Microsoft Azure

Azure Information Protection User Guide

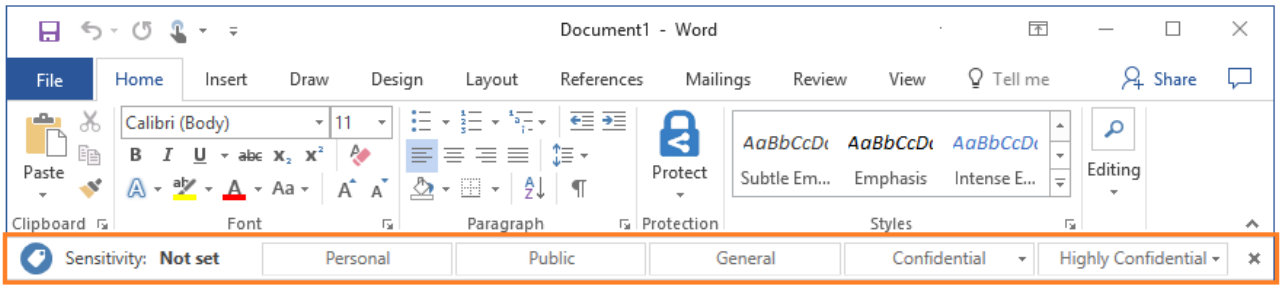
INDEX

1. Classify a file or email by using Azure Information Protection

Using Office apps to classify your documents and emails

Use the Azure Information Protection bar and select one of the labels that has been configured for you.

For example, the following picture shows that the document hasn't yet been labeled because the **Sensitivity** shows **Not set**. To set a label, such as "General", click **General**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.



If a label is already applied to the document and you want to change it, you can select a different label. If the labels are not displayed on the bar, first click the **Edit Label** icon, next to the current label value.

In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label (), which you can keep or change.
- Your administrator configured recommended prompts to select a specific label when sensitive data is detected. You can accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

Using File Explorer to classify files

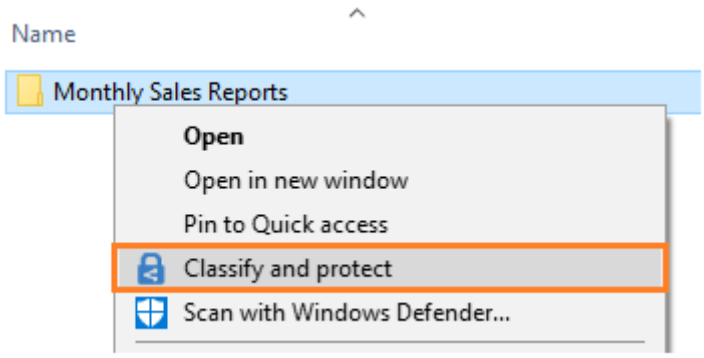
When you use File Explorer, you can quickly classify a single file, multiple files, or a folder.

When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification that you set. However, new files that you create in that folder or subfolders are not automatically classified.

When you use File Explorer to classify your files, if one or more of the labels appear dimmed, the files that you selected do not support classification without also protecting them.

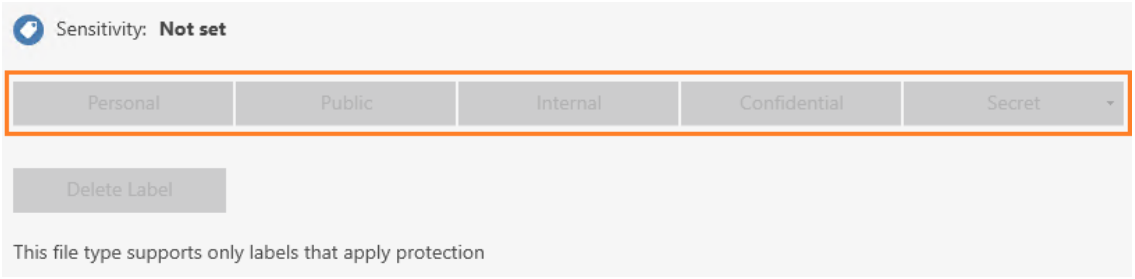
● To classify a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the **Classify and protect - Azure Information Protection** dialog box, use the labels as you would do in an Office application, which sets the classification as defined by your administrator.

   If none of the labels can be selected (they appear dimmed): The selected file does not support classification. For example:



3. If you selected a file that does not support classification, click **Close**. You cannot classify this file without also protecting it.

