Webinar FAQ: New features to help secure external collaboration using Microsoft Information Protection (MIP)

Prepared by:
Microsoft 365 Security & Compliance Team, September 28, 2021

1. **View** the Microsoft Information Protection documentation for additional information: Microsoft Information Protection in Microsoft 365 - Microsoft 365 Compliance | Microsoft Docs
2. **Sign up** for the MIP Preview Program: https://aka.ms/MIP-Preview
3. **Follow** us on twitter: twitter.com/MIPnews
4. **Watch** previous webinars: http://aka.ms/MIPC/webinars

Features & Capabilities

Q: What is the best practice to share a confidential protected document with Customer domain?

A: Here are a few proposals:

- *Add your guest users to AAD via AAD admin flow or sending guest invitation flow and then share the files with these guest users using SharePoint guest flow.*
- *If you want to keep the documents in Cloud, then you can prevent download.*
- *For business reasons, if the documents need to be downloaded, use MIP Sensitivity labels for office files and use encryption that covers your guest users as well.*

Q: Can you explain any limitations with sharing information with customers without a Microsoft 365 tenant?

A: Customers without a M365 tenant can still consume protected content. In the case of protected emails there are no significant limitations, as OME will allow them to consume the content in a web interface and sign in with whatever email address they have. In the case of protected documents, they will be able to consume the protected content in Office, but they will have to sign in with a Microsoft account associated with their email address, or if using an old version of Office using RMS for individuals (though in that case you will have to send them instructions to do that). The primary limitation in this case is that the recipient will have to use Office (and not other

applications which may be able to consume Office documents but not protected documents). Also keep in mind that if there are any constraints in the access such as Conditional Access policies configured in the source tenant, they will have to be provisioned a guest account in the source tenant as per the requirements of those constraints. But a guest account is not required unless such special access constraint is defined in the source tenant for access to protected content.

Q: What is best practice for sharing PDFs externally?
A: OME supports encryption of PDF as email attachments. Organizations can enable PDF encryption using the Exchange Online PowerShell Set-IRMConfiguration cmdlet. This setting applies to autolabeling, DLP policy, and mail flow rule. Not all Outlook clients support PDF encryption. Please refer to https://aka.ms/omefaq for details. For consumer facing situations, use a mail flow rule to enforce a linked based experience to help the recipients view the PDF in the OME portal in a web browser without the need to download any additional PDF viewing applications.

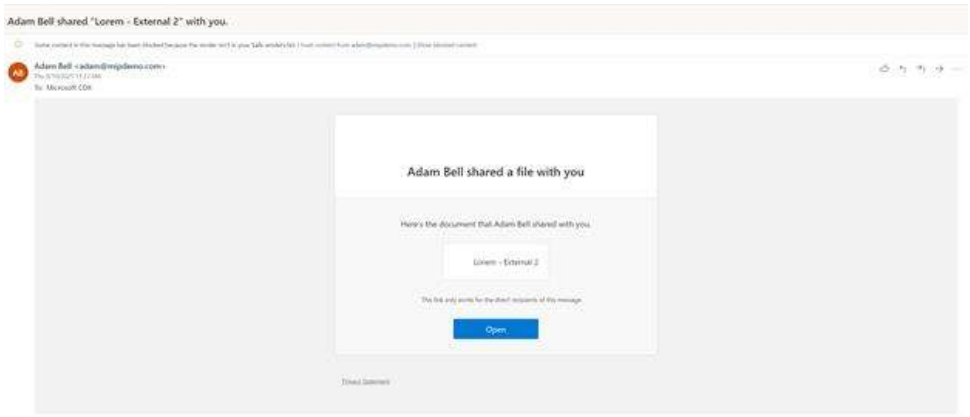
Q: Is there any guidance on interoperability between GCCH and Commercial clouds? Like how to label and send emails or files from a commercial cloud, for consumption by users on GCCH?
A: Cross-cloud collab is a known gap. A .gov customer will have their identity in GCCH and cannot auth into a commercial tenant. Will work for OME through a one-time passcode but not "seamlessly" as with other commercial tenants. Absolutely will not work for SharePoint without creating a guest user out of this .gov email address.

Q: Mark sensitive by default is enabled at the tenant level but does it need to be enabled at the site level also?
A: No this is one time setting for the entire tenant.

