with the link can edit >

To: Name, group or email

Message...

Send

Copy link Outlook



Documents

Documents

Name
Created inside SPO.docx
Lorem - External 2.docx
Protected outside - uploaded to SPO.docx

Link settings

Who would you like this link to work for?

[Learn more](#)

- Anyone with the link
- People in MIPDemo with the link
- People with existing access
- Specific people

Other settings

- Allow editing
- Open in review mode only
- Block download

Apply

Cancel



SPO: External Sharing – integration with AAD B2B

SharePoint and OneDrive integration with Azure AD B2B

08/27/2021 • 3 minutes to read • 

This article describes how to enable Microsoft SharePoint and Microsoft OneDrive integration with Azure AD B2B.

Azure AD B2B provides authentication and management of guests. Authentication happens via one-time passcode when they don't already have a work or school account or a Microsoft account.

With SharePoint and OneDrive integration with Azure B2B Invitation Manager enabled, Azure B2B Invitation Manager can be used for sharing of files, folders, list items, document libraries and sites with people outside your organization. This feature provides an upgraded experience from the existing secure external sharing recipient experience. Additionally, Azure B2B Invitation Manager one-time passcode feature allows users who do not have existing Work or School accounts or Microsoft Accounts to not have to create accounts in order to authenticate, but can instead use the one time passcode to verify their identity.

Enabling this integration does not change your sharing settings. For example, if you have site collections where external sharing is turned off, it will remain off.

Once the integration is enabled you and your users do not have to reshare or do any manual migration for guests previously shared with. Instead, when someone outside your organization clicks on a link that was created before Azure AD B2B integration was enabled, SharePoint will automatically create a B2B guest account. This guest account is created on behalf of the user who originally created the sharing link. (If the user who created the link is no longer in the organization or no longer has permission to share, the guest will not be added to the directory and the file will need to be reshared.)

SharePoint and OneDrive integration with the Azure AD B2B one-time passcode feature is currently not enabled by default. Later, this feature will replace the ad-hoc external sharing experience used in OneDrive and SharePoint today.

Advantages of Azure AD B2B include:

- Invited people outside your organization are each given an account in the directory and are subject to Azure AD access policies such as multi-factor authentication.
- Invitations to a SharePoint site use Azure AD B2B and no longer require users to have or create a Microsoft account.
- If you have configured Google federation in Azure AD, federated users can now access SharePoint and OneDrive resources that you have shared with them.
- SharePoint and OneDrive sharing is subject to the Azure AD organizational relationships settings, such as **Members can invite** and **Guests can invite**. As with Microsoft 365 Groups and Teams, if an Azure AD organizational relationship setting is more restrictive than a SharePoint or OneDrive setting, the Azure AD setting will prevail.

<https://docs.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration>



SPO: External Sharing – enabling the integration with AAD B2B

- Pre-requisite:
 - your organization needs to have Azure AD email one-time passcode authentication enabled.

1. Use the SharePoint Online Management Shell and run the following commands:

PowerShell

```
Set-SPOTenant -EnableAzureADB2BIntegration $true  
Set-SPOTenant -SyncAadB2BManagementPolicy $true
```

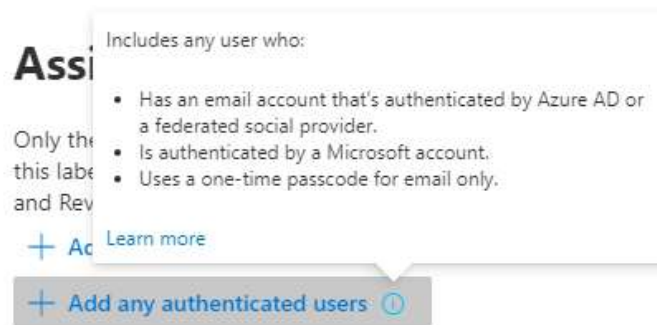
<https://docs.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration>



SPO: External Sharing – M365 dynamic groups Vs. “any auth user”

- What if I don't know who I'll be sharing with when configuring the admin-defined permissions?
 - Manually add guest accounts to the group used for Admin-Defined permissions
 - Use “any authenticated user” right (USE WITH CAUTION)
 - Use M365 Dynamic Groups

From the Assign Permissions blade when configuring permissions on the label:





SPO: External Sharing – M365 dynamic groups Vs. “any auth user”

Dynamic group example:

External Guest Access | Dynamic membership rules

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Administrative units

Group memberships

Applications

Save Discard Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	userType	Equals	Guest

+ Add expression

+ Get custom extension properties

Rule syntax

{user.userType -eq "Guest"}

SPO: Default sharing link

Approach of least privilege:

Use PowerShell to set the below to a container label of your choice.

