



Viewing details about the private data stored in your organization

Cloud Manager

Tom Onacki
February 08, 2021

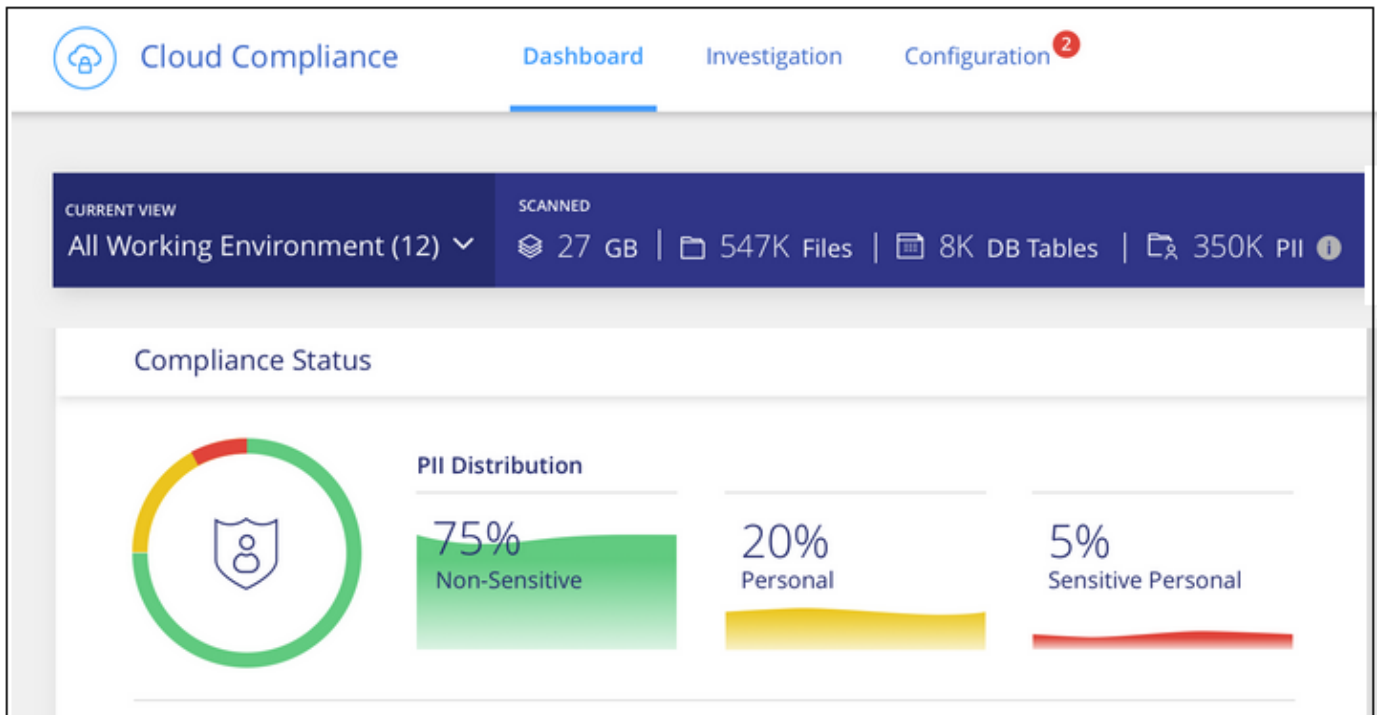
Table of Contents

- Viewing details about the private data stored in your organization 1
 - Personal data 1
 - Sensitive personal data 4
 - Categories 5
 - File types 6
 - Viewing file metadata and permissions 7
 - Viewing Dashboard data for specific working environments 8
 - Filtering data in the Data Investigation page 9
 - What’s included in each file list report (CSV file) 10

Viewing details about the private data stored in your organization

Gain control of your private data by viewing details about the personal data and sensitive personal data in your organization. You can also gain visibility by reviewing the categories and file types that Cloud Compliance found in your data.

By default, the Cloud Compliance dashboard displays compliance data for all working environments and databases.



If you want to see data for only some of the working environments, [select those working environments](#).

You can also filter the results from the Data Investigation page and download a report of the results as a CSV file. See [Filtering data in the Data Investigation page](#) for details.

Personal data

Cloud Compliance automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, Personal Identification Information (PII), credit card numbers, social security numbers, bank account numbers, and more. [See the full list](#).

