How to create a new label for Azure Information Protection

How to configure Policy Settings

To view contributors to this article access the following link

https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-settings

In this article

Applies to: Azure Information Protection

Instructions for: Azure Information Protection client for Windows

Note

To provide a unified and streamlined customer experience, **Azure Information Protection client (classic)** and **Label Management** in the Azure Portal are being **deprecated** as of **March 31, 2021**. This time-frame allows all current Azure Information Protection customers to transition to our unified labeling solution using the Microsoft Information Protection Unified Labeling platform. Learn more in the official deprecation notice.

Although Azure Information Protection comes with default labels that you can customize, you can also create your own labels.

You can add a new label, or add a new sublabel to an existing label when you need a further level of classification. For example, the last label in the default policy, contains sublabels.

When you create the first sublabel for a label, users can no longer select the original, parent label. If necessary, create a new sublabel to recreate the parent label settings so that users can apply the same settings.

Use the following instructions to add a new label that can then be added to an Azure Information Protection policy.

To create a new label

1. If you haven't already done so, open a new browser window and sign in to the Azure portal. Then navigate to the **Azure Information Protection** pane.

   For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications** > **Labels** menu option: On the **Azure Information Protection - Labels** pane, do one of the following actions:
    - To create a new label: Click **Add a new label**.
    - To create a new sublabel: Right-click or select the context menu (**...**) for the label that you want to create a sublabel for, and then click **Add a sub-label**.
3. On the **Label** or **Sub-label** pane, select the options that you want for this new label, and then click **Save**.

    When you specify a display name, you are prevented from specifying some characters (such as a backslash and ampersand) because not all services and applications that use Azure Information Protection can support these characters. In addition to the characters that are blocked, do not specify the # character.

    Note that new labels are automatically assigned the color black. Choose a distinguishing color from the list of colors, or enter a hex triplet code for the red, green, and blue (RGB) components of the color. For example, **#DAA520**. If you need a reference for these codes, you'll find a helpful table from the <color> page from the MSDN web docs. You also find these codes in many applications that let you edit pictures. For example, Microsoft Paint lets you choose a custom color from a palette and the RGB values are automatically displayed, which you can then copy.

4. To make your new label available to users: From the **Classifications** > **Policies** menu option, select the policy to contain the new label. Select **Add or remove labels**. Select the label from the **Policy: Add or remove labels** pane, select **OK**, and then select **Save**.

    Tip

    For new labels, consider adding them first to a scoped policy that you use for testing. When you are satisfied with the results, remove the label from this testing scope, and then add the label to a policy that you use in production.

    For more information about adding labels, see How to add or remove a label.

    Your changes are automatically available to users and services. There's no longer a separate publish option.

5. If you want this new label name and description to display in different languages for users: Follow the procedures in How to configure labels for different languages.

To configure the policy settings

1. If you haven't already done so, open a new browser window and sign in to the Azure portal. Then navigate to the **Azure Information Protection** pane.

    For example, in the search box for resources, services, and docs: Start typing **Information** and select **Azure Information Protection**.

2. From the **Classifications** > **Policies** menu option: On the **Azure Information Protection - Policies** pane, select **Global** if the settings that you want to configure will apply to all users.

   If the settings that you want to configure are in a scoped policy so that they apply to selected users only, select your scoped policy instead.

3. On the **Policy** pane, configure the settings:
   - **Select the default label**: When you set this option, select the label to assign to documents and emails that do not have a label. You cannot set a label as the default if it has sublabels.

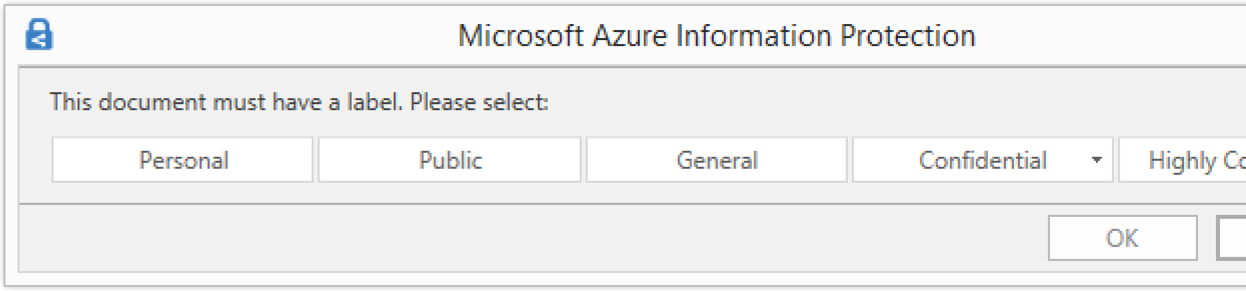
     This setting applies to Office apps and the scanner. It does not apply to File Explorer, or PowerShell.

   - **Send audit data to Azure Information Protection analytics**: Before you create an Azure Log Analytics workspace for Azure Information analytics, the values for this setting display **Off** and **Not configured**. When you create the workspace, the values change to **Off** and **On**.

     When the setting is **On**, clients that support central reporting send data to the Azure Information Protection service. This information includes what labels are applied and when a user selects a label with a lower classification, or removes a label. For more information about what information is sent and stored, see the Information collected and sent to Microsoft section in the central reporting documentation. Set this policy setting to **Off** to prevent this data from being sent.

   - **All documents and emails must have a label**: When you set this option to **On**, all saved documents and sent emails must have a label applied. The labeling might be manually assigned by a user, automatically as a result of a condition, or be assigned by default (by setting the **Select the default label** option).

