



Managing your private data

Cloud Manager

Tom Onacki
February 09, 2021

Table of Contents

- Managing your private data 1
 - Controlling your data using Highlights 1
 - Categorizing your data using AIP labels 4
 - Sending email alerts when non-compliant data is found 8
 - Deleting source files 9

Managing your private data

Cloud Compliance 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 "highlight" 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 highlights return results.
- If you are subscribed to [Azure Information Protection \(AIP\)](#) to classify and protect your files, you can use Cloud Compliance to manage those AIP labels.
- You can delete files that seem insecure or too risky to leave in your storage system.

See below for more functionality that is provided with both the highlights and AIP features.

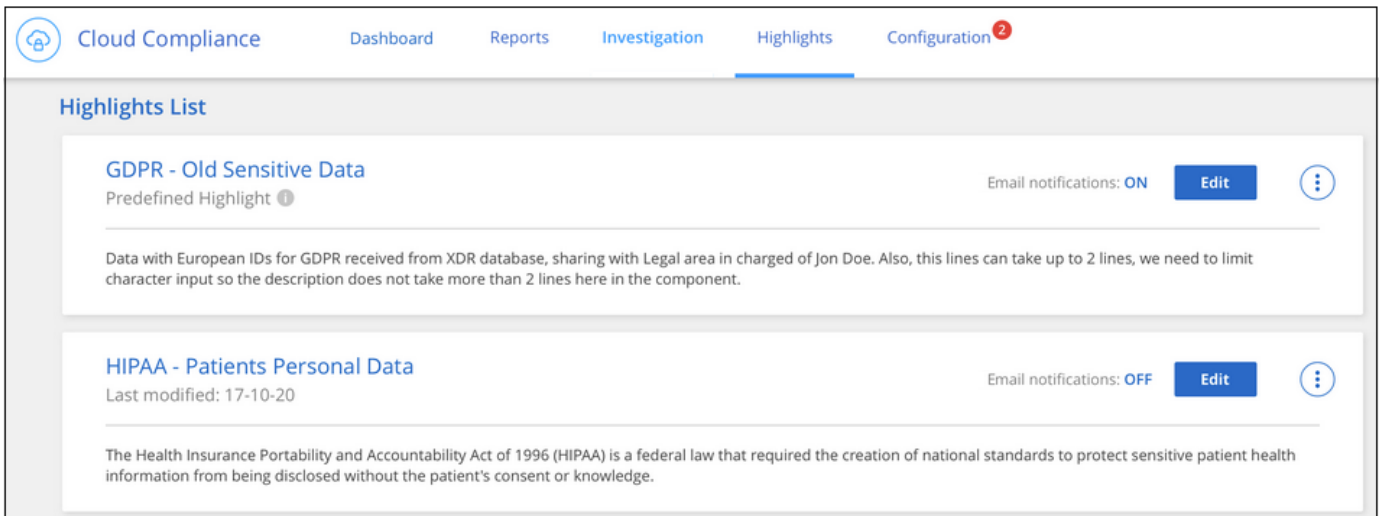
Controlling your data using Highlights

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

Highlights provide the following functionality:

- [Predefined highlights](#) from NetApp based on user requests
- Ability to create your own custom highlights
- Launch the Investigation page with the results from your highlights in one click
- Send email alerts to Cloud Manager users when certain critical highlights 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 highlight

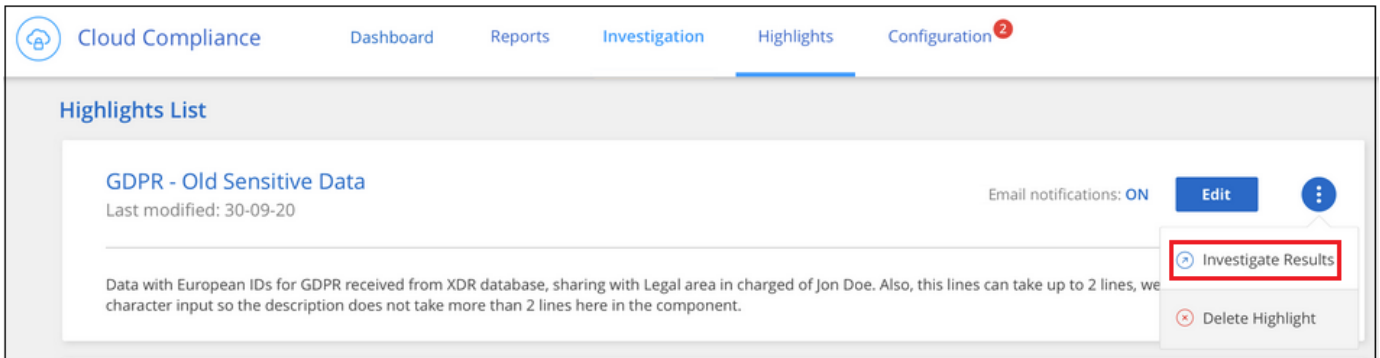
The **Highlights** tab in the Compliance Dashboard lists all the Highlights available on this instance of Cloud Compliance.