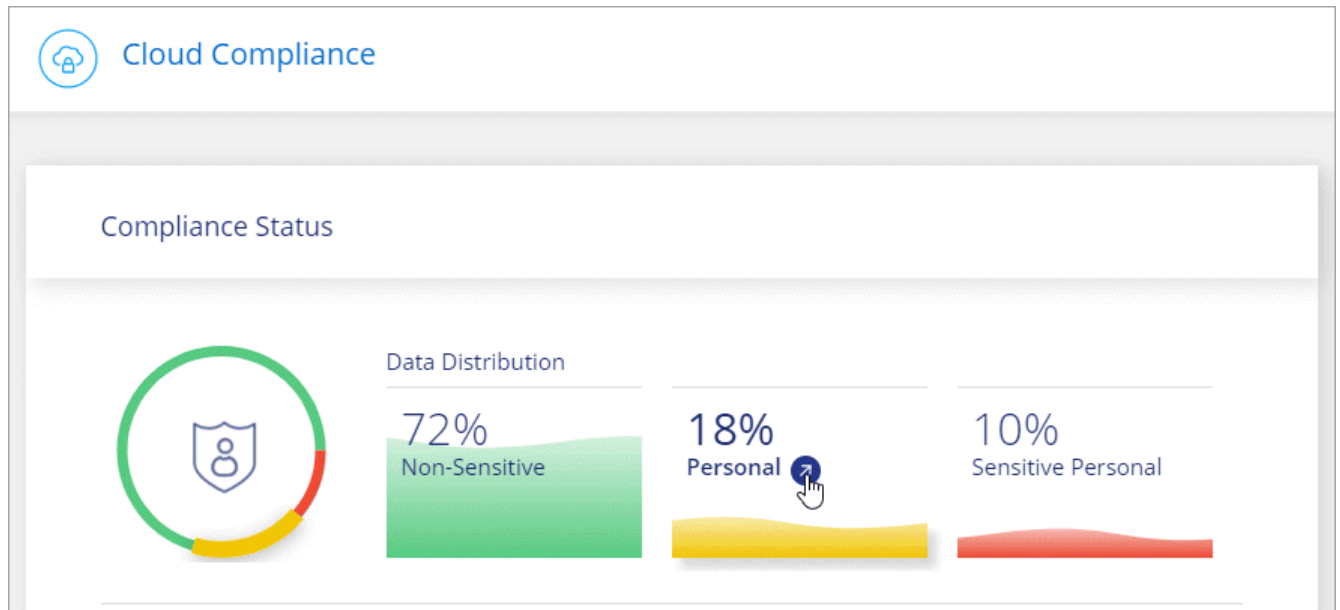
Additionally, if you have added a database server to be scanned, the *Data Fusion* feature allows you to scan your files to identify whether unique identifiers from your databases are found in those files or other databases. See [Adding personal data identifiers using Data Fusion](#) for details.

For some types of personal data, Cloud Compliance uses *proximity validation* to validate its findings. The validation occurs by looking for one or more predefined keywords in proximity to the personal data that was found. For example, Cloud Compliance identifies a U.S. social security number (SSN) as a SSN if it sees a proximity word next to it—for example, *SSN* or *social security*. [The table of personal data](#) shows when Cloud Compliance uses proximity validation.

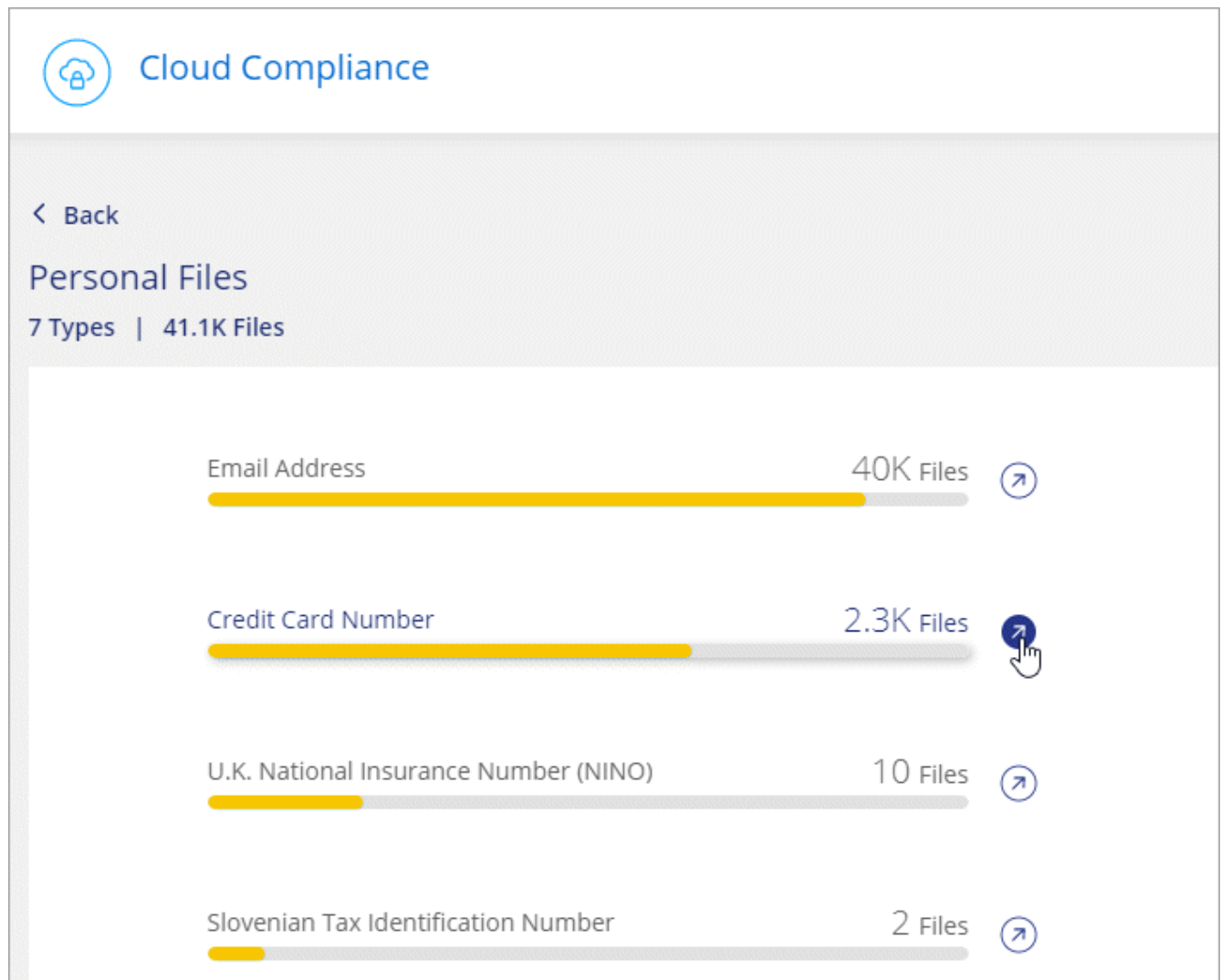
Viewing files that contain personal data