   If you selected a label, click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.

If you change your mind about the label you chose, simply repeat this process and choose a different label.

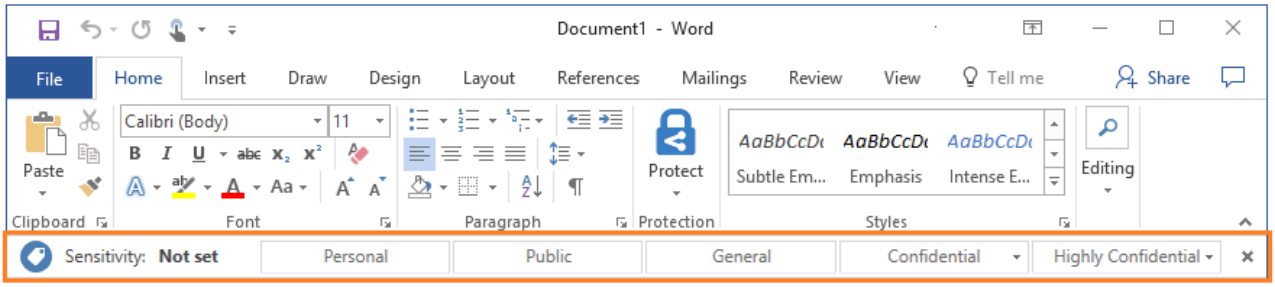
The classification that you specified stays with the file, even if you email the file or save it to another location.

2. Classify and protect a file or email by using Azure Information Protection

Using Office apps to classify and protect your documents and emails

Use the Azure Information Protection bar or the **Protect** button on the ribbon to select one of the labels that has been configured for you.

For example, the following picture shows that the document hasn't yet been labeled because the **Sensitivity** shows **Not set** on the Azure Information Protection bar. To set a label, such as "General", click **General**. If you're not sure which label to apply to the current document or email, use the label tooltips to learn more about each label and when to apply it.



If a label is already applied to the document and you want to change it, you can select a different label. If the labels are not displayed on the bar, first click the **Edit Label** icon, next to the current label value.

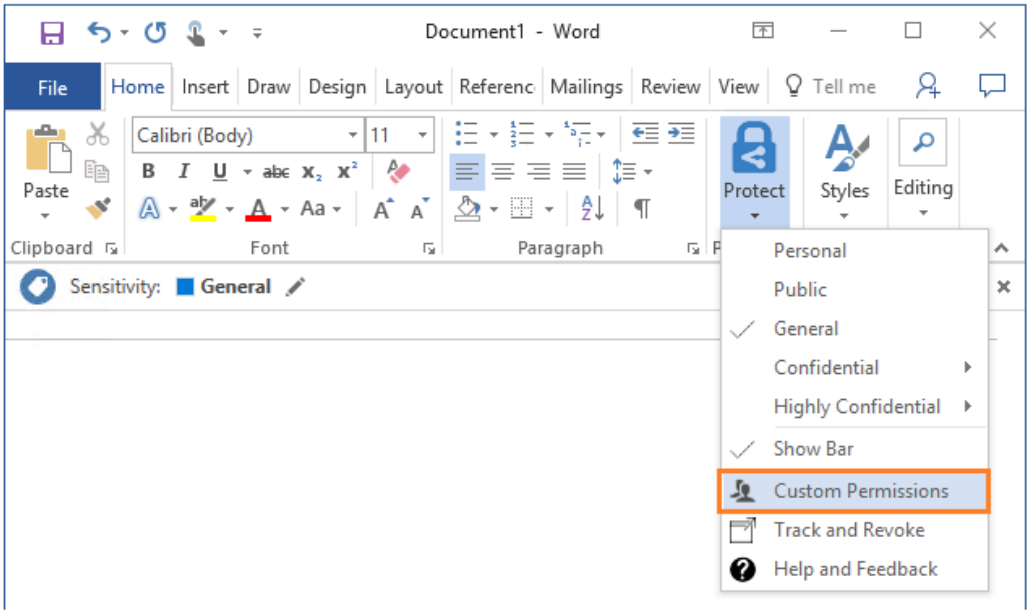
In addition to manually selecting labels, labels can also be applied in the following ways:

- Your administrator configured a default label, which you can keep or change.
- Your administrator configured recommended prompts to select a specific label when sensitive data is detected. You can accept the recommendation (and the label is applied), or reject it (the recommended label is not applied).

