



# **Managing your private data**

## **Cloud Manager**

Tom Onacki  
July 02, 2021

# Table of Contents

- Managing your private data ..... 1
  - Controlling your data using Policies ..... 1
  - Applying Status tags to manage your scanned files ..... 5
  - Assigning users to manage certain files ..... 6
  - Categorizing your data using AIP labels ..... 7
  - Sending email alerts when non-compliant data is found ..... 11
  - Deleting source files ..... 13
  - Moving source files to an NFS share ..... 14

# Managing your private data

Cloud Data Sense provides many ways for you to manage your private data. Some functionality just makes it easier to see the data that is most important to you, and other functionality allows you to make changes to the data.

- Using the "Policy" functionality you can create your own custom search queries so that you can easily see the results by clicking one button.
- You can send email alerts to Cloud Manager users when certain critical Policies return results.
- You can add a Status to files that you want to mark for some type of follow-up.
- If you are subscribed to [Azure Information Protection \(AIP\)](#) to classify and protect your files, you can use Cloud Data Sense to manage those AIP labels.
- You can delete files that seem insecure or too risky to leave in your storage system, or that you have identified as a duplicate.



The capabilities described in this section are available only if you have chosen to perform a full classification scan on your data sources. Data sources that have had a mapping-only scan do not show file-level details.

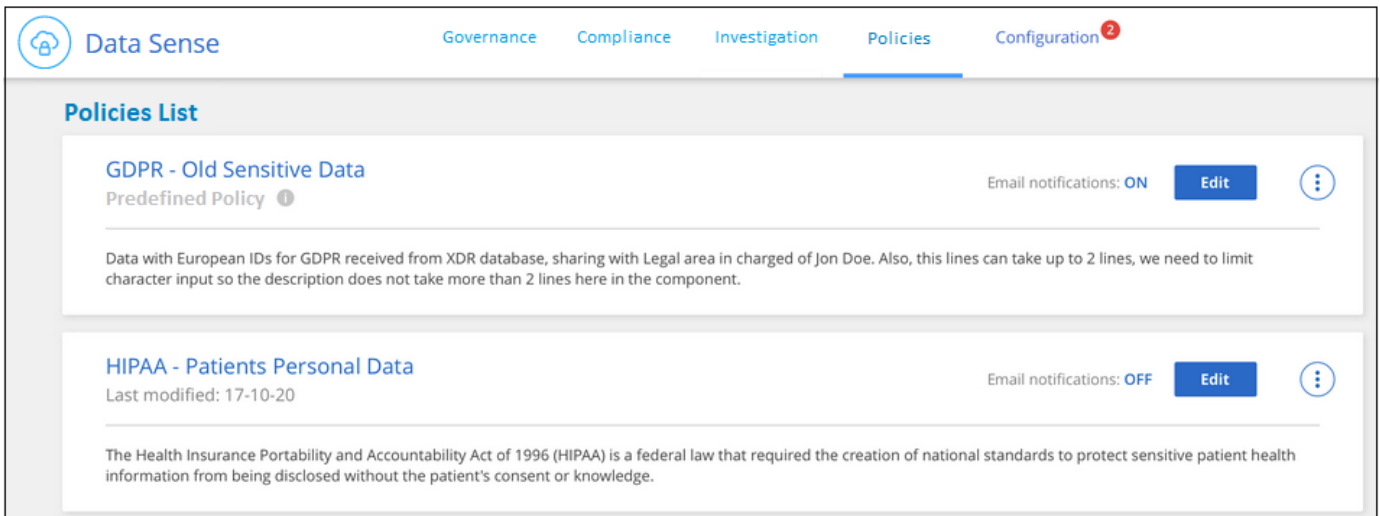
## Controlling your data using Policies

Policies are like a favorites list of custom filters that provide search results in the Investigation page for commonly requested compliance queries. Cloud Data Sense provides a set of predefined Policies based on common customer requests. You can create custom Policies that provide results for searches specific to your organization.

Policies provide the following functionality:

- [Predefined Policies](#) from NetApp based on user requests
- Ability to create your own custom Policies
- Launch the Investigation page with the results from your Policies in one click
- Send email alerts to Cloud Manager users when certain critical Policies return results so you can get notifications to protect your data
- Assign AIP (Azure Information Protection) labels automatically to all files that match the criteria defined in a Policy

