Azure Information Protection Instructions

Office of Information Security

Created by Jeroen Barendse

Updated August 16, 2017

What is it?

Azure Information Protection, or AIP, is a file encryption software provided by Microsoft that allows users to restrict access to files.

Where can I get it?

For those of you that want to jump the gun and get started right away, you can download the Azure Information Protection Software here: https://www.microsoft.com/en-us/download/details.aspx?id=53018.

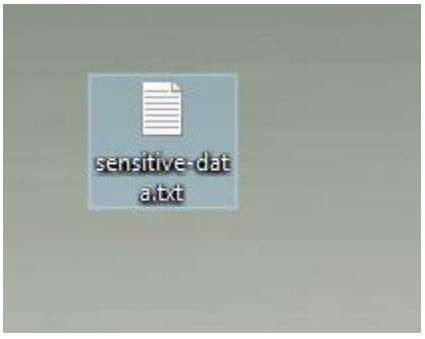
How does it work?

AIP restricts access to files based on your CSUSM user account, so you never have to enter a password to unlock a file. In addition, you can choose other CSUSM users that you would like to have access to the file by entering in their email address.

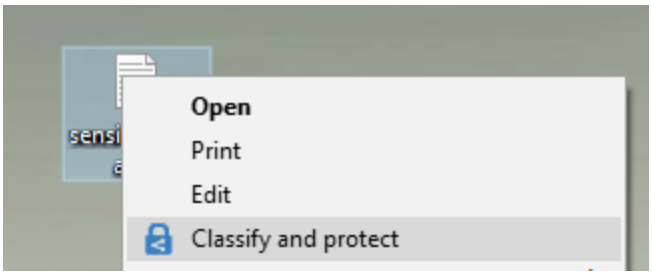
How to use AIP

There are two ways of protecting a document with AIP. On Windows, you can simply right-click a file that you wish to protect and choose Azure Information Protection.

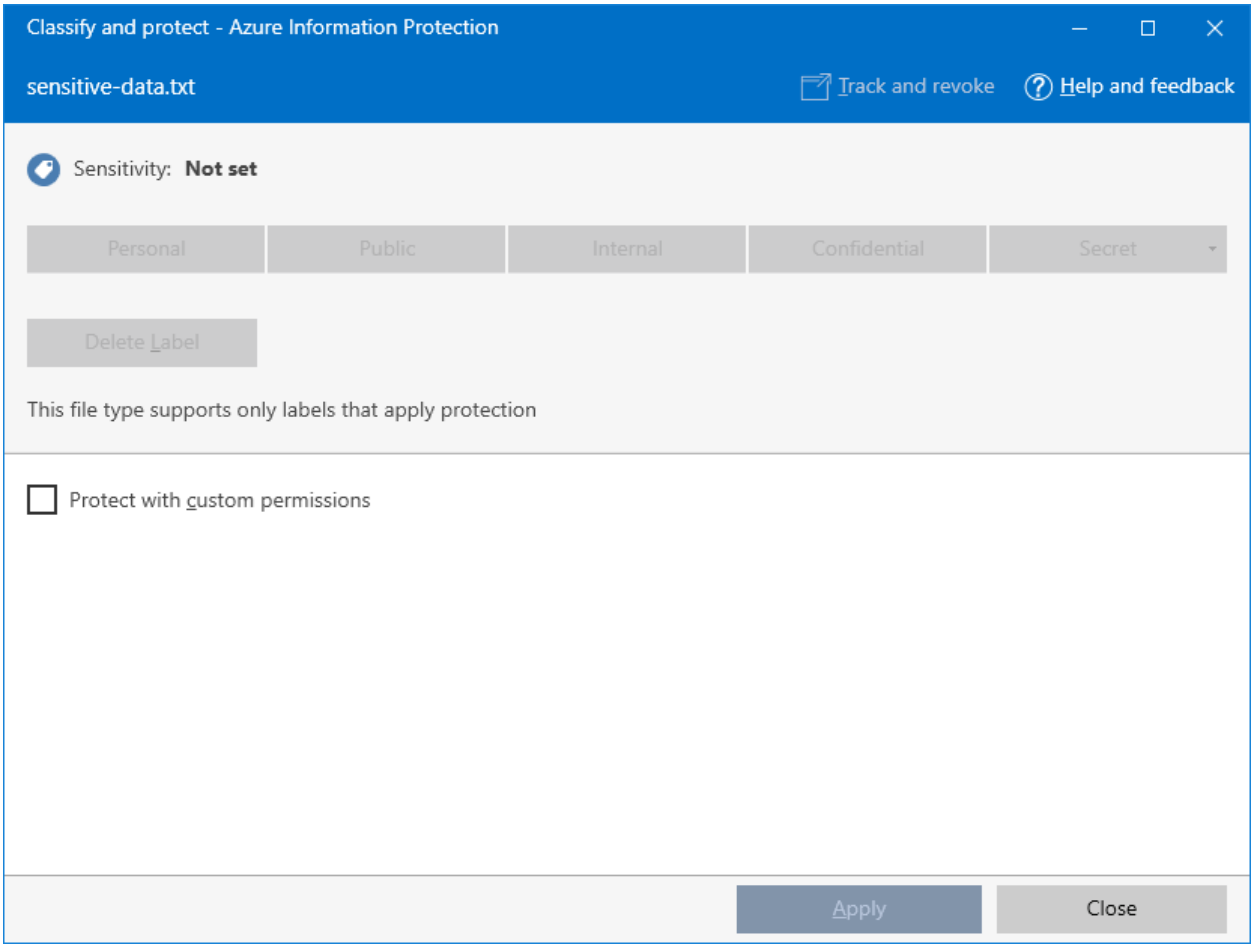
For example, the file named “sensitive-data.txt” contains social security numbers and must be encrypted by California and Federal laws:



By right-clicking on the file, the AIP option can be selected by clicking “Classify and Protect”:

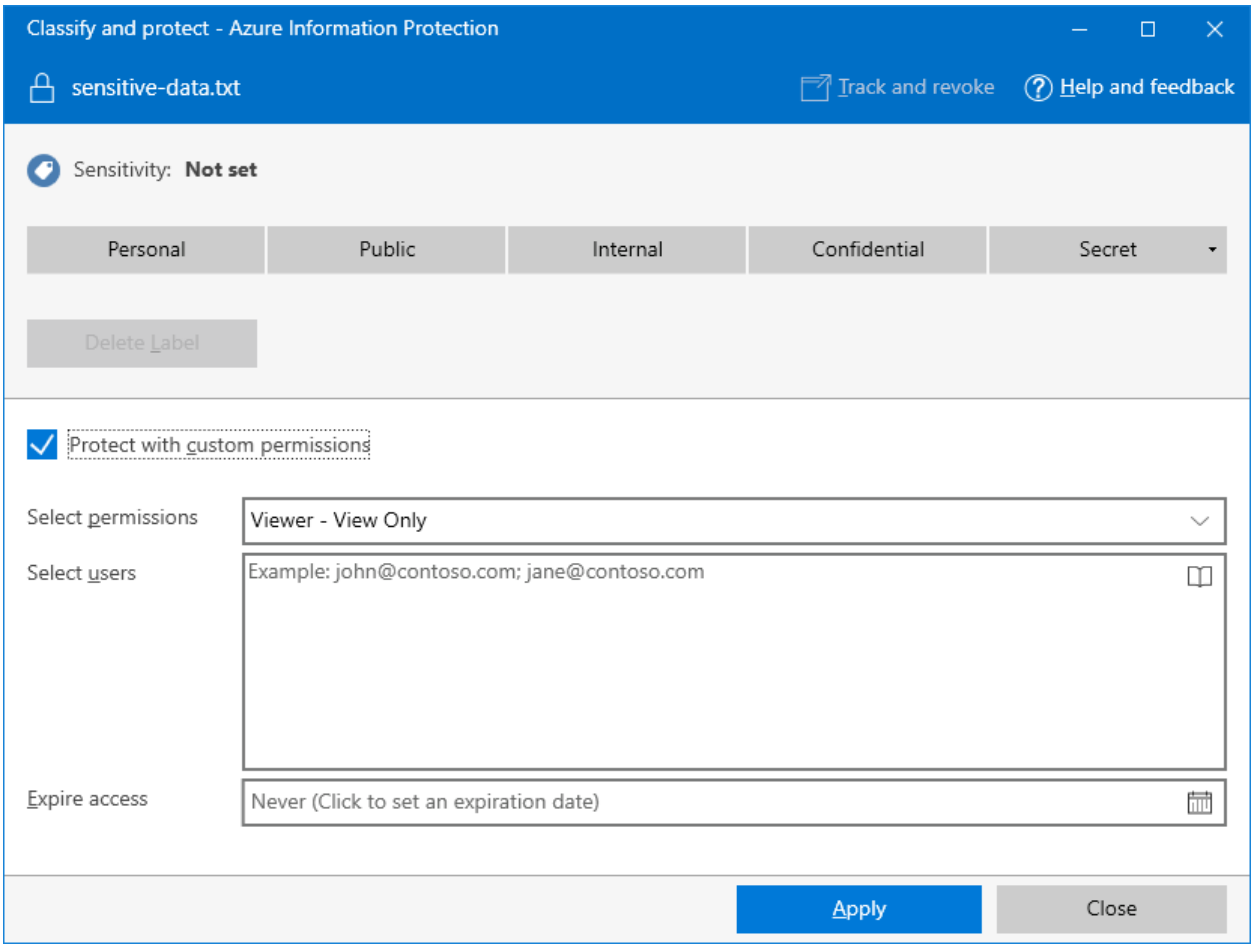


The Azure Information Protection dialogue box will open, and to grant certain individuals, choose "Protect with custom permissions":



After the custom permissions check box has been selected, you will see three new sections:

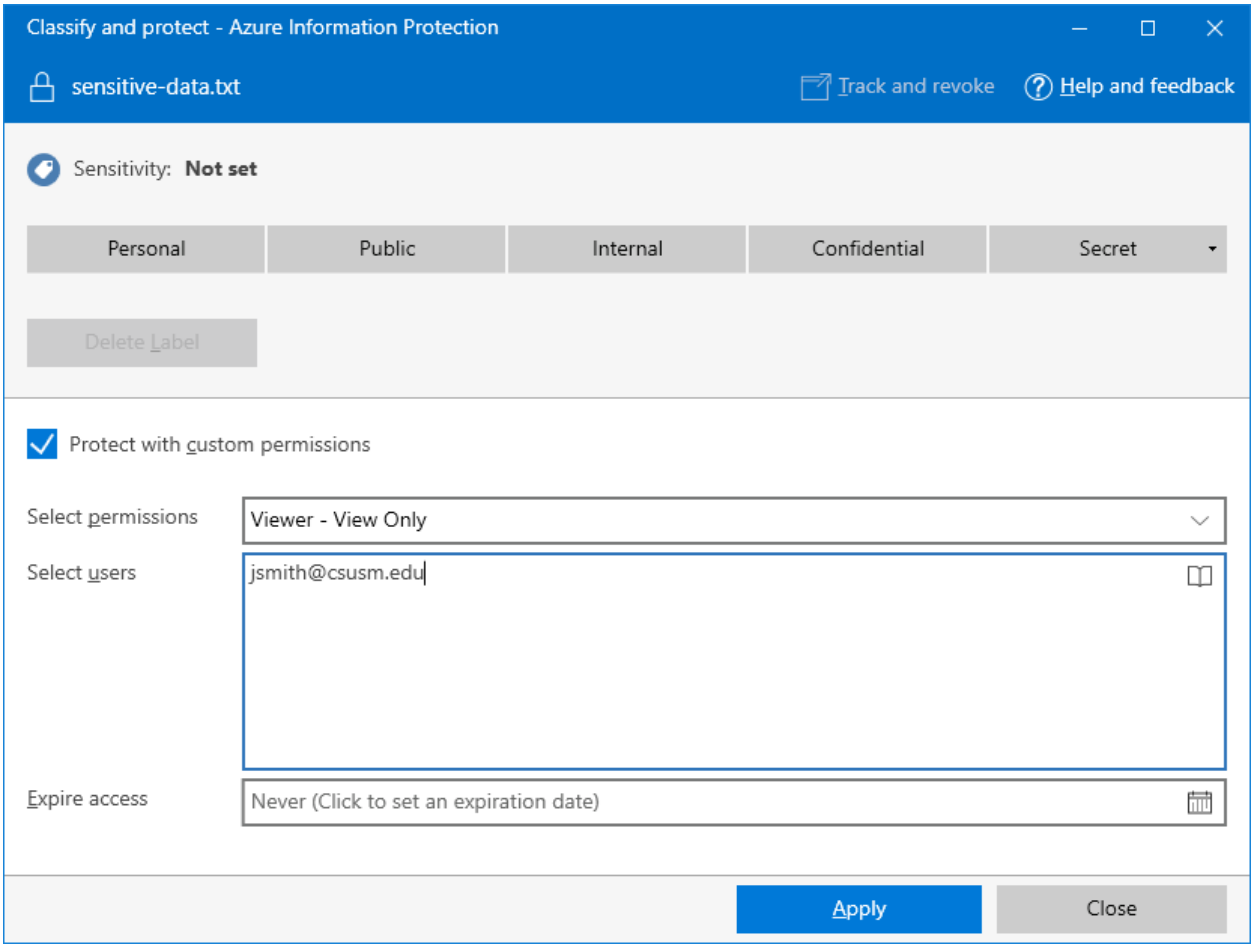
1. Select permissions
2. Select users
3. Expire access