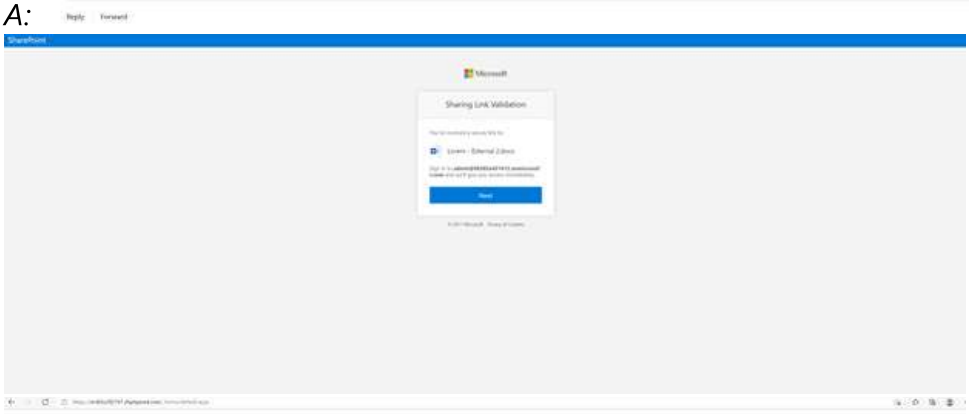
Q: If you are using Sensitive by Default, what if a guest user creates a document? He will not have access to his own created document. How do we solve that?
A: He will still have access to the document. It prevents external users from accessing newly added files.

Q: What is the main use case for M365 dynamic groups? (Can it replace any authenticated users?)
A: M365 dynamic groups are typically used when access needs to be granted based on Azure AD properties of the recipient, or when access needs to be granted based on combinations of memberships such as "member of project team A, and of nationalities B or C, but not under restricted group C". These scenarios are common in highly regulated environments.

Q: Do you have a more detailed description of the first-time experience for guests and permission via dynamic group?



A:



Q: Do you have a document for initial use and configuration with MIP?

A: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Q: Does sensitive by default work with existing documents created before setting?

A: This is only for newly created files.

Q: The labels applied on SharePoint are at the container level and the documents will not inherit this label?

*A: Currently, container labels are more so about the sharing side. For this container-level classification and protection, use the following label settings:
Privacy (public or private) of teams sites and Microsoft 365 groups
External user access
External sharing from SharePoint sites
Access from unmanaged devices
Authentication contexts (in*

*preview)
* [*https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide*](https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide)

Q: How does Azure Information Protection relate to OME & AME?

A: OME and AME encryption is based on the core encryption used by MIP and AIP, and emails protected with MIP and AIP will be encrypted using OME/AME. What is special about OME and AME is that on top of the regular encrypted format they add a "wrapper" so users with an email client that's unable to consume the protected content directly can view the email and any attachments in a web viewer and authenticate with other additional such as a Gmail account or a one-time passcode. This option still uses the same encryption and protection methods in the main protected email, only that this is all handled by the web service that provides the UI so no setup is required on the client side.

Q: We use EXO rules to apply Encrypt to outgoing email based on a label... how and when can users do revocation themselves in this scenario?

A: Only admins can revoke mail applied by auto labeling policy, for those external mail that are stored in OME portal.

Q. Is there a way to force users to access the OME portal for all platforms when sending with Encrypt-only? The main complaint I'm dealing with is external recipients struggling to decrypt the content. I have E5.

A: If a user can't open protected content directly in Outlook, they should automatically view the link to the web portal, so they should not have any struggles to open the protected email. If for some reason they do and you want to enforce the web view, you just have to create a custom branded wrapper email [*https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide#:~:text=For%20example%2C%20you%20might%20want%20to%20apply%20a,flow%20rule%20to%20apply%20encryption%20and%20custom%20branding*](https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide#:~:text=For%20example%2C%20you%20might%20want%20to%20apply%20a,flow%20rule%20to%20apply%20encryption%20and%20custom%20branding) *and this will automatically enforce usage of the web view for all users that receive the email. E3 can enforce the web view with default branded wrapper email. E5 can enforce with custom branded wrapper mail.*

Q: What is the recommendation for emails: use native encryption (do not forward and encrypt only) or sensitivity labels? As both are available for emails, it is confusing.

A: Both methods use exactly the same encryption technology and email format, but sensitivity labels offer a simpler and more customizable UI and provide additional actions that can be added to the email such as applying visual markings, so sensitivity labels are highly recommended.

Q: If I create a new SIT and publish an automatic label to protect documents containing this SIT, will all my documents be rescanned or just a new document? How can I be sure that all documents on the tenant are rescanned?

A: These files can be auto-labeled at rest before or after the auto-labeling policies are created. Files cannot be auto-labeled if they are part of an open session (the file is open). Auto-labeling based on custom sensitive information types applies only to newly created or modified content in OneDrive and SharePoint; not to existing content. This limitation also applies to auto-labeling polices. https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#:~:text=Automatic%20labeling%20in%20Office%20apps%20for%20Windows%20is,when%20you%20create%20or%20edit%20a%20sensitivity%20label

Q: How do admins and users revoke emails in AME? So far, we are only aware of how users can revoke protected documents via portal.azurerms.com.