● Set custom permissions for a document

You can specify your own protection settings for documents rather than use the protection settings that your administrator might have included with your selected label. This option is specific to documents and is not available with Outlook.

1. On the **Home** tab, in the **Protection** group, click **Protect** > **Custom Permissions**:



   If you do not see **Custom Permissions**, your administrator does not allow you to use this option.

2. In the **Microsoft Azure Information Protection** dialog box, specify the following:
   - **Protect with custom permissions**: Make sure that this is selected so that you can specify and apply your custom permissions. Clear this option to remove any custom permissions.
   - **Select permissions**: If you want to protect the file so that only you can access it, select **Only for me**. Otherwise, select the level of access that you want people to have.
   - **Select users, groups, or organizations**: Specify the people who should have the permissions you selected for your file or files. Type their full email address, a group email address, or a domain name from the organization for all users in that organization.

     You can also use the address book icon to select users or groups from the Outlook address book.

   - **Expire access**: Select this option only for time-sensitive files so that the people you specified will not be able to open your selected file or files after a date that you set. You will still be able to

open the original file but after midnight (your current time zone), on the day that you set, the people that you specified will not be able to open the file.

3. Click **Apply** and wait for the **Custom permissions applied** message. Then click **Close**.

● Safely sharing by email

When you share Office documents by email, you can attach the document to an email that you protect, and the document is automatically protected with the same restrictions that apply to the email.

However, we recommend that you protect the document first, and then attach it to the email. Protect the email as well if the email message contains sensitive information. Two benefits of protecting the document before you attach it to an email:

- You can track and if necessary, revoke the document after you have emailed it.
- You can apply different permissions to the document than to the email message.

Using File Explorer to classify and protect files

When you use File Explorer, you can quickly classify and protect a single file, multiple files, or a folder.

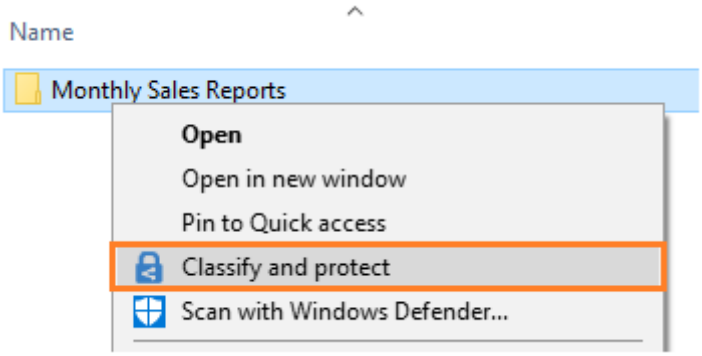
When you select a folder, all the files in that folder and any subfolders it has are automatically selected for the classification and protection options that you set. However, new files that you create in that folder or subfolders are not automatically configured with those options.

When you use File Explorer to classify and protect your files, if one or more of the labels appear dimmed, the files that you selected do not support classification. For these files, you can select a label only if your administrator has configured the label to apply protection. Or, you can specify your own protection settings.

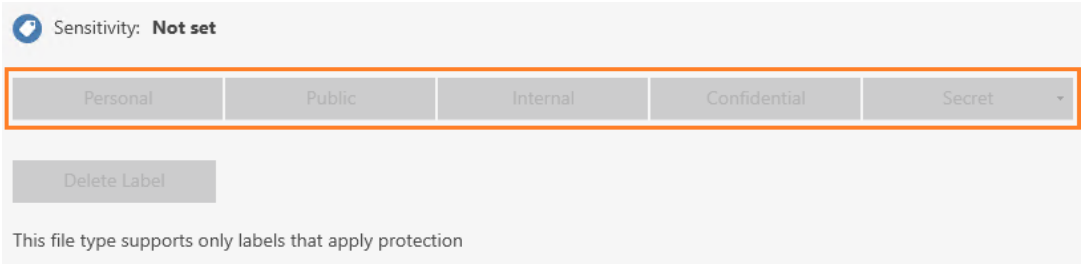
Some files are automatically excluded from classification and protection, because changing them might stop your PC from running. Although you can select these files, they are skipped as an excluded folder or file. Examples include executable files and your Windows folder.