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

Viewing highlights results in the Investigation page

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



Creating custom highlights

You can create your own custom highlights 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 **Save this search as a Highlight**.

Data Investigation

FILTERS

Clear All

Search filters

×

Highlights

+

Working Environment

4

+

Storage Repository

+

Category

+

Private Data

6

+

File Type

+

Save this search as a Highlight

3. Name the highlight and select other actions that can be performed by the highlight:
 - 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 highlight parameters, and select the label. (Learn more about [AIP labels](#).)
 - d. Click **Create Highlight**.

Create Highlight

Saving this filtered view will create a new Highlight, you can view/edit it in the "Highlights" tab

Name this Highlight

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

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

Week

☐ Automatically label matches of this Highlight with:

select label

Create Highlight

Cancel

Result

The new highlight appears in the Highlights tab.

Editing highlights

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

- Custom highlights - You can modify the *Name*, the *Description*, whether email notifications are sent, and whether AIP labels are added.
- Predefined highlights - 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 highlight, you'll need to create a new highlight with the parameters you want, and then delete the old highlight.

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

Deleting highlights

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

To delete a highlight, click the  button for a specific highlight, click **Delete Highlight**, and then click **Delete Highlight** again in the confirmation dialog.

Categorizing your data using AIP labels

You can manage AIP labels in the files that Cloud Compliance 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. Cloud Compliance 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 Compliance support AIP labels within the following file types: .PDF, .DOCX, .DOC, .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 Compliance 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 Compliance 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 current Cloud Manager workspace.

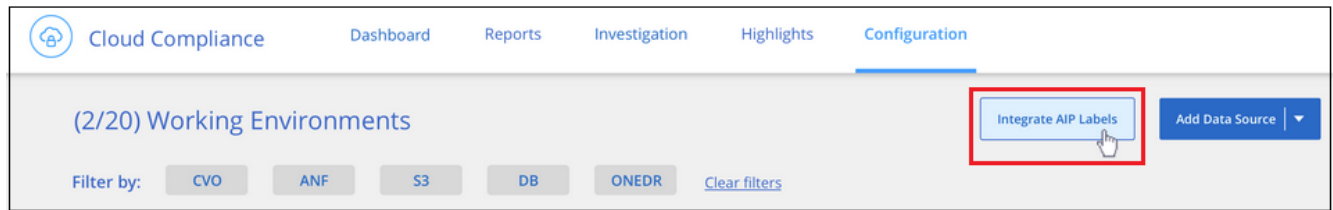
Requirements

- You must have an account and an Azure Information Protection license.
- You must have the login credentials for the Azure account.

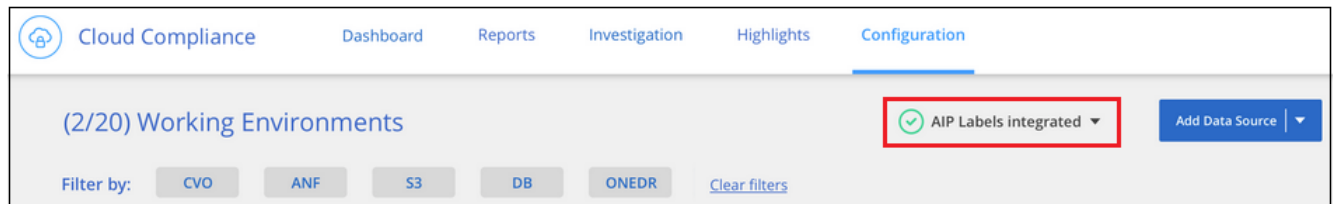
- If you plan to change labels in files that reside in Amazon S3 buckets, ensure that the permission `s3:PutObject` is included in the IAM role. See [setting up the IAM role](#).

Steps

1. From the Cloud Compliance 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 Compliance 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 highlights.

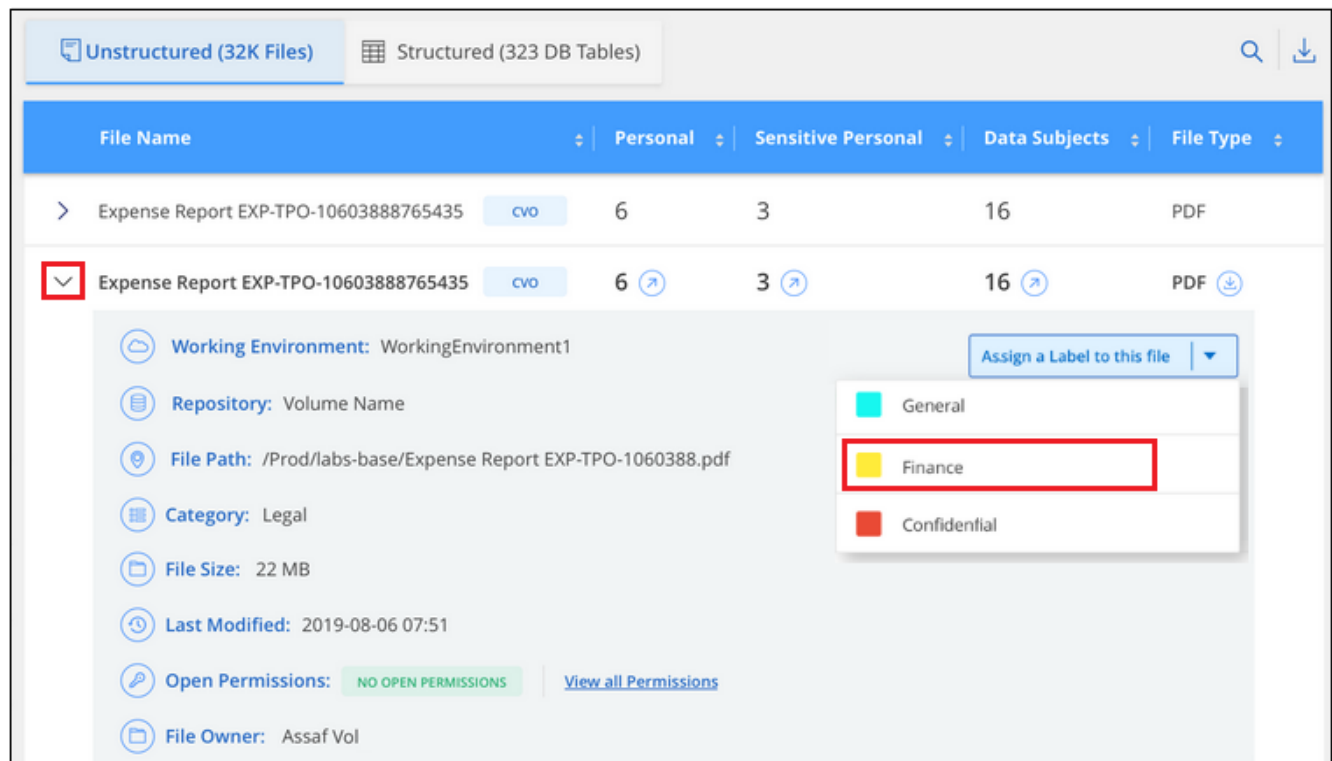
Assigning AIP labels manually

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

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.



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 highlights

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

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

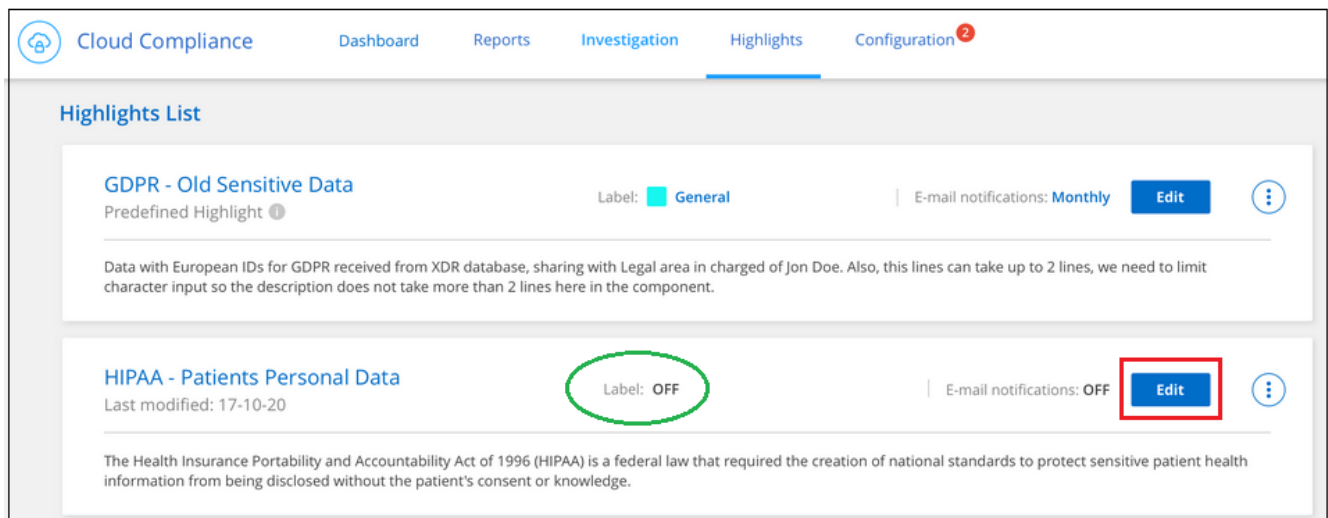
Depending on whether a label is already applied to a file, and the classification level of the label, the following actions are taken when changing a label:

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 highlight	The higher level label is added
Is assigned two different labels by two highlights	The higher level label is added

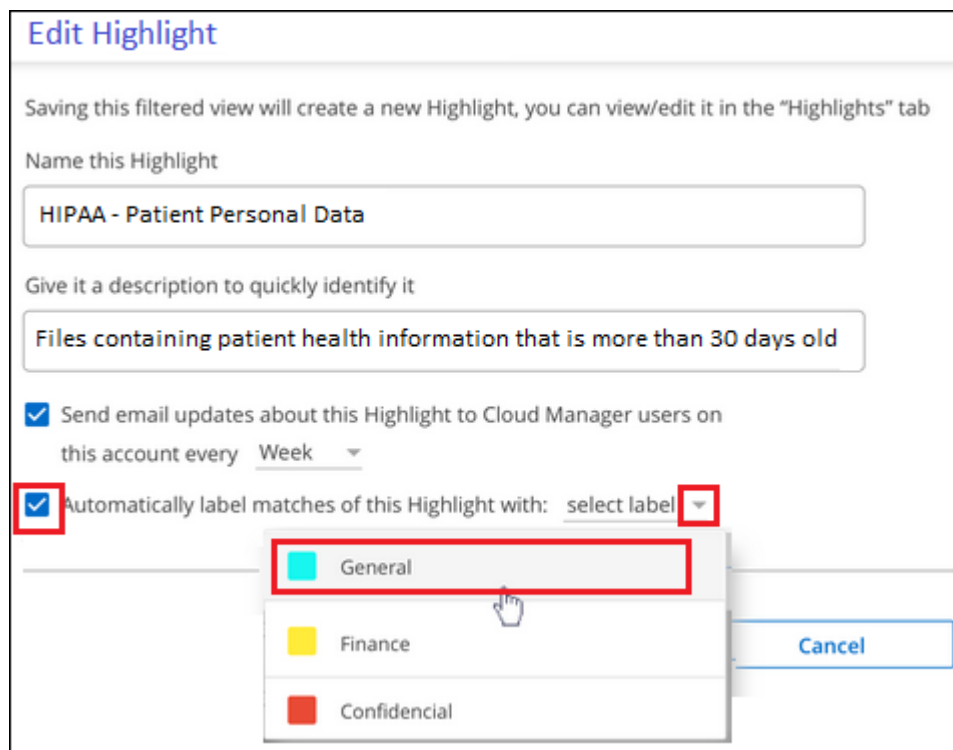
Follow these steps to add an AIP label to an existing highlight.

Steps

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



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



3. Click **Save Highlight** and the label appears in the highlight description.



If a highlight 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.

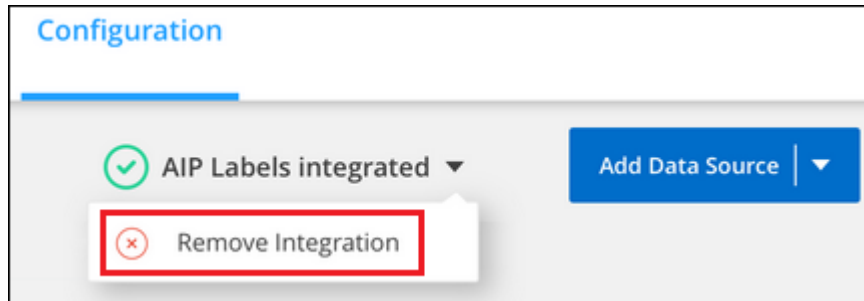
Removing the AIP integration

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

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

Steps

1. From the *Scan 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

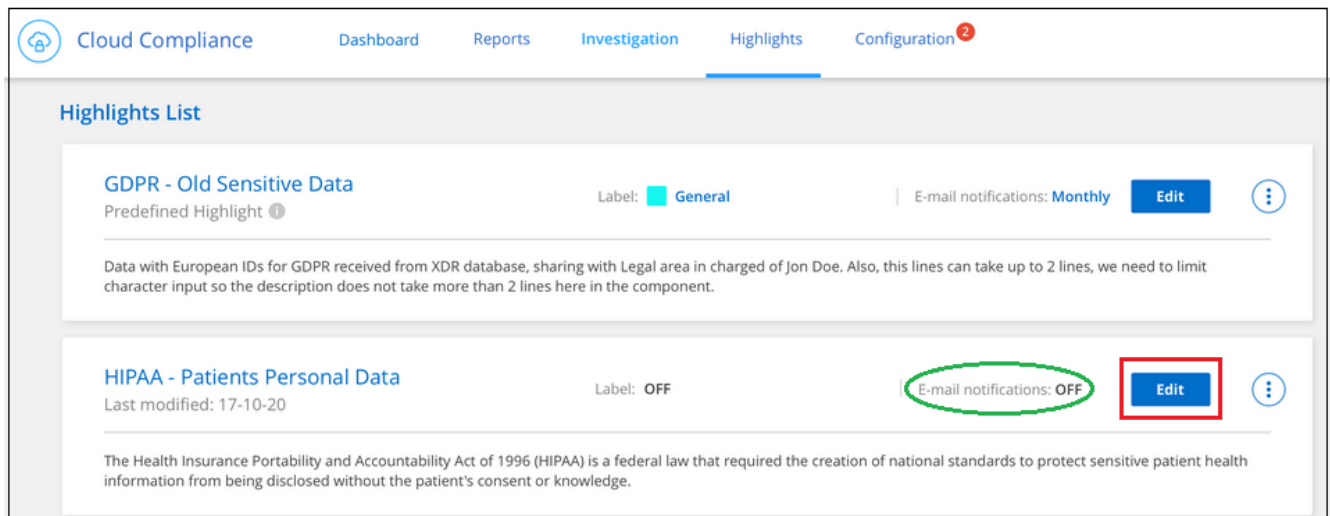
Cloud Compliance can send email alerts to Cloud Manager users when certain critical highlights return results so you can get notifications to protect your data. You can choose to send the email notifications on a daily, weekly, or monthly basis.

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

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

Steps

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



2. In the Edit Highlight 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, **Week**).

Edit Highlight

Saving this filtered view will create a new Highlight, you can view/edit it in the "Highlights" tab

Name this Highlight

HIPAA - Patient Personal Data

Give it a description to quickly identify it

Files containing patient health information that is more than 30 days old

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

Day

Week

Month

Save Highlight

Cancel

- Click **Save Highlight** and the interval at which the email is sent appears in the highlight description.

Result

The first email is sent now if there are any results from the highlight - but only if any files meet the highlight criteria. No personal information is sent in the notification emails. The email indicates that there are files that match the highlight criteria, and it provides a link to the highlight results.

Deleting source files

You can permanently remove source files that seem insecure or too risky to leave in your storage system. This action is permanent and there is no undo.



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

Steps

- 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-1060388765435	cvo 6	3	16	PDF
<input checked="" type="checkbox"/> Expense Report EXP-TPO-1060388765435	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

- Click **Delete this file**.

3. Because the delete operation is permanent, you must type "**permanently delete**" in the subsequent *Delete File* dialog and click **Delete File**.

List of predefined highlights

Cloud Compliance provides the following system-defined highlights:

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
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.