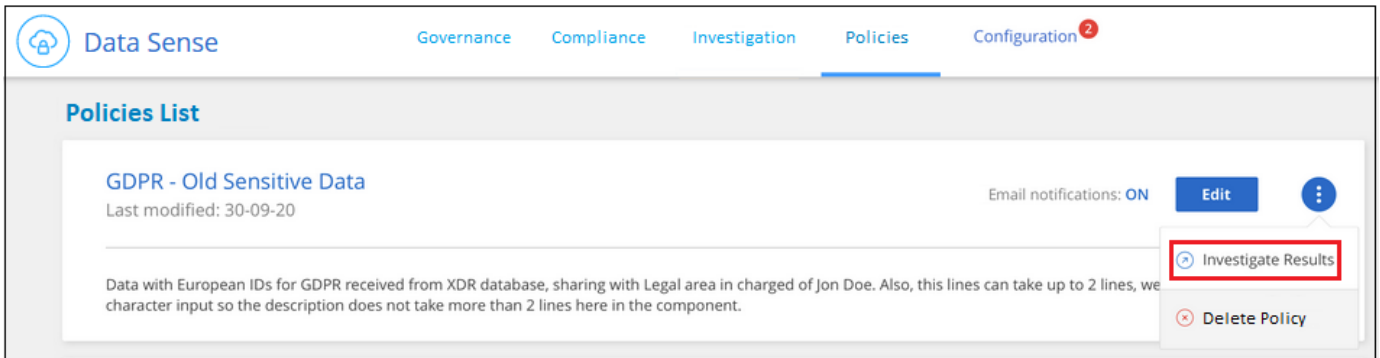
The **Policies** tab in the Compliance Dashboard lists all the predefined and custom Policies available on this instance of Cloud Data Sense.



In addition, Policies appear in the list of Filters in the Investigation page.

## Viewing Policy results in the Investigation page

To display the results for a Policy in the Investigation page, click the  button for a specific Policy, and then select **Investigate Results**.



## Creating custom Policies

You can create your own custom Policies that provide results for searches specific to your organization.

### Steps

1. From the Data Investigation page, define your search by selecting all the filters you want to use. See [Filtering data in the Data Investigation page](#) for details.
2. Once you have all the filter characteristics just the way you want them, click **Create Policy from this search**.



3. Name the Policy and select other actions that can be performed by the Policy:
  - a. Enter a unique name and description.
  - b. Optionally, check the box if you want notification emails sent to Cloud Manager users, and choose the interval at which the email is sent.
  - c. Optionally, check the box to automatically assign AIP labels to files that match the Policy parameters, and select the label. (Only if you have already integrated AIP labels. Learn more about [AIP labels](#).)
  - d. Click **Create Policy**.

## Create Policy

This will create a new Policy according to the current selected filters and search term. You can view or delete this later from the "Policies" tab.

Note it may take up to 15 minutes for results to be displayed for a new Policy.

Name this Policy

New Policy to view all files that were created over 60 days ago

Give it a detailed description that explains what it searches for

See if any files greater than 60 days old should be deleted from the file system.

☒ Send email updates about this Policy to Cloud Manager users on this account every 

Day

☐ Automatically label this Policy's matches with: 

Select a label

Create PolicyCancel

### Result

The new Policy appears in the Policies tab.

## Editing Policies

You can modify certain parts of a Policy depending on the type of Policy:

- Custom Policies - You can modify the *Name*, the *Description*, whether email notifications are sent, and whether AIP labels are added.
- Predefined Policies - You can modify only whether email notifications are sent and whether AIP labels are added.



If you need to change the filter parameters for a custom Policy, you'll need to create a new Policy with the parameters you want, and then delete the old Policy.

To modify a Policy, click the **Edit** button, enter your changes on the *Edit Policy* page, and click **Save Policy**.

## Deleting Policies

You can delete any custom Policy that you created if you no longer need it. You can't delete any of the predefined Policies.

To delete a Policy, click the  button for a specific Policy, click **Delete Policy**, and then click **Delete Policy**

again in the confirmation dialog.

## Applying Status tags to manage your scanned files

You can add a Status to files that you want to mark for some type of follow-up. For example, you may have found some duplicate files and you want to delete one of them, but you need to check to see which one should be deleted. You could add a status of "Check to delete" to the file so you know this file requires some research and some type of future action.

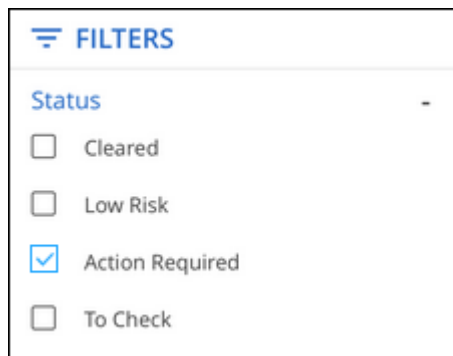
Data Sense enables you to view the Statuses that are assigned to files, add or remove a Status from files, and change the name or delete an existing Status.

Note that the Status is not added to the file in the same way as AIP Labels are part of the file metadata. The Status is just seen by Cloud Manager users using Cloud Data Sense so you can see if a file needs to be deleted, or checked for some type of follow-up.

