Azure Rights Management

Configuring RMS Templates and Labels

Azure Information Protection (AIP) builds on the Azure Rights Management Services (Azure RMS) and uses RMS templates for different features. RMS templates are utilized to apply labels to documents processed with on-premises services and for Office 365 Message Encryption (OME).

Rights included in the default templates

The following table lists the usage rights that are included when the default templates are created. The usage rights are listed by their common name.

These default templates are created when your subscription was purchased, and the names and usage rights can be changed in the Azure portal and with PowerShell.

TABLE 3

Display name of template	Usage rights October 6, 2017 to current date	Usage rights before October 6, 2017
<organization name> - Confidential View Only or *Highly Confidential \ All Employees*	View, Open, Read; Copy; View Rights; Allow Macros; Print; Forward; Reply; Reply All; Save; Edit Content, Edit	View, Open, Read
<organization name>- Confidential or	View, Open, Read; Save As, Export; Copy; View Rights; Change Rights; Allow Macros; Print; Forward; Reply; Reply All; Save; Edit Content, Edit; Full Control	View, Open, Read; Save As, Export; Edit Content, Edit; View Rights; Allow Macros; Forward; Reply; Reply All

TABLE 3

Display name of template	Usage rights October 6, 2017 to current date	Usage rights before October 6, 2017
Confidential \ All Employees		

Do Not Forward option for emails

Exchange clients and services (for example, the Outlook client, Outlook on the web, Exchange mail flow rules, and DLP actions for Exchange) have an additional information rights protection option for emails: **Do Not Forward**.

Although this option appears to users (and Exchange administrators) as if it's a default Rights Management template that they can select, **Do Not Forward** is not a template. That explains why you cannot see it in the Azure portal when you view and manage protection templates. Instead, the **Do Not Forward** option is a set of usage rights that is dynamically applied by users to their email recipients.

When the **Do Not Forward** option is applied to an email, the email is encrypted and recipients must be authenticated. Then, the recipients cannot forward it, print it, or copy from it. For example, in the Outlook client, the Forward button is not available, the **Save As** and **Print** menu options are not available, and you cannot add or change recipients in the **To**, **Cc**, or **Bcc** boxes.

Unprotected Office documents that are attached to the email automatically inherit the same restrictions. The usage rights applied to these documents are **Edit Content, Edit**; **Save**; **View, Open, Read**; and **Allow Macros**. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited

protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

Difference between Do Not Forward and not granting the Forward usage right

There's an important distinction between applying the **Do Not Forward** option and applying a template that doesn't grant the **Forward** usage right to an email: The **Do Not Forward** option uses a dynamic list of authorized users that is based on the user's chosen recipients of the original email; whereas the rights in the template have a static list of authorized users that the administrator has previously specified. What's the difference? Let's take an example:

A user wants to email some information to specific people in the Marketing department that shouldn't be shared with anybody else. Should she protect the email with a template that restricts rights (viewing, replying, and saving) to the Marketing department? Or should she choose the **Do Not Forward** option? Both choices would result in the recipients not able to forward the email.

- If she applied the template, the recipients could still share the information with others in the marketing department. For example, a recipient could use Explorer to drag and drop the email to a shared location or a USB drive. Now, anybody from the marketing department (and the email owner) who has access to this location can view the information in the email.
- If she applied the **Do Not Forward** option, the recipients will not be able to share the information with anybody else in the marketing department by moving the email to another location. In this scenario, only the original recipients (and the email owner) will be able to view the information in the email.

Note

Use **Do Not Forward** when it's important that only the recipients that the sender chooses should see the information in the email. Use a template for emails to restrict rights to a group of people that the administrator specifies in advance, independently from the sender's chosen recipients.

Encrypt-Only option for emails

When Exchange Online uses the new capabilities for Office 365 Message Encryption, a new email option becomes available: **Encrypt-Only**.

This option is available to tenants who use Exchange Online and can be selected in Outlook on the web, as another rights protection option for a mail flow rule, as an Office 365 DLP action, and from Outlook (minimum version of 1804 for Office 365 ProPlus, and minimum version of 1805 when you have Office 365 apps that support Azure RMS. For more information about the Encrypt-Only option, see the following blog post announcement from the Office team: Encrypt only rolling out in Office 365 Message Encryption.

When this option is selected, the email is encrypted and recipients must be authenticated. Then, the recipients have all usage rights except **Save As, Export** and **Full Control**. This combination of usage rights means that the recipients have no restrictions except that they cannot remove the protection. For example, a recipient can copy from the email, print it, and forward it.

Similarly, by default, unprotected Office documents that are attached to the email inherit the same permissions. These documents are automatically protected and when

they are downloaded, they can be saved, edited, copied, and printed from Office applications by the recipients. When the document is saved by a recipient, it can be saved to a new name and even a different format. However, only file formats that support protection are available so that the document cannot be saved without the original protection. If you want different usage rights for an attachment, or your attachment is not an Office document that supports this inherited protection, protect the file before you attach it to the email. You can then assign the specific usage rights that you need for the file.