● To classify and protect a file by using File Explorer

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**. For example:



2. In the Classify and protect - Azure Information Protection dialog box, use the labels as you would do in an Office application, which sets the classification and protection as defined by your administrator.
    - If none of the labels can be selected (they appear dimmed): The selected file does not support classification but you can protect it with custom permissions (step 3). For example:



3. You can specify your own protection settings rather than use the protection settings that your administrator might have included with your selected label. To do this, select Protect with custom permissions.

    If you do not see Protect with custom permissions, your administrator does not allow you to use this option.

    Any custom permissions that you specify replace rather than supplement protection settings that your administrator might have defined for your chosen label.

4. If you selected the custom permissions option, now specify the following:
    - Select permissions: Select the level of access that you want people to have when you protect the selected file or files.
    - Select users, groups, or organizations: Specify the people who should have the permissions you selected for your file or files.Type their full email address, a group email address, or a domain name from the organization for all users in that organization.

      Alternatively, you can use the address book icon to select users or groups from the Outlook address book.

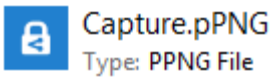
- Expire access: Select this option only for time-sensitive files so that the people you specified will not be able to open your selected file or files after a date that you set You will still be able to open the original file but after midnight (your current time zone), on the day that you set, the people that you specified will not be able to open the file.

  Note that if this setting was previously configured by using custom permissions from an Office 2010 app, the specified expiry date does not display in this dialog box but the expiry date is still set. This is a display issue only for when the expiry date was configured in Office 2010.

5. Click Apply and wait for the Work finished message to see the results. Then click Close.

The selected file or files are now classified and protected, according to your selections. In some cases (when adding protection changes the file name extension), the original file in File Explorer is replaced with a new file that has the Azure Information Protection lock icon.

For example:



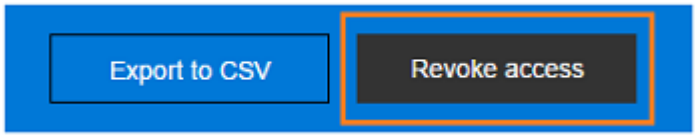
3. Track and revoke your documents when you use Azure Information Protection

After you have protected your documents by using Azure Information Protection, you can track how people are using these documents.

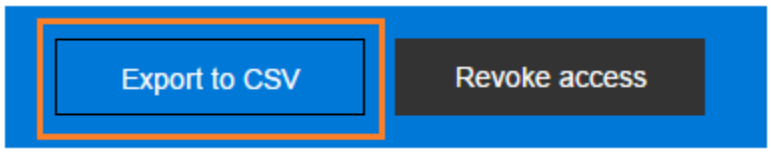
If necessary, you can also revoke access to them if people should no longer be able to read them. To do this, you use the **document tracking site**. You can access this site from Windows computers, Mac computers, and even from tablets and phones.

Actions you can take in the document tracking site:

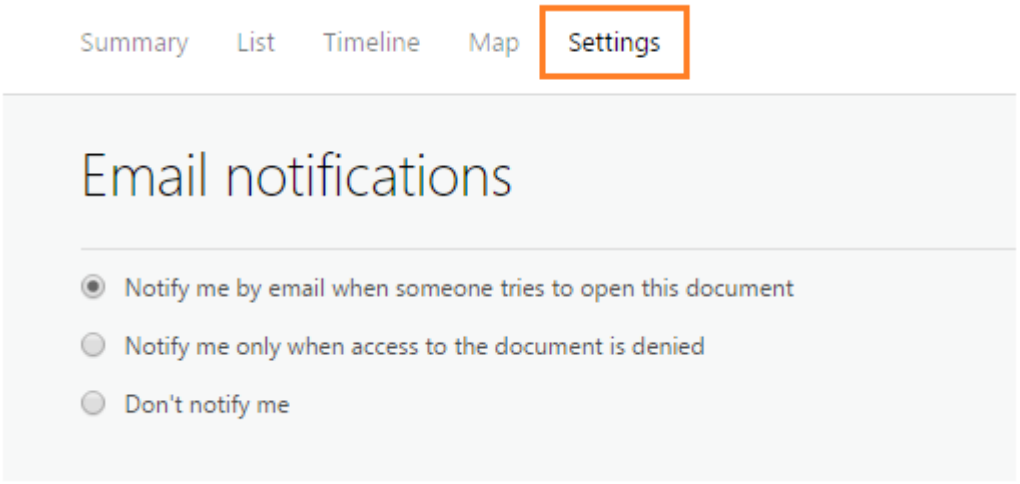
- **If you need to stop sharing a document:**
  - Click **Revoke access**. Note the period of time that the document continues to be available. Decide whether to let people know that you're revoking access to the document you previously shared by providing a customized message. When you revoke a document, it doesn't delete the document that you shared, but authorized users can no longer open it:



- If you want to export to Excel:
  - Click **Export to CSV**, so that you can then modify the data, and create your own views and graphs:



- If you want to configure email notifications:
  - Click **Settings** and select how and whether to be emailed when the document is accessed:



- If you want to track and revoke shared documents for others:
  - Administrators for Azure Information Protection can click the Admin icon to track and revoke protected documents for users when those users have registered their documents with the document tracking site. Only administrators see this icon:

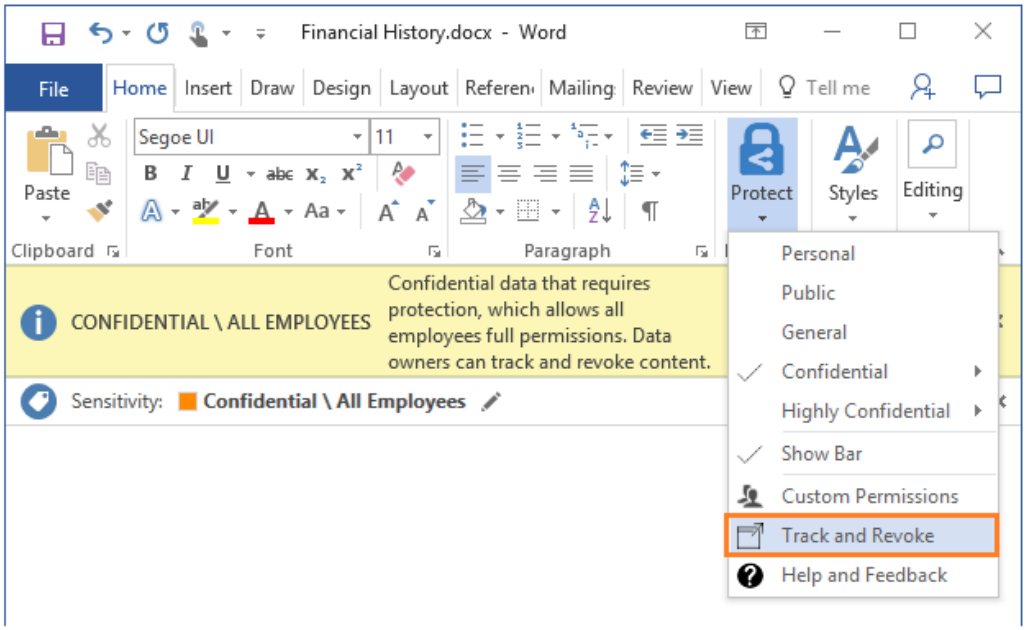
    If you do not see this icon, despite being a global admin, it's because you haven't yet shared any documents. In this case, use the following URL to access the document tracking site: https://portal.azurerms.com/#/admin

To track a document that you have protected, you must use your Windows computer to register it with the document tracking site. To do this, use either File Explorer, or your Office apps.

Using Office to track or revoke the document

For the Office applications, Word, Excel, and PowerPoint:

1. Open the protected document that you want to track or revoke.
2. On the **Home** tab, in the **Protection** group, click **Protect** > **Track and Revoke**:



Using File Explorer to track or revoke the document

1. Right-click the protected file, and select **Classify and protect**.
2. From the **Classify and protect - Azure Information Protection** dialog box, select **Track and revoke**.

Using a web browser to track and revoke documents that you have registered

After you have registered the protected document by using your Office apps or File Explorer, you can track and revoke these documents by using a supported web browser:

- Using your Windows PC, Mac computer, or mobile device, visit the document tracking site.

  Supported browsers: We recommend using Internet Explorer that is at least version 10, but you can use any of following browsers to use the document tracking site:

  - Internet Explorer: At least version 10
  - Internet Explorer 9 with at least MS12-037: Cumulative Security Update for Internet Explorer: June 12, 2012
  - Mozilla Firefox: At least version 12
  - Apple Safari 5: At least version 5
  - Google Chrome: At least version 18

4. View and use files that have been protected by Rights Management

You can often view a protected document by simply opening it. For example, you might double-click an attachment in an email message or double-click a file from File Explorer, or you might click a link to a file.