### Viewing Status tags assigned to your files

You can view all the files that have a specific Status assigned.

1. Click the **Investigation** tab from Cloud Data Sense.
2. In the Data Investigation page, click **Status** in the Filters pane and then select the required Status.




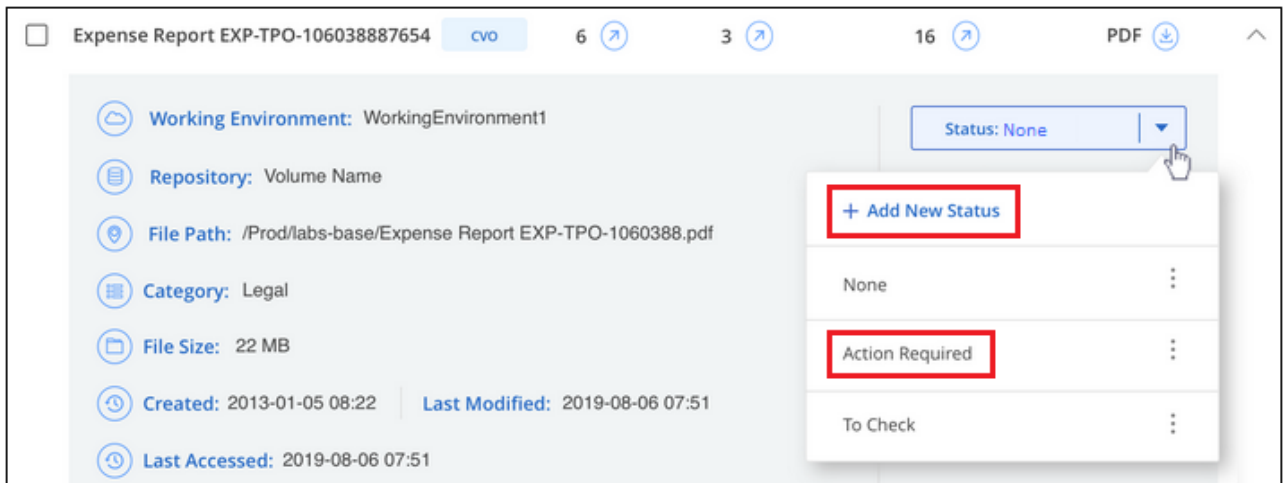
The Investigation Results pane lists all the files that have that Status assigned.

### Assigning a Status tag to files

You can add, change, and remove a Status tag from your files.


#### Steps

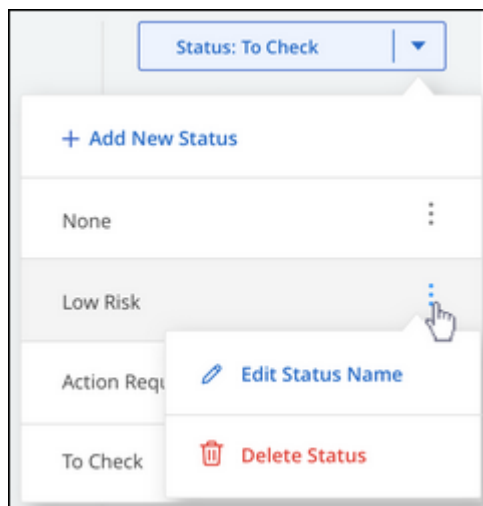
1. In the Data Investigation results pane, click  for the file to expand the file metadata details.
2. Click the **Status** field and assign a Status:
  - To assign an existing Status, click that Status. For example, "Action Required".
  - To create a new Status and assign it to the file, click **Add New Status**, enter the name of the new Status, and click **Done**.



The Status tag appears in the file metadata.

## Editing and deleting a Status tag

You can edit a Status tag to change the name, or you can delete a Status if you don't need to use it anymore. Click the  for an existing Status and click **Edit Status Name** or **Delete Status**.



When you change a Status name, it is changed for all files that were using the old name.

When you delete a Status tag, it is cleared from all files that were using the Status.

## Assigning users to manage certain files

You can assign a Cloud Manager user to a specific file so that person can be responsible for any follow-up actions that need to be done on the file. This capability is often used with the feature to add custom Status tags to a file.

For example, you might have a file that contains certain personal data that allows too many users read and write access (open permissions). So you could assign the Status tag "Change permissions" and assign this file to user "Joan Smith" so they can decide how to fix the issue. When they have fixed the issue they could change the Status tag to "Completed".