     If a label is not assigned when users save a document or send an email, they are prompted to select a label. For example:

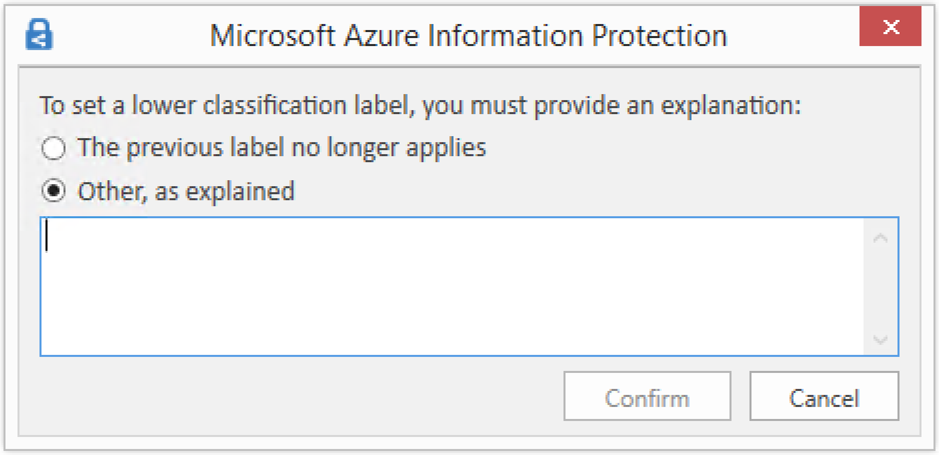


Microsoft Azure Information Protection

This document must have a label. Please select:

     This option does not apply when you remove a label by using the Set-AIPFileLabel PowerShell cmdlet with the *RemoveLabel* parameter.

- **Users must provide justification to set a lower classification label, remove a label, or remove protection**: When you set this option to **On** and a user does any of these actions (for example, change the **Public** label to **Personal**), the user is prompted to provide an explanation for this action. For example, the user might explain that the document no longer contains sensitive information. The action and its justification reason are logged in their local Windows event log: **Applications and Services Logs** > **Azure Information Protection**.

  To set a lower classification label, you must provide an explanation:

  ○ The previous label no longer applies

  ● Other, as explained

  This option is not applicable for lowering the classification of sublabels under the same parent label.

- **For email messages with attachments, apply a label that matches the highest classification of those attachments**: When you set this option to **Recommended**, users are prompted to apply a label to their email message. The label is dynamically chosen, based on the classification labels that are applied to the attachments, and the highest classification label is selected. The attachment must be a physical file, and cannot be a link to a file (for example, a link to a file on SharePoint or OneDrive for Business). Users can accept the recommendation or dismiss it. When you set this option to **Automatic**, the label is automatically applied but users can remove the label or select a different label before sending the email.

  To take the ordering of sublabels into consideration when you use this policy setting, you must configure an advanced client setting.

  When the attachment with the highest classification label is configured for protection with the preview setting of user-defined permissions: - When the label's user-defined permissions include Outlook (Do Not Forward), that label is applied and Do Not Forward protection is applied to the email. When the label's user-defined permissions are just for Word, Excel, PowerPoint, and File Explorer, that label is not applied to the email, and neither is protection.

- **Display the Information Protection bar in Office apps**: When this setting is off, users cannot select labels from a bar in Word, Excel, PowerPoint, and Outlook. Instead, users must select labels from the **Protect** button on the ribbon. When this setting is on, users can select labels from either the bar or the button.

  When this setting is on, it can be used in conjunction with an advanced client setting so that users can permanently hide the Azure Information Protection bar if they choose not to show the bar. They can do this by clearing the **Show Bar** option from the **Protect** button.

- **Add the Do Not Forward button to the Outlook ribbon**: When this setting is on, users can select this button from the **Protection** group on the Outlook ribbon in addition to selecting the **Do Not Forward** option from Outlook menus. To help ensure that users classify their emails as well as protect them, you might prefer to not add this button but instead, configure a label for protection and a user=defined permission for Outlook. This protection setting is functionally the same as selecting the **Do Not Forward** button, but when this functionality is included with a label, emails are classified as well as protected.

  This policy setting can also be configured with an advanced client setting as a client customization.

- **Make the custom permissions option available to users**: When this setting is on, users see options to set their own protection settings that can override any protection settings that you might have included with a label configuration. Users can also see an option to remove protection. When this setting is off, users do not see these options.

  Note that this policy setting has no effect on custom permissions that users can configure from Office menu options. However, it can also be configured with an advanced client setting as a client customization.

  The custom permissions options are located in the following places:

  - In Office applications: From the ribbon, **Home** tab > **Protection** group > **Protect** > **Custom Permissions**
  - From File Explorer: Right-click > **Classify and protect** > **Custom permissions**

- **Provide a custom URL for the Azure Information Protection client "Tell me more" web page**: Users see this link in the **Microsoft Azure Information Protection** dialog box, **Help and Feedback** section, when they select **Protect** > **Help and feedback** from the **Home** tab in their Office applications. By default, this link goes to the Azure Information Protection website. You can enter an HTTP or HTTPS (recommended) URL if you want this link to go to an alternative web page. No check is made to verify that the custom URL entered is accessible or displays correctly on all devices.

As an example, for your help desk, you might enter the Microsoft documentation page that includes information about installing and using the client: `https://docs.microsoft.com/information-protection/rms-client/info-protect-client`. Or release version information: `https://docs.microsoft.com/information-protection/rms-client/client-version-release-history`. Alternatively, you might publish your own webpage that includes information for users to contact your help desk, or a video that steps users through how to use the labels that you have configured.

4. To save your changes and make them available to users, click **Save**.

When you click **Save**, your changes are automatically available to users and services. There's no longer a separate publish option.