Steps

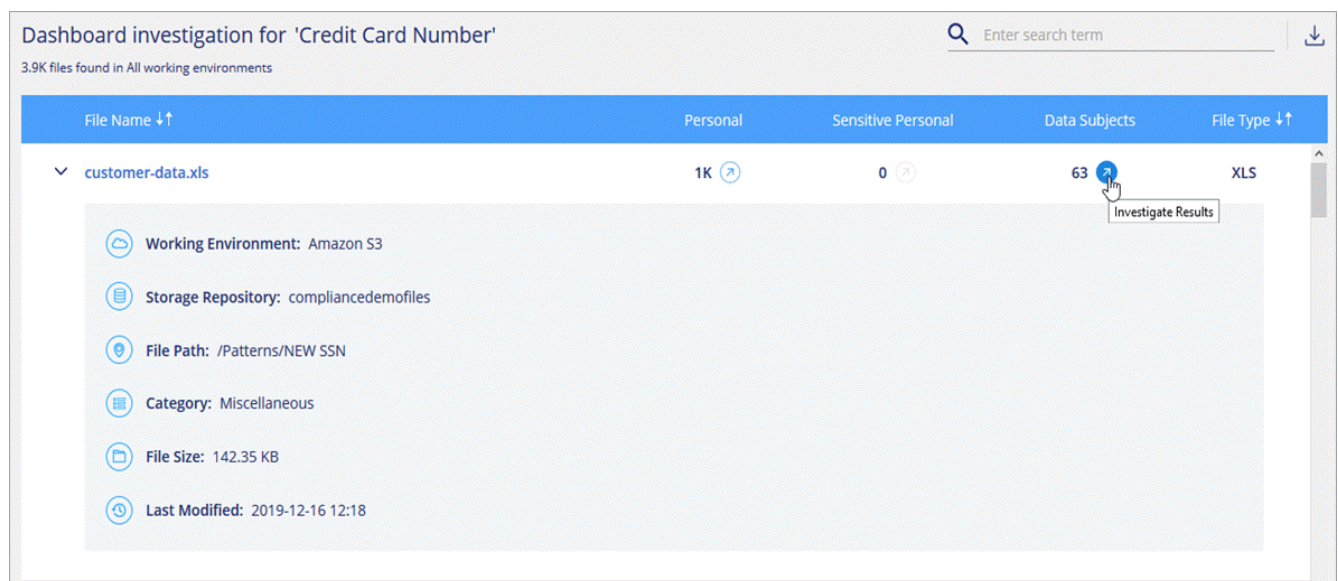
1. At the top of Cloud Manager, click **Compliance** and click the **Dashboard** tab.
2. To investigate the details for all personal data, click the icon next to the personal data percentage.



3. To investigate the details for a specific type of personal data, click **View All** and then click the **Investigate Results** icon for a specific type of personal data.



4. Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.