Alternatively, you can change this protection inheritance of documents by specifying `Set-IRMConfiguration -DecryptAttachmentForEncryptOnly $true` with Exchange Online PowerShell. Use this configuration when you don't need to retain the original protection for the document after the user is authenticated. When recipients open the email message, the document is not protected.

If you do need an attached document to retain the original protection, see Secure document collaboration by using Azure Information Protection.

Note: If you see references to **DecryptAttachmentFromPortal**, this parameter is now deprecated for Set-IRMConfiguration. Unless you have previously set this parameter, it is not available.

Automatically encrypt PDF documents with Exchange Online

When Exchange Online uses the new capabilities for Office 365 Message Encryption, you can automatically encrypt unprotected PDF documents when they are attached to an encrypted email. The document inherits the same permissions as those for the email

message. To enable this configuration, set **EnablePdfEncryption $True** with Set-IRMConfiguration.

Recipients who don't already have a reader installed that supports the ISO standard for PDF encryption can install one of the readers listed in PDF readers that support Microsoft Information Protection. Alternatively, recipients can read the protected PDF document in the OME portal.

Rights Management issuer and Rights Management owner

When a document or email is protected by using the Azure Rights Management service, the account that protects that content automatically becomes the Rights Management issuer for that content. This account is logged as the **issuer** field in the usage logs.

The Rights Management issuer is always granted the Full Control usage right for the document or email, and in addition:

- If the protection settings include an expiry date, the Rights Management issuer can still open and edit the document or email after that date.
- The Rights Management issuer can always access the document or email offline.
- The Rights Management issuer can still open a document after it is revoked.

By default, this account is also the **Rights Management owner** for that content, which is the case when a user who created the document or email initiates the protection. But there are some scenarios where an administrator or service can protect content on behalf of users. For example:

- An administrator bulk-protects files on a file share: The administrator account in Azure AD protects the documents for the users.
- The Rights Management connector protects Office documents on a Windows Server folder: The service principal account in Azure AD that is created for the RMS connector protects the documents for the users.

In these scenarios, the Rights Management issuer can assign the Rights Management owner to another account by using the Azure Information Protection SDKs or PowerShell. For example, when you use the Protect-RMSFile PowerShell cmdlet with the Azure Information Protection client, you can specify the **OwnerEmail** parameter to assign the Rights Management owner to another account.

When the Rights Management issuer protects on behalf of users, assigning the Rights Management owner ensures that the original document or email owner has the same level of control for their protected content as if they initiated the protection themselves.

For example, the user who created the document can print it, even though it's now protected with a template that doesn't include the Print usage right. The same user can always access their document, regardless of the offline access setting or expiry date that might have been configured in that template. In addition, because the Rights Management owner has the Full Control usage right, this user can also reprotect the document to grant additional users access (at which point the user then becomes the Rights Management issuer as well as the Rights Management owner), and this user can even remove the protection. However, only the Rights Management issuer can track and revoke a document.

The Rights Management owner for a document or email is logged as the **owner-email** field in the usage logs.

Note that the Rights Management owner is independent from the Windows file system Owner. They are often the same but can be different, even if you don't use the SDKs or PowerShell.

Rights Management use license

When a user opens a document or email that has been protected by Azure Rights Management, a Rights Management use license for that content is granted to the user. This use license is a certificate that contains the user's usage rights for the document or email message, and the encryption key that was used to encrypt the content. The use license also contains an expiry date if this has been set, and how long the use license is valid.

A user must have a valid use license to open the content in addition to their rights account certificate (RAC), which is a certificate that's granted when the user environment is initialized and then renewed every 31 days.

For the duration of the use license, the user is not reauthenticated or reauthorized for the content. This lets the user continue to open the protected document or email without an internet connection. When the use license validity period expires, the next time the user accesses the protected document or email, the user must be reauthenticated and reauthorized.

When documents and email messages are protected by using a label or a template that defines the protection settings, you can change these settings in your label or template

without having to reprotect the content. If the user has already accessed the content, the changes take effect after their use license has expired. However, when users apply custom permissions (also known as an ad-hoc rights policy) and these permissions need to change after the document or email is protected, that content must be protected again with the new permissions. Custom permissions for an email message are implemented with the Do Not Forward option.

The default use license validity period for a tenant is 30 days and you can configure this value by using the PowerShell cmdlet, Set-AipServiceMaxUseLicenseValidityTime. You can configure a more restrictive setting for when protection is applied by using a label or template:

- When you configure a label or template in the Azure portal, the use license validity period takes its value from the **Allow offline access setting**.

  For more information and guidance to configure this setting in the Azure portal, see the Information about the protection settings table from the instructions how to configure a label for Rights Management protection.

- When you configure a template by using PowerShell, the use license validity period takes its value from the *LicenseValidityDuration* parameter in the Set-AipServiceTemplateProperty and Add-AipServiceTemplate cmdlets.

  For more information and guidance to configure this setting by using PowerShell, see the help for each cmdlet.