A: Email can be revoked using Exchange Online PowerShell cmdlet **Set-**OMEMessageRevocation. There is also an encryption report in the security & compliance portal to show recent encrypted messages

Q: Lowering the classification in SharePoint doesn't seek Justification. Any plans to introduce this in SharePoint?

A: If this is about lowering the classification of files hosted in SharePoint then yes, we have plan to introduce the justification dialogue soon.

Q: How can the OME portal be used to access encrypted FILES? Messages, yes, no problem --- but protected documents?!

A: OME portal can render office documents and PDF files as long as the recipient has permissions. A sender can attach already encrypted documents, and M365 recipients can view them in the Office apps or in Outlook on the web directly. For non-M365 recipients, they will receive a notification/wrapper mail to logon to the OME portal to view the protected document.

Q: Is there any best practice around supporting user (from Service Operations point of view) e.g., if user is having difficulties, files are protected so can't be seen by the support staff.

A: We have many components like activity explorer/content explorer and even other tools to help you see things like mismatch. In addition, we can see the source file or even matching sensitive information within the portal as well with the right permissions.

Q: Just to follow up on the use case with GCC. If we are on commercial, there is no method to share MIP protected emails and files with recipients on GCCH?

A: You absolutely can but it comes down to the protection within that file. For an example, if you have the domain gov.com, then you can add them to the label so that if sent to someone@gov.com, they can open it, but another org cannot.

Q: Is there any support for protecting PDF documents?

A: For service side, Office files for Word (.docx), PowerPoint (.pptx), and Excel (.xlsx) are supported. In the meantime, many of our customers use MCAS to do auto labeling for PDFs with the MIP integration. OME can be enabled to support encrypting PDF attachments.

Q: Sensitivity label encryption is using RMS services for encryption. Is exchange online encryption by default using RMS to encrypt the email too?

A: Yes, OME and sensitivity label both use RMS to protect email.

Q: I have not checked recently but we had issues with protecting PDF documents and then sharing externally

A: We have recently incorporated support for the standard protected PDF format in many other PDF viewers and in Microsoft Edge, so most users should be able to view the protected PDF directly in the PDF viewer they regularly use.

Q: How does Exact Data Match work?

A: It's a complex process, but at its core it allows you to detect sensitive content by matching text in rows of a supplied table of sensitive data. You upload to your tenant a table with an obfuscated version of the sensitive data you want to detect (it's a table of hashes of the values which can't be reversed to the original data) and define combinations of columns in that table you want to detect (e.g., "any presence of a value in the first column plus values in the same row from any two other columns within 300 characters"). Our service will scan all the content in your documents or emails by also hashing the words or strings in the document and comparing it to the hashes in the columns in the provided table. If the hashes match, it means that the text values also match, so when text is flagged as a match to the EDM rules it means that the conditions you defined are met, i.e. some string in the document matches the exact text of one value in the column you defined as the primary element to match in your table, and values for the other columns you defined as additional evidence in the same row where the primary match was found were also found nearby. This is usually used to identify PII with extreme accuracy since it is not purely based on patterns but on matches to the exact data you provided. We will soon publish updated documentation for EDM that gives much more detail on how the solution works.

Q: Is there any plans to allow this OME one time password to be sent to a mobile phone number or other email address?

A: Thank you for the inquiry. We have collected your feedback as input to the product backlog.

Q: To simplify, can we say that sensitivity labels are for documents (even if it works for emails) and OME/AME is for emails?

A: Almost. OME/AME can also be driven by sensitivity labels, so sensitivity labels are for both documents and emails, but OME/AME are specifically for emails and their attached documents.

Q: when will browser versions of word/excel/ppt be able to consume protected content?

A: It already does. Except UDP/DKE labeled files, all other encrypted docs can be viewed and edited in browser. Let us know if you see otherwise.

Q: If a user leaves the organization, is this something can be reconfigured through super user?
A: If the user leaves the org, then he will be removed from AAD. So, he will lose access to encryption. So can't open any email and docs he/she "had" access.

Q: OME allows for read-only access to attachments in the OME portal for non-AAD account. Is there plans to allow edit and resend?
A: Thank you for the inquiry. OME portal currently does not support editing of encrypted documents. We have collected your feedback as input to the product backlog.

Q: In UDP can we limit which external users are added to the ACL e.g., on domain name basis and can the limitation be set by label?
A: The current (informal) limit is ~700 entries in the rights-management ACL. With UDP, each entry is an email address as broad domains are not allowed. If you want to include entire domains, then the only way is to add the domain to the rights-management ACL list for a label.