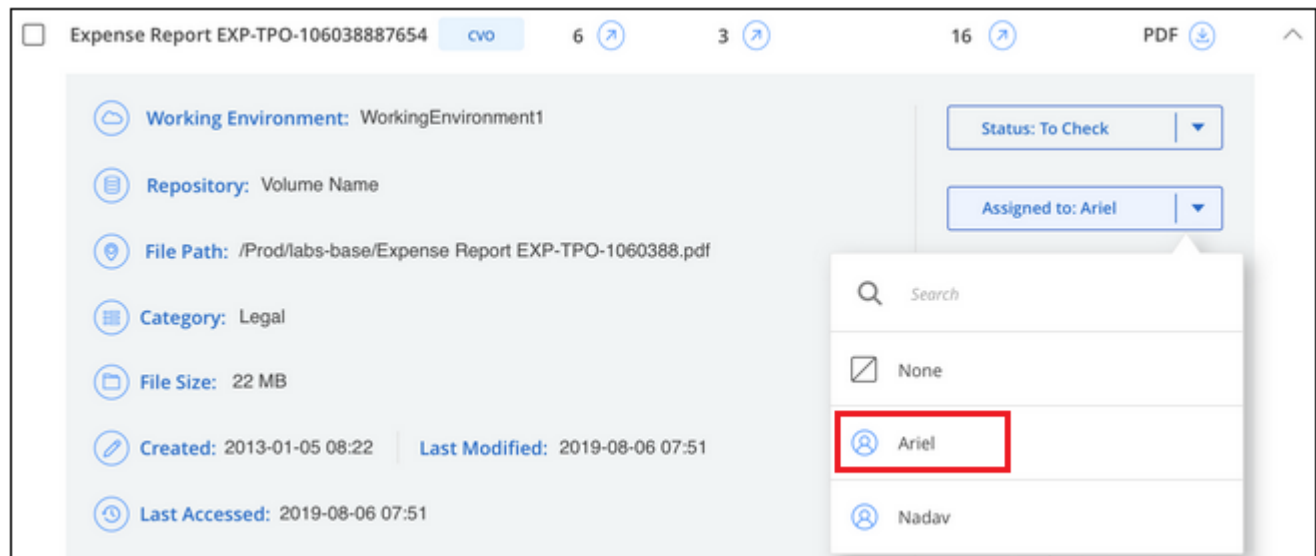
Note that the user name is not added to the file as part of the file metadata - it is just seen by Cloud Manager



users when using Cloud Data Sense.

### Steps

1. In the Data Investigation results pane, click ▼ for the file to expand the file metadata details.
2. Click the **Assigned to** field and select the user name.



The User name appears in the file metadata.

A new Filter in the Investigation page enables you to easily view all files that have the same person in the "Assigned To" field.

## Categorizing your data using AIP labels

You can manage AIP labels in the files that Cloud Data Sense is scanning if you have subscribed to [Azure Information Protection \(AIP\)](#). AIP enables you to classify and protect documents and files by applying labels to content. Data Sense enables you to view the labels that are already assigned to files, add labels to files, and change labels when a label already exists.

Cloud Data Sense supports AIP labels within the following file types: .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX.

Note that you can't currently change labels in files larger than 30 MB. For OneDrive accounts the maximum file size is 4 MB.



If a file has a label which doesn't exist anymore in AIP, Cloud Data Sense considers it as a file without a label.

### Integrating AIP labels in your workspace

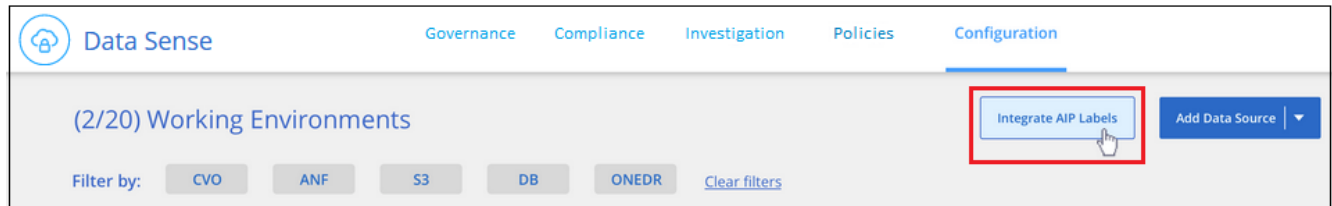
Before you can manage AIP labels, you need to integrate the AIP label functionality into Cloud Data Sense by signing into your existing Azure account. Once enabled, you can manage AIP labels within files for all [working environments and data sources](#) in your Cloud Manager workspace.