- 1) Open PowerShell
- 2) `$UserCredential = Get-Credential`
- 3) `$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.compliance.protection.outlook.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection`
- 4) `Import-PSSession $Session -DisableNameChecking`
- 5) `Get-Label | Format-Table -Property DisplayName, Name, Guid`

This shows you all the labels from the tenant. Now for a given label → Say "Confidential – External Sharing" you can do like this:

```
Set-Label -Identity 'External Sharing' -AdvancedSettings @{DefaultSharingScope = "SpecificPeople"}  
Set-Label -Identity 'External Sharing' -AdvancedSettings @{DefaultShareLinkPermission = "Edit"}
```

Send link

 People you specify can edit >

To: Name, group or email

Message...

Send



Copy link



Outlook



SPO: Sensitive by default

Mark new files as sensitive by default

08/27/2021 • 2 minutes to read •  +5

When new files are added to SharePoint or OneDrive in Microsoft 365, it takes a while for them to be crawled and indexed. It takes additional time for the [Office Data Loss Prevention \(DLP\) policy](#) to scan the content and apply rules to help protect sensitive content. If external sharing is turned on, sensitive content could be shared and accessed by guests before the Office DLP rule finishes processing.

Instead of turning off external sharing entirely, you can address this issue by using a PowerShell cmdlet to block external access to new content unless it's explicitly authorized in a DLP rule and it has been verified that there's no sensitive content that goes against the policy rules. The setting enabled by this cmdlet prevents external users from accessing newly added files until at least one Office DLP policy scans the content and determines that the document doesn't contain any sensitive information that's against the rules defined in the policy. If the file has been indexed and scanned and it has no sensitive content that's against the rules in the DLP policy, then guests can access the file. If the policy identifies sensitive content in the document, or if there's no DLP rule explicitly authorizing access to the file, then guests will not be able to access the file, and they will receive the following access denied error message: "This file is being scanned right now. Please try again in a few minutes. If you still don't have access, contact the file owner."

Note

This cmdlet applies to newly added files in all SharePoint sites and OneDrive accounts. It doesn't block sharing if an existing file is changed.

<https://aka.ms/MIPC/sensitivebydefault>



Sensitive by default

- Use the SharePoint Online Management Shell
 - Enable:
 - Set-SPOTenant -MarkNewFilesSensitiveByDefault BlockExternalSharing
 - Disable
 - Set-SPOTenant -MarkNewFilesSensitiveByDefault AllowExternalSharing



Best practice

- Do you know who content will be shared with?
- Static groups for MIP permissions = best experience
- Balance collaboration with security posture when considering “any authenticated user
- When using M365 dynamic groups factor in the “1st time experience” and test end to end



Sharing with Email

Encryption ecosystem across MIP, DLP, and OME

Document attachment improvements in the OME portal

Encryption flow improvements through Exchange Online

Encryption across ecosystem

- ***Different MIP solutions use the same underlying encryption technology to control access on documents and email***

New sensitivity label

Name:

*Apply this rule if...
Select one
add condition

*Do the following...
Apply Office 365 Message Encryption
add action

Except if...
add exception

Properties of this rule:
☒ Audit this rule with severity level:
Not specified ▼

Choose protection settings for files and emails

Configure encryption and content marking settings to protect labeled emails and Office files. Also define auto-labeling conditions to automatically apply this label to sensitive content in Office, files in Azure, and more.

☒ **Encrypt files and emails**
Control who can access files and emails that have this label applied.

☐ **Mark the content of files**
Add custom headers, footers, and watermarks to files and emails that have this label applied.

Create rule

Exceptions
We won't apply this rule to content that matches any of these exceptions.
+ Add exception ▼