Q: Doesn't forcing the web view (OME) via custom branded email for a requirement to have licensing for AME?
A: OME supports enforcing web view with mail flow rules using the default OME branding configuration. AME supports enforcing web view with mail flow rules using custom branding configurations.

Q: Several of my FSI Banking customers do not permit the use of Outlook via a web browser, so is there any other workaround possible?
A: The OME portal is a different application than Outlook on the web. For external recipients, we recommend enforcing a linked based experience to request exception to the OME portal. Depending on your organization's region, the OME Portal that Microsoft provides has a URL such as https://outlook.office365.com/Encryption/.

Q: Does the b2b user have to have a guest object when sharing?
A: When sharing between two organizations, no guest object is needed if the recipient's organization uses Azure AD in the same cloud or the recipient uses a Microsoft account (e.g.: thor@outlook.com). The 2 main scenarios where a guest object is needed are:
1. The recipient does not have an Azure AD identity supplied by their organization. For example, a Zoho user.
2. The recipient has an Azure AD identity supplied by their organization but is in another cloud environment like GCC High.

Q: What happens when I use a modern attachment? (So not a copy but a link) - will the encryption extend?

A: Yes. That's the link to the same document. So, all encryptions will be applied by SharePoint. Encrypting an email does not inherit the protection of the modern attachment. The encryption on the modern attachment will be applied by SharePoint.

Q: How does this work with Teams external co-authoring?

A: Teams document authoring is backed by SharePoint Online. So, whatever you can do in SharePoint is supported in Teams as well.

Q: With external domains, can you say external users in isis.org cannot be added to the ACL for one label but can be for another label?

A: Yes, you can choose the authorized list of users for each label. External users can be added to one label and be dropped from another.

Q: Does advanced office message encryption support automatic decryption of exchange journaled messages (sent to 3rd parties as part of the exchange journal rule)?

A: Decryption is supported in the tenant that encrypted the message. To comply with the requirements of the sender's organization and possible regulations affecting it, it won't allow a recipient's organization to persistently decrypt the email.

Q: Can the rule be configured in the compliance center rather than the EXO admin center?

A: No, mail flow rule resides in the Exchange Admin Center. Alternatively, use the compliance center to apply encryption using auto-labeling or DLP.

Q: Great example right now of the EXO rules. If the user then wanted to revoke the message, they do it how?

A: Encryption applied by policies such as mail flow rule can only be revoked by admins.

Q: "This limitation also applies to auto-labeling polices." but you can define a MCAS rule to encrypt every file in a folder (SPO, OD4B)

A: You can but then you'll be hitting MCAS's labeling limits. It is a common MCAS use case right now currently as well. The limit can be increased with a ticket.

Q: Does PDF viewer for protected documents in MS Edge require any add-in to be deployed or is it natively supported?

A: No, Edge will work as you signed-in to the domain.

Q: What happens if a user sends an OME message to an external and afterward this account is removed by an admin? For example, if the user leaves the company. Can the external still read the OME protected message?

A: External users can only read mail stored in the OME portal if they have an active account to receive the OTP passcode.

Q: What are the recommendations to prevent users from downgrading labels for documents that have sensitive information?

A: If your users are not Label Owner then they can't apply/change/remove the label.

Q: How does journaling work when an email is Encrypted?

A: Exchange Online can automatically decrypt mail that was encrypted by the organization and deliver to the specified mailbox.

Q: Are hashing also used in auto labeling in apps for enterprise, so content is not sent to the O365 service?

A: Since we need to match the content using patterns, and hashing would not allow for the detection of patterns, the content can't be hashed when transmitted upstream. But the content is encrypted when transmitted to the service, and other than logging of matches in the tenant's unified audit log the content is discarded after analysis and not stored persistently in the cloud (unless it was already in the cloud to begin with).

Q: Can we unencrypt the Journaled email?

A: Yes, this is done automatically using Exchange Online journaling.

Q: Does unencrypt the Journal email also works for advanced OME with custom templates etc.? It didn't in the past.

A: No. The recommendation is to apply a mail flow rule to make (bcc) copy of the mail and then a mail flow rule to specifically remove the encryption from the copied mail.

Q: Revoke email is only available in G5 or Advanced Message Encryption, correct?

A: Yes, revocation a feature in AME, as part of G5.

Q: Will the encryption report be migrated to new compliance or security portals?

A: Yes. It will be available later this year in the Microsoft 365 compliance center.

Q: How can I encrypt emails existing on my exchange before migrating to Outlook? Using MIP labels?

A: No, we do not have any ability to encrypt mail that is already stored in a mailbox