### Requirements

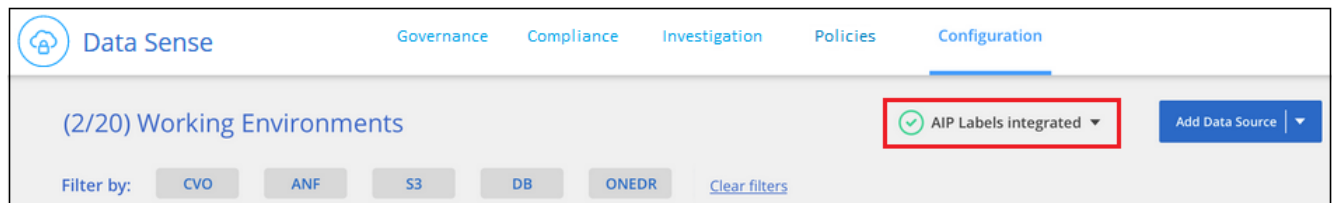
- You must have an account and an Azure Information Protection license.
- You must have the login credentials for the Azure account.
- If you plan to change labels in files that reside in Amazon S3 buckets, ensure that the permission `s3:PutObject` is included in the IAM role. See [setting up the IAM role](#).

## Steps

1. From the Cloud Data Sense Configuration page, click **Integrate AIP Labels**.



2. In the Integrate AIP Labels dialog, click **Sign in to Azure**.
3. In the Microsoft page that appears, select the account and enter the required credentials.
4. Return to the Cloud Data Sense tab and you'll see the message *"AIP Labels were integrated successfully with the account <account\_name>"*.
5. Click **Close** and you'll see the text *AIP Labels integrated* at the top of the page.



## Result

You can view and assign AIP labels from the results pane of the Investigation page. You can also assign AIP labels to files using Policies.

## Viewing AIP labels in your files

You can view the current AIP label that is assigned to a file.

In the Data Investigation results pane, click  for the file to expand the file metadata details.

Unstructured (32K Files)

Structured (323 DB Tables)

🔍

⬇

File Name		Personal	Sensitive Personal	Data Subjects	File Type	
Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF	⌵
Expense Report EXP-TPO-10603888765435	cvo	6 ⚙	3 ⚙	16 ⚙	PDF ⚙	⬅

☁

Working Environment: WorkingEnvironment1

📄

Repository: Volume Name

Label:

Finance

⌵

## Assigning AIP labels manually

You can add, change, and remove AIP labels from your files using Cloud Data Sense.

Follow these steps to assign an AIP label to a single file.

### Steps

1. In the Data Investigation results pane, click  for the file to expand the file metadata details.

Unstructured (32K Files)		Structured (323 DB Tables)							
File Name		Personal	Sensitive Personal	Data Subjects	File Type				
Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF				
Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF				
Working Environment: WorkingEnvironment1		Assign a Label to this file							
Repository: Volume Name		<div> <div>General</div> <div>Finance</div> <div>Confidential</div> </div>							
File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf									
Category: Legal									
File Size: 22 MB									
Last Modified: 2019-08-06 07:51									
Open Permissions: NO OPEN PERMISSIONS		View all Permissions							
File Owner: Assaf Vol									

2. Click **Assign a Label to this file** and then select the label.

The label appears in the file metadata.

# Assigning AIP labels automatically with Policies

You can assign an AIP label to all the files that meet the criteria of the Policy. You can specify the AIP label when creating the Policy, or you can add the label when editing any Policy.

Labels are added or updated in files continuously as Cloud Data Sense scans your files.

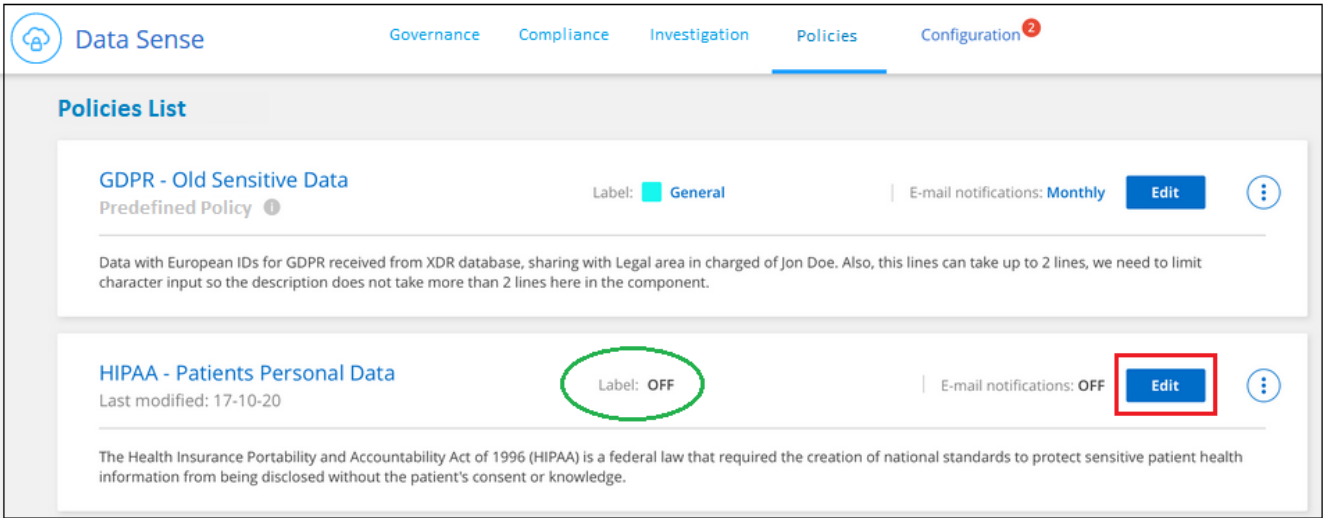
Depending on whether a label is already applied to a file, and the classification level of the label, the following actions are taken when changing a label:

If the file...	Then...
Has no label	The label is added
Has an existing label of a lower level of classification	The higher level label is added
Has an existing label of a higher level of classification	The higher level label is retained
Is assigned a label both manually and by a Policy	The higher level label is added
Is assigned two different labels by two Policies	The higher level label is added

Follow these steps to add an AIP label to an existing Policy.

## Steps

1. From the Policies List page, click **Edit** for the Policy where you want to add (or change) the AIP label.



2. In the Edit Policy page, check the box to enable automatic labels for files that match the Policy parameters, and select the label (for example, **General**).

3. Click **Save Policy** and the label appears in the Policy description.



If a Policy was configured with a label, but the label has since been removed from AIP, the label name is turned to OFF and the label is not assigned anymore.

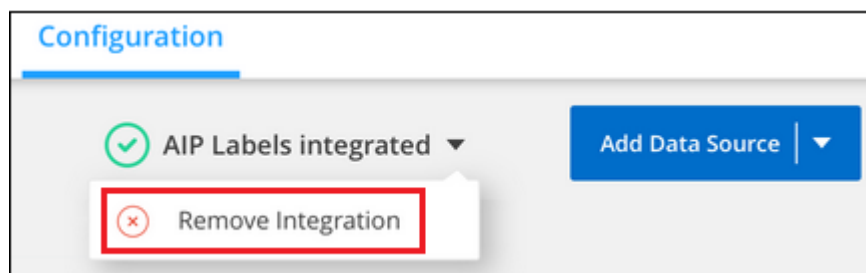
## Removing the AIP integration

If you no longer want the ability to manage AIP labels in files, you can remove the AIP account from the Cloud Data Sense interface.

Note that no changes are made to the labels you have added using Data Sense. The labels that exist in files will stay as they currently exist.

### Steps

1. From the *Configuration* page, click **AIP Labels integrated > Remove Integration**.



2. Click **Remove Integration** from the confirmation dialog.

## Sending email alerts when non-compliant data is found

Cloud Data Sense can send email alerts to Cloud Manager users when certain critical Policies return results so

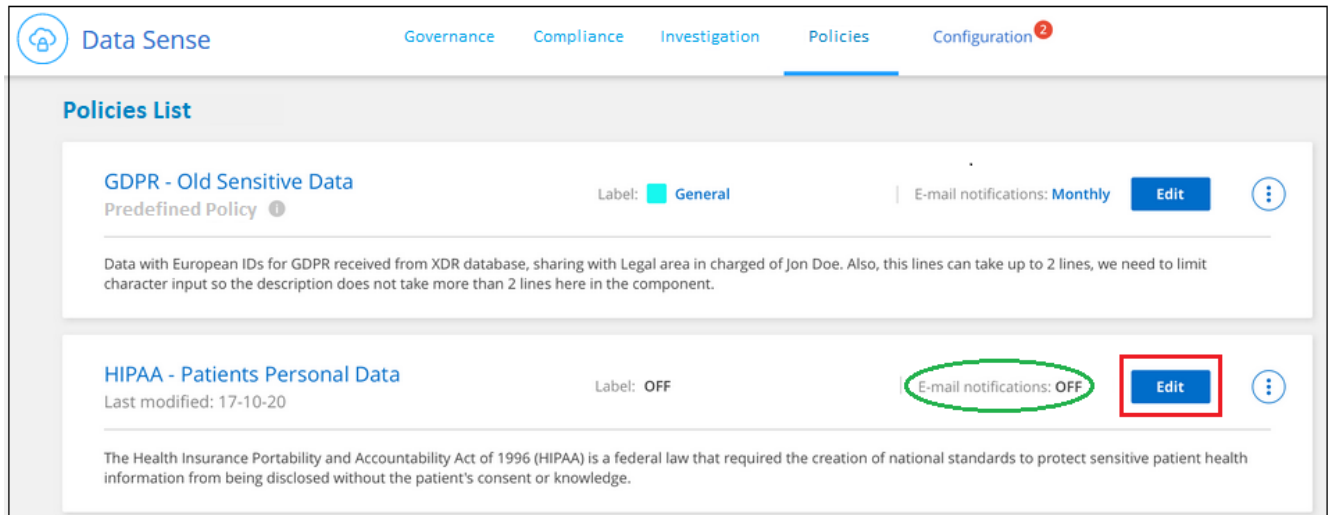
you can get notifications to protect your data. You can choose to send the email notifications on a daily, weekly, or monthly basis.

You can configure this setting when creating the Policy or when editing any Policy.

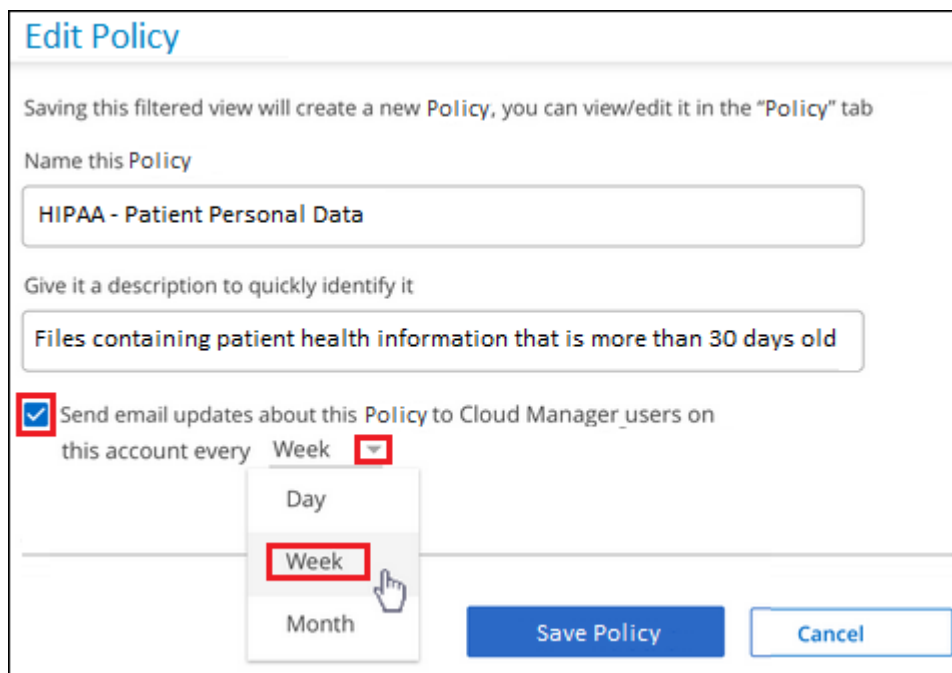
Follow these steps to add email updates to an existing Policy.

### Steps

1. From the Policies List page, click **Edit** for the Policy where you want to add (or change) the email setting.



2. In the Edit Policy page, check the box if you want notification emails sent to Cloud Manager users, and choose the interval at which the email is sent (for example, every **Week**).



3. Click **Save Policy** and the interval at which the email is sent appears in the Policy description.

### Result

The first email is sent now if there are any results from the Policy - but only if any files meet the Policy criteria.

No personal information is sent in the notification emails. The email indicates that there are files that match the Policy criteria, and it provides a link to the Policy results.

## Deleting source files

You can permanently remove source files that seem insecure or too risky to leave in your storage system, or that you have identified as a duplicate. This action is permanent and there is no undo.



You can't delete files that reside in databases or files that reside in volume Backups.

### Requirements

You must have the Account Admin or Workspace Admin role to delete files.

Deleting files requires the following permissions:

- For NFS data – the export policy needs to be defined with write permissions.
- For CIFS data – the CIFS credentials need to have write permissions.
- For S3 data - the IAM role must include the following permission: `s3:DeleteObject`

### Steps

1. In the Data Investigation results pane, select the file, or files, that you want to delete and click **Delete** from the button bar.

2345 items		Move  Delete				
<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF

- To select all files on the current page, check the box in the title row (☒ File Name). (You can't select files from more than one page.)
  - To select individual files, check the box for each file (☒ Volume\_1).
2. Because the delete operation is permanent, you must type "**permanently delete**" in the subsequent *Delete File* dialog and click **Delete File**.

Note that you can also delete an individual file when viewing the metadata details for a file. Just click **Delete this file**.

Unstructured (32K Files)

Structured (323 DB Tables)

File Name

Personal

Sensitive Personal

Data Subjects

File Type

<input type="checkbox"/>	Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-10603888765435	cvo	6	3	16	PDF	◀

Working Environment: WorkingEnvironment1

Repository: Volume Name

File Path: /Prod/labs-base/Expense Report EXP-TPO-1060388.pdf

Assign a Label to this file

Delete this file

## Moving source files to an NFS share

You can move source files that Data Sense is scanning to any NFS share. The NFS share does not need to be integrated with Data Sense (see [Scanning file shares](#)).



