Use Data Classification

NetApp Data Classification

NetApp
February 06, 2026

Table of Contents

Use Data Classification

View governance details about the data stored in your organization with NetApp Data Classification