Sensitive personal data

Cloud Compliance automatically identifies special types of sensitive personal information, as defined by privacy regulations such as [articles 9 and 10 of the GDPR](#). For example, information regarding a person's health, ethnic origin, or sexual orientation. [See the full list](#).

Cloud Compliance uses artificial intelligence (AI), natural language processing (NLP), machine learning (ML), and cognitive computing (CC) to understand the meaning of the content that it scans in order to extract entities and categorize it accordingly.

For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, Cloud Compliance can distinguish the difference between a sentence that reads "George is Mexican" (indicating sensitive data as specified in article 9 of the GDPR), versus "George is eating Mexican food."

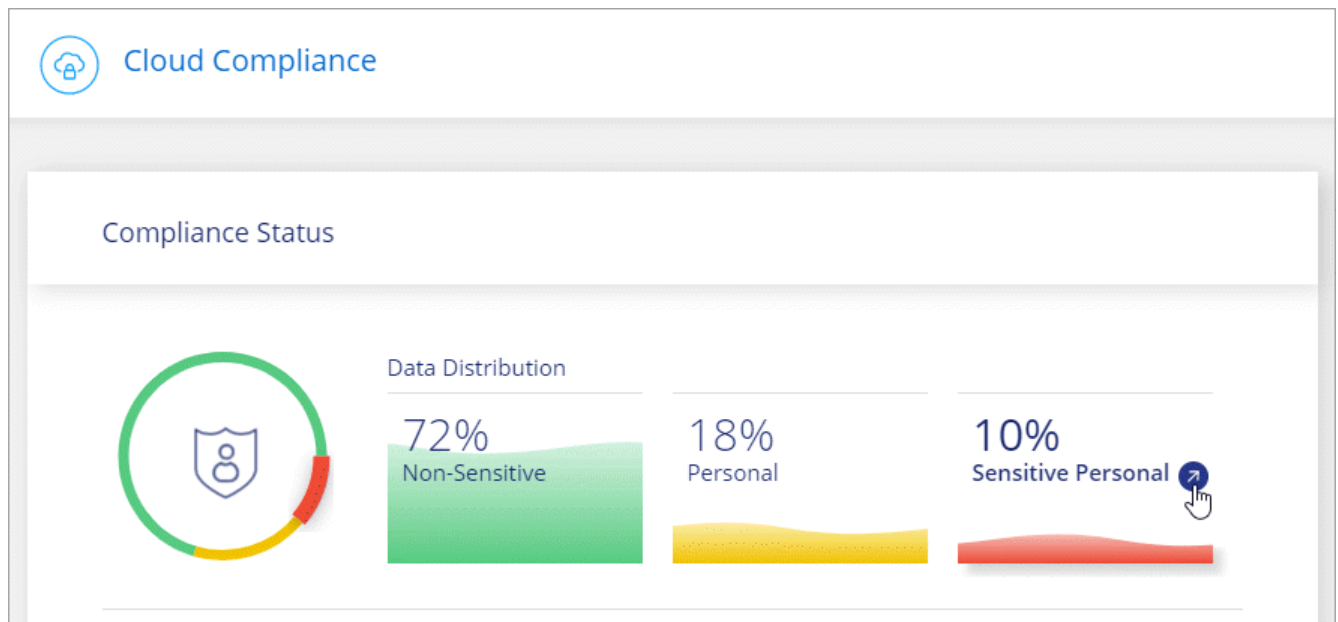


Only English is supported when scanning for sensitive personal data. Support for more languages will be added later.

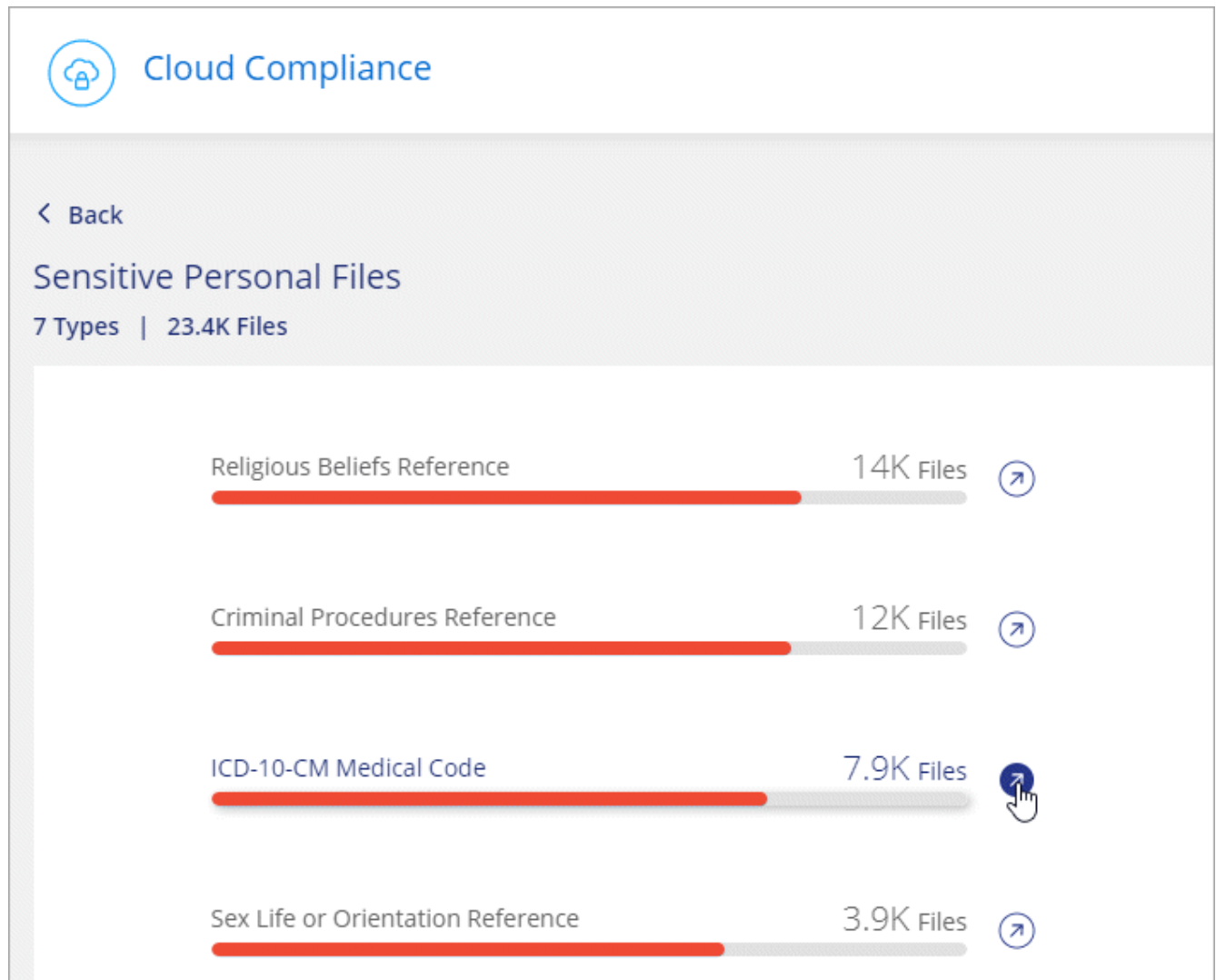
Viewing files that contain sensitive personal data

Steps

1. At the top of Cloud Manager, click **Compliance**.
2. To investigate the details for all sensitive personal data, click the icon next to the sensitive personal data percentage.



3. To investigate the details for a specific type of sensitive personal data, click **View All** and then click the **Investigate Results** icon for a specific type of sensitive personal data.



- Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

Categories

Cloud Compliance takes the data that it scanned and divides it into different types of categories. Categories are topics based on AI analysis of the content and metadata of each file. [See the list of categories.](#)

Categories can help you understand what's happening with your data by showing you the types of information that you have. For example, a category like resumes or employee contracts can include sensitive data. When you investigate the results, you might find that employee contracts are stored in an insecure location. You can then correct that issue.



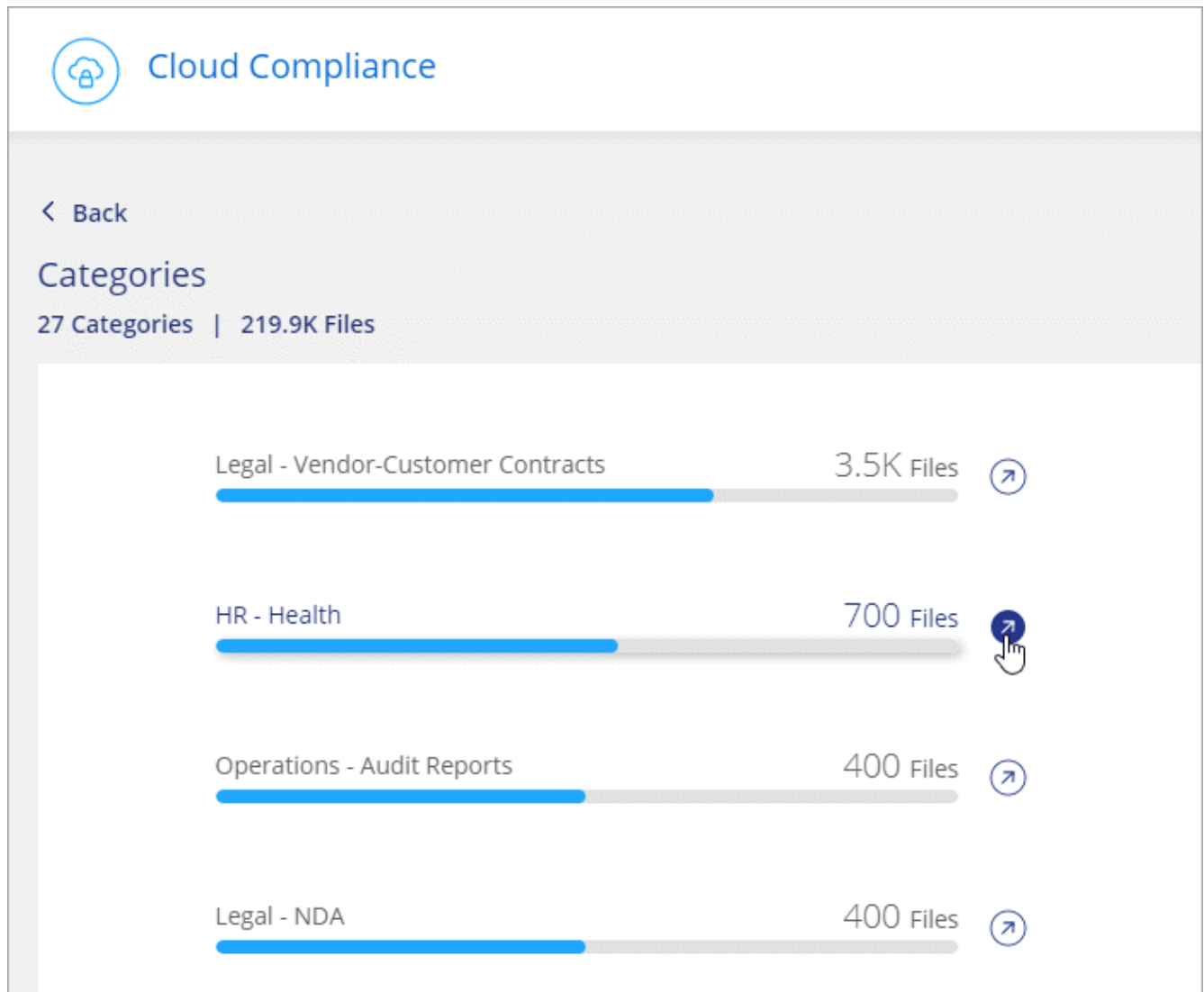
Only English is supported for categories. Support for more languages will be added later.

Viewing files by categories

Steps

- At the top of Cloud Manager, click **Compliance**.
- Click the **Investigate Results** icon for one of the top 4 categories directly from the main screen, or click

View All and then click the icon for any of the categories.



- Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

File types

Cloud Compliance takes the data that it scanned and breaks it down by file type. Reviewing your file types can help you control your sensitive data because you might find that certain file types are not stored correctly. [See the list of file types.](#)

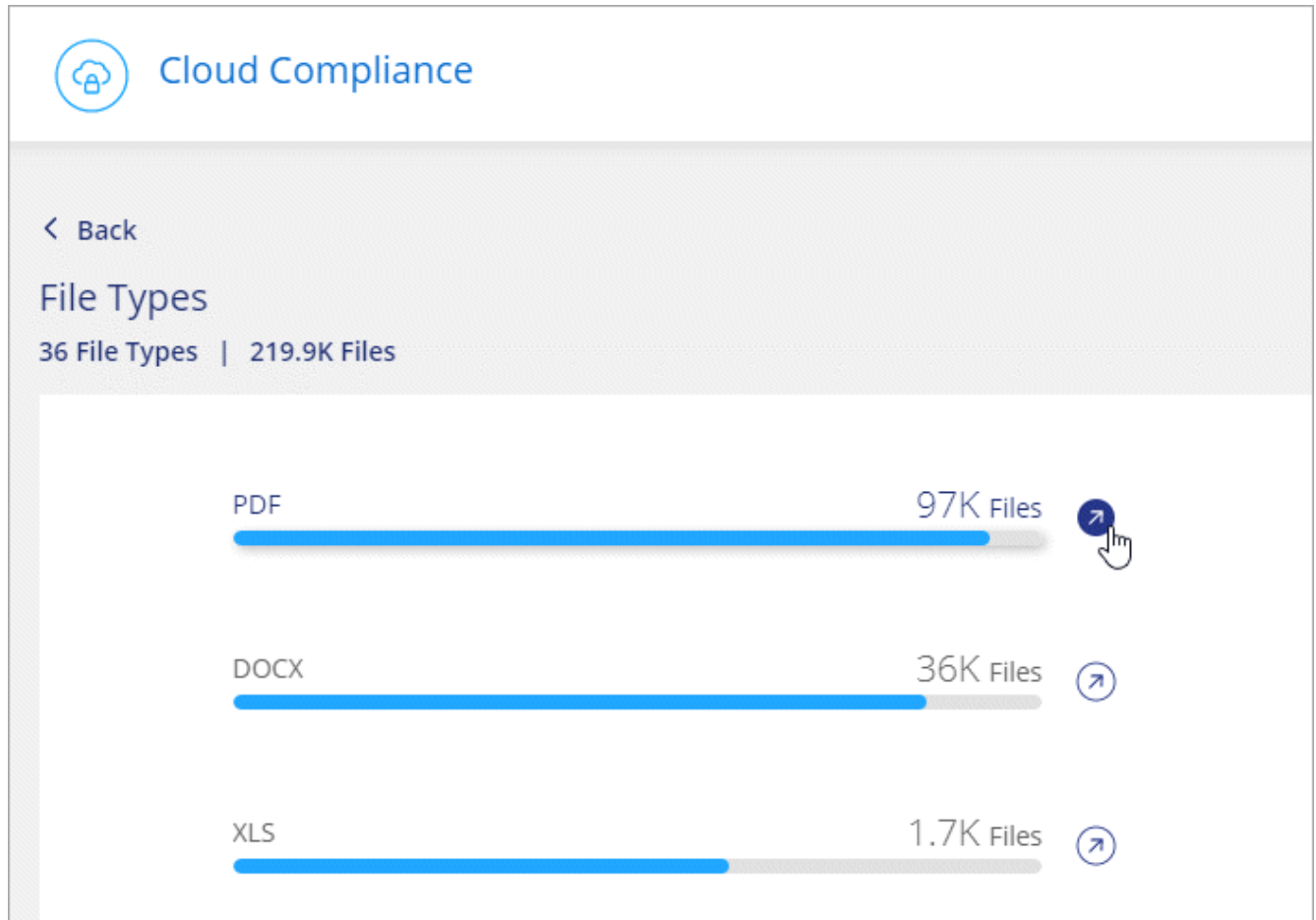
For example, you might be storing CAD files that include very sensitive information about your organization. If they are unsecured, you can take control of the sensitive data by restricting permissions or moving the files to another location.

Viewing file types

Steps

- At the top of Cloud Manager, click **Compliance**.
- Click the **Investigate Results** icon for one of the top 4 file types directly from the main screen, or click

View All and then click the icon for any of the file types.



- Investigate the data by searching, sorting, expanding details for a specific file, clicking **Investigate Results** to see masked information, or by downloading the file list.

Viewing file metadata and permissions

In the Data Investigation results pane you can click  for any single file to view the file metadata.

The screenshot displays the Cloud Compliance dashboard interface. At the top, there are tabs for 'Unstructured (32K Files)' and 'Structured (323 DB Tables)'. Below this is a header bar with filters for 'File Name', 'Personal', 'Sensitive Personal', 'Data Subjects', and 'File Type'. The main content area shows a list of files. The selected file, 'Expense Report EXP-TPO-10603888765435', is highlighted. Its metadata is shown in a detailed view below the list, including: Working Environment (WorkingEnvironment1), Repository (Volume Name), 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), and File Owner (Assaf Vol). On the right side of the metadata view, there are buttons for 'Assign a Label to this file' and 'Delete this file'. A link to 'Give feedback on this result' is also present at the bottom right of the metadata section.

In addition to showing you the working environment and volume where the file resides, the metadata shows much more information, including the file permissions, file owner, and assigned AIP label (if you have [integrated AIP in Cloud Compliance](#)). This information is useful if you're planning to create highlights because you can see all the information that you can use to filter your data.

Note that not all information is available for all data sources - just what is appropriate for that data source. For example, permissions and AIP labels are not relevant for database files.

There are also two items in this metadata that allow you to make changes to files:

- If you have integrated AIP labels with Cloud Compliance, you can assign a label to this file, or change to a different label if one already exists. See [Assigning AIP labels manually](#) for details.
- You can delete the file. See [Deleting source files](#) for details.

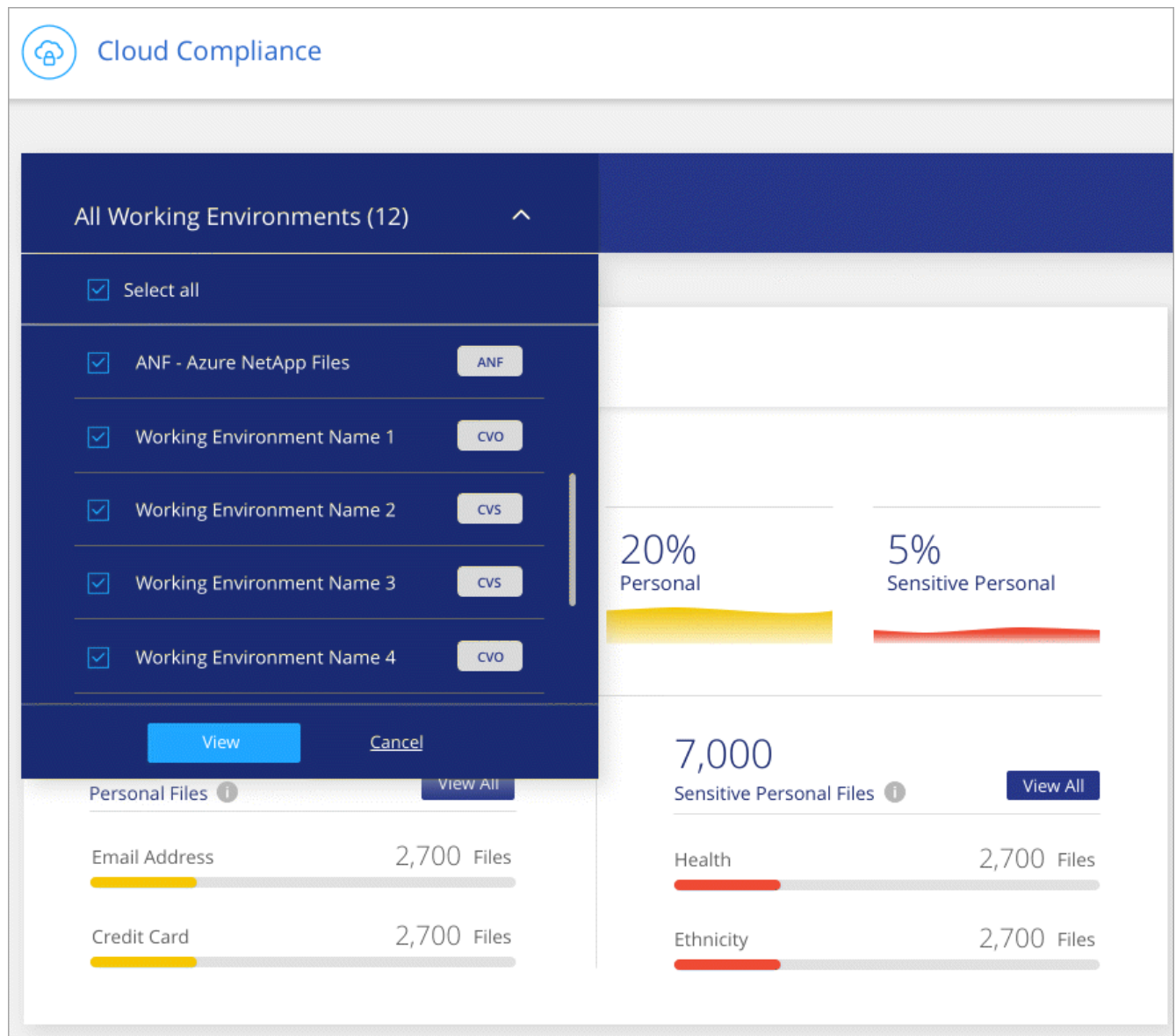
Viewing Dashboard data for specific working environments

You can filter the contents of the Cloud Compliance dashboard to see compliance data for all working environments and databases, or for just specific working environments.


When you filter the dashboard, Cloud Compliance scopes the compliance data and reports to just those working environments that you selected.

Steps

1. Click the filter drop-down, select the working environments that you'd like to view data for, and click **View**.




Filtering data in the Data Investigation page

You can filter the contents of the investigation page to display only the results you want to see. If you want to save a CSV version of the content as a report after you have refined it, click the  button.

Data Investigation		Unstructured (32K Files)		Structured (323 DB Tables)			
FILTERS		File Name	Personal	Sensitive Personal	Data Subjects	File Type	
Clear All		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Search filters		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Highlights		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Working Environment 4		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Storage Repository		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Category		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Private Data 6		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
File Type		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	

- The top-level tabs allow you to view data from files (unstructured data) or from databases (structured data).
- The controls at the top of each column allow you to sort the results in numerical or alphabetical order.
- The left-pane filters enable you to refine the results by working environment, storage repository, category, private data, file type, file size, last modified date, whether the S3 object's permissions are open to public access, etc...
- The *Highlights* filter at the top of the Filters pane lists the custom filters that provide commonly requested combinations of filters; like a saved database query or Favorites list. Go [here](#) to view the list of predefined highlights and to see how you can create your own custom highlights.

What's included in each file list report (CSV file)

From each Investigation page you can click the  button to download file lists (in CSV format) that include details about the identified files. If there are more than 10,000 results, only the top 10,000 appear in the list.

Each file list includes the following information:

- File name
- Location type
- Working environment
- Storage repository
- Protocol
- File path
- File type
- File size
- File owner
- Category
- Personal information
- Sensitive personal information
- Deletion detection date

A deletion detection date identifies the date that the file was deleted or moved. This enables you to identify when sensitive files have been moved. Deleted files aren't part of the file number count that appears in the dashboard or on the Investigation page. The files only appear in the CSV reports.

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.