You can't move files that reside in databases or files that reside in volume Backups.

### Requirements

You must have the Account Admin or Workspace Admin role to move files.

Moving files requires that the NFS share allows access from the Data Sense instance.

### Steps

- In the Data Investigation results pane, select the file, or files, that you want to move and click **Move** from the button bar.

2345 items

Move

Delete

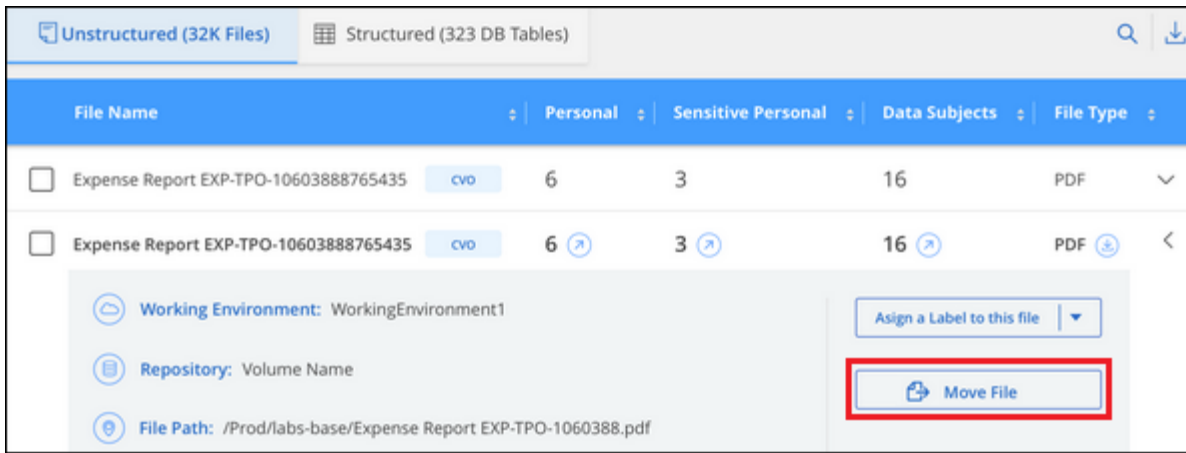
<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input checked="" type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	6	PDF	▼

- To select all files on the current page, check the box in the title row (☒ File Name). (You can't select files from more than one page.)
- To select individual files, check the box for each file (☒ Volume\_1).

- In the *Move File* dialog, enter the name of the NFS share where all selected files will be moved in the format `<host_name>:/<share_path>`, and click **Move File**.

Note that you can also move an individual file when viewing the metadata details for a file. Just click **Move file**.





## List of predefined Policies

Cloud Data Sense provides the following system-defined Policies:

Name	Description	Logic
S3 publicly-exposed private data	S3 Objects containing personal or sensitive personal information, with open Public read access.	(S3 Public) AND contains personal OR sensitive personal info)
PCI DSS – Stale data over 30 days	Files containing Credit Card information, last modified over 30 days ago.	Contains credit card AND last modified over 30 days
HIPAA – Stale data over 30 days	Files containing Health information, last modified over 30 days ago.	Contains health data (defined same way as in HIPAA report) AND last modified over 30 days
Private data – Stale over 7 years	Files containing personal or sensitive personal information, last modified over 7 years ago.	Files containing personal or sensitive personal information, last modified over 7 years ago
GDPR – European citizens	Files containing more than 5 identifiers of an EU country's citizens or DB Tables containing identifiers of an EU country's citizens.	Files containing over 5 identifiers of an (one) EU citizens or DB Tables containing rows with over 15% of columns with one country's EU identifiers. (any one of the national identifiers of the European countries. Does not include Brazil, California, USA SSN, Israel, South Africa)
CCPA – California residents	Files containing over 10 California Driver's License identifiers or DB Tables with this identifier.	Files containing over 10 California Driver's License identifiers OR DB Tables containing California Driver's license
Data Subject names – High risk	Files with over 50 Data Subject names.	Files with over 50 Data Subject names
Email Addresses – High risk	Files with over 50 Email Addresses, or DB Columns with over 50% of their rows containing Email Addresses	Files with over 50 Email Addresses, or DB Columns with over 50% of their rows containing Email Addresses

Name	Description	Logic
Personal data – High risk	Files with over 20 Personal data identifiers, or DB Columns with over 50% of their rows containing Personal data identifiers.	Files with over 20 personal, or DB Columns with over 50% of their rows containing personal
Sensitive Personal data – High risk	Files with over 20 Sensitive Personal data identifiers, or DB Columns with over 50% of their rows containing Sensitive Personal data.	Files with over 20 sensitive personal, or DB Columns with over 50% of their rows containing sensitive personal

## Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.