Message.rpmsg as an email attachment

If you see **message.rpmsg** as a file attachment in an email, this file is not a protected document but a protected email message that displays as an attachment. You can't use the Azure Information Protection Viewer for Windows to view this protected email message on your Windows PC. Instead, you need an email application for Windows that supports Rights Management protection, such as Office Outlook. Or you can use Outlook on the web.

Prompts for authentication

Before you can view the protected file, the Rights Management service that was used to protect the file must first confirm that you are authorized to view the file. The service does this confirmation by checking your user name and password. In some cases, these credentials might be cached and you do not see a prompt that asks you to sign in. In other cases, you are prompted to supply your credentials.

To view and use a protected document

1. Open the protected file (for example, by double-clicking the file or attachment, or by clicking the link to the file). If you are prompted to select an app, select **Azure Information Protection Viewer**.
2. If you see a page to **Sign in** or **Sign up**: Click **Sign in** and enter your credentials. If the protected file was sent to you as an attachment, be sure to specify the same email address that was used to send you the file.
3. A read-only version of the file opens in the **Azure Information Protection Viewer**. If you have sufficient permissions, you can print the file, and edit it.

   You can check your permissions for the file by clicking **Permissions**. From the **Permissions** dialog box, you can also identify the file owner to contact if you want to request a new version of the file with additional permissions.

4. To edit the file, click **Save As**, which lets you save the file without the label and with no protection to its original file name extension. You can then edit the file by using the application that's associated with that file type.

   When you have finished editing the file, in File Explorer, right-click the file to reapply the label, which in turn reapplies protection.

5. If you have additional protected files to open, you can browse directly to them from the viewer, by using the **Open** option. Your selected file replaces the original file in the viewer.

Hint

If the protected file does not open and you have the full Azure Information Protection client installed, try the **Reset Settings** option.

To access this option, from an Office app, select the **Protect** button > **Help and Feedback** > **Reset Settings**.

5. Remove labels and protection from files and emails that have been labeled by Azure Information Protection or protected by Rights Management

When the label that you remove is configured to apply protection, this action also removes protection from the file. You might be prompted to record why you are removing the label.

Important

You must be the owner of the file to remove protection, or been granted permissions to remove protection (the Rights Management Extract or Full Control permission).

If you want to choose a different label or a different set of protection settings, you do not need to remove the label or protection.

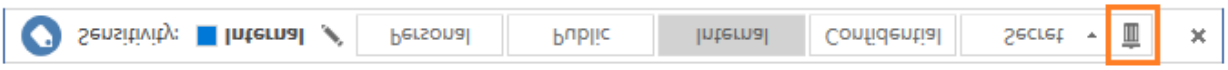
Instead, choose a new label and if necessary, you can define custom permissions if your administrator allows this configuration.

You can remove labels and protection from Office documents and emails when you are creating or editing them from within your Office desktop apps: **Word**, **Excel**, **PowerPoint**, **Outlook**.

You can also remove labels and protection by using **File Explorer**, which supports additional file types and is a convenient way to remove labels and protection from multiple files at once.

Using Office apps to remove labels and protection from documents and emails

On the Information Protection bar, click the **Delete Label** icon:



If the **Delete Label** icon is not immediately available, first click the **Edit Label** icon:

Using File Explorer to remove labels and protection from files

When you use File Explorer, you can quickly remove labels and protection from a single file, multiple files, or a folder. When you select a folder, all the files in that folder and any subfolders it has are automatically selected.

1. In File Explorer, select your file, multiple files, or a folder. Right-click, and select **Classify and protect**.
2. To remove a label: In the **Classify and protect - Azure Information Protection** dialog box, click **Delete Label**. If the label was configured to apply protection, that protection is automatically removed.
3. To remove custom protection from a single file: In the **Classify and protect - Azure Information Protection** dialog box, clear the **Protect with custom permissions** option.

   If you do not see the **Protect with custom permissions** option, your administrator does not allow you to use this option.

4. To remove custom protection from multiple files: In the **Classify and protect - Azure Information Protection** dialog box, click **Remove custom permissions**.

   If you do not see the **Remove custom permissions** option, your administrator does not allow you to use this option.

5. Click **Apply** and wait for the **Work finished** message to see the results. Then click **Close**.