Actions
Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

☒ **Restrict access or encrypt the content in Microsoft 365 locations**

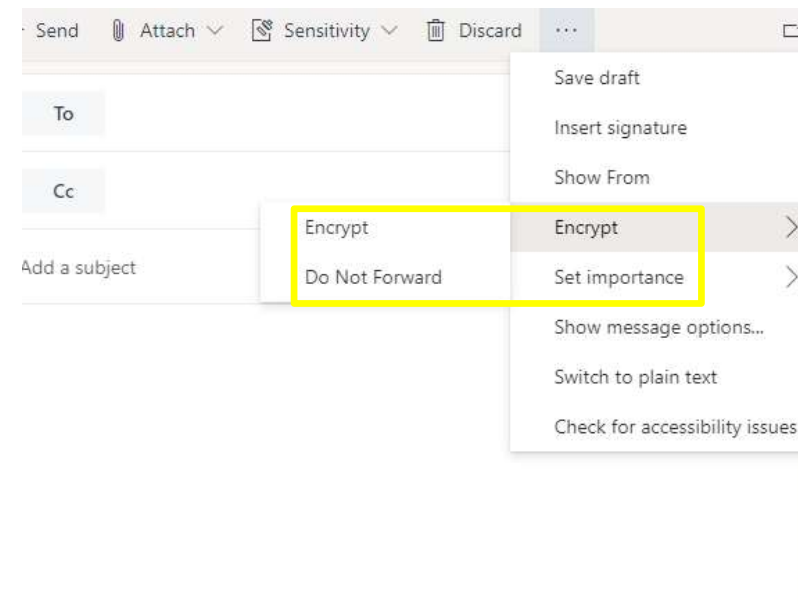
☐ Block users from accessing shared SharePoint, OneDrive, and Teams content

☒ Encrypt email messages (applies only to content in Exchange)
Encrypt ▼

+ Add an action ▼

OME & AME

- **Office 365 Message Encryption (OME) & Office 365 Advanced Message Encryption (AME) is the underlying solution that provides a consistent consumption experience across all the different MIP solutions that applies encryption to mail and document attachments**
- **OME offers fundamental functionality across all MIP encrypted mail**
 - Zero setup with built-in encryption (Do Not Forward and encrypt-only) to Outlook clients and other MIP solutions to create encrypted mail to any recipients
 - An OME portal to store all encrypted mail for (non-M365) external recipients
 - A single default OME branding configuration for customizing the notification mail and OME portal
- **AME offers additional functionality across all MIP encrypted mail**
 - Creation of custom OME branding configurations to apply based on your intended audience
 - OME branding configurations with expiration on access to mail stored in OME portal
 - Admin and end-user revocation to mail stored in OME portal



Using UDP for external collaboration with email

- **UDP provides the flexibility for users in your organizations to protect documents and emails to specific audiences on-demand**
- **Use *Encrypt-Only* protection to give permissions to recipients in the mail conversation to extend collaboration and communication with other relevant people**
- **Use *OME portal* to provide a consistent experience to external users to consume encrypted messages and any encrypted documents, even for non-M365 users**

Encryption

Control who can access files and email messages that have this label applied. [Learn more about encryption settings](#)

☐ Remove encryption if the file or email is encrypted

☒ Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Let users assign permissions when they apply the label

ⓘ The labeling behavior for these settings varies depending on which operating system platform is used to apply the label. [Learn more](#)

☒ In Outlook, enforce one of the following restrictions

☐ Do Not Forward ⓘ

☒ Encrypt-Only ⓘ

☒ In Word, PowerPoint, and Excel, prompt users to specify permissions ⓘ

☐ Use Double Key Encryption ⓘ

Encryption removal and external collaboration

- There are situations when there is a need to use a 3rd party solution that cannot reason/respond over encrypted mail conversations but need to transmit sensitive content with protection
- OME allows admins to create mail flow rules to apply or remove encryption as appropriate on outgoing mail
- Mail flow rules can also remove encryption on mail replies

Support inquiries

Name:

Support inquiries

*Apply this rule if..

✕ The sender is located...

[Outside the organization](#)

and

✕ The recipient is located...

[Inside the organization](#)

and

✕ The recipient is...

[*Select people...](#)

add condition

*Do the following..

Remove Office 365 Message Encryption applied by the organization

add action

Except if..

add exception

Properties of this rule:

Priority:

4

☒ Audit this rule with severity level:

Best practice and guidance

- *For customer facing communication and document sharing, it would be appropriate to send secure email and apply OME branding templates to ensure all external recipients retrieve mail from OME portal*
- *Automated system such as customer support or payroll would benefit from using OME and setup mail flow rule to encrypt/unencrypt mail*
- *3rd party journaling solution that cannot reason over encrypted mail can use OME to generate a compatible mail for storage by leveraging mail flow rules to remove the encryption from a bcc copy*



Resources

- One-Stop-Shop – <https://aka.ms/MIPC/OSS>
 - Webinars – <https://aka.ms/MIPC/Webinars>
 - Previews – <https://aka.ms/MIPC/Previews>
- Scenario Based Demo's video series – <https://aka.ms/MIPC/SBD>
- SharePoint - <https://aka.ms/MIPC/ExternalCollab>
- SharePoint & AAD B2B - <https://docs.microsoft.com/en-us/sharepoint/sharepoint-azureb2b-integration>
- AAD - <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/o365-external-user>