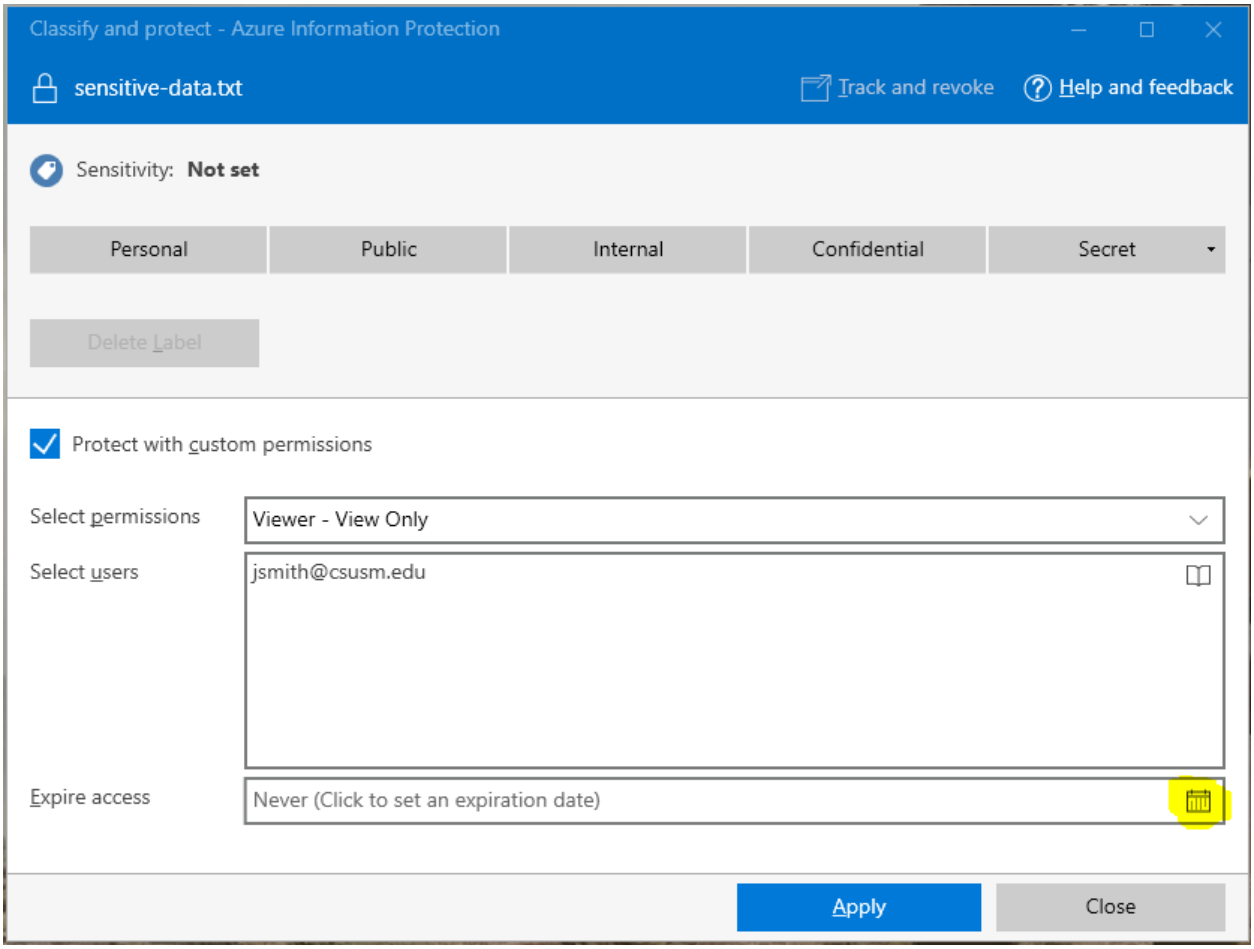
In the "Select permissions" section, choose which permissions you'd like to apply to the document. There are four different permission levels:

1. Viewer – View Only
2. Reviewer – View, Edit
3. Co-Author – View, Edit, Copy, Print
4. Co-Owner – All Permissions

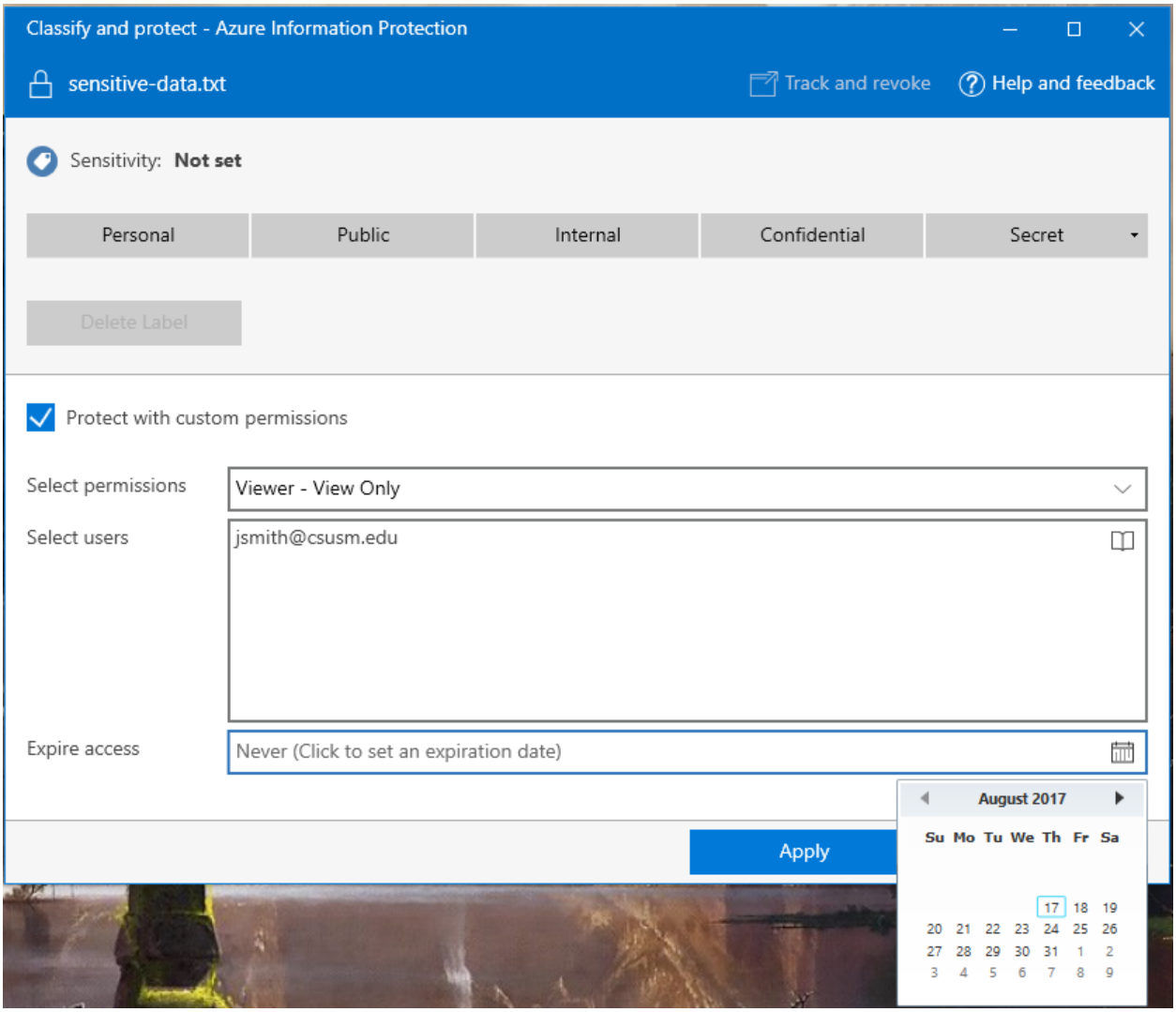
In the "Select users" section, enter the email addresses of the users you'd like to grant access to. For instance, if John Smith needs access to this document, I would type jsmith@csusm.edu in to the Select users box:



Finally, if you want to select a date on which this document can no longer be accessed, click the calendar icon in the “Expire access” box and you can select a date to expire the access, making it so only you can view this document:



Sensitivity: Secret



You can also classify the type of information stored in this document by selecting one of the options at the top of the AIP dialogue box:

1. **Personal** – Use this classification for information that should not be shared outside your department
2. **Public** – Use this classification for information that does not need to be protected
3. **Internal** – Use this classification for information that should not be shared with individuals outside the University (Defined as Protected Level 2 Data by the CSU Data Classification Standard)
4. **Confidential** – Use this classification for information that is required to be kept confidential by law (Defined as Protected Level 1 Data by the CSU Data Classification Standard)
5. **Secret** – Use this classification for information where if the confidentiality of such information were to be breached, we would be required to report it by law

Some file types will not allow you to classify the document until after you have selected to apply custom permissions. If you see the message, “This file type only supports labels that apply protection” be sure to click the “Protect with custom permissions” check box to enable classification.

*****A quick note on classifying – classifying the data stored in the document does not protect or encrypt the document! Be sure to properly protect the document by selecting the "Protect with custom permissions" check box.**

Classification within Office

Documents containing sensitive or confidential information that are created with Microsoft Office, such as Excel spreadsheets or Word documents, can be classified directly in the application by selecting the appropriate classification from the Sensitivity bar seen below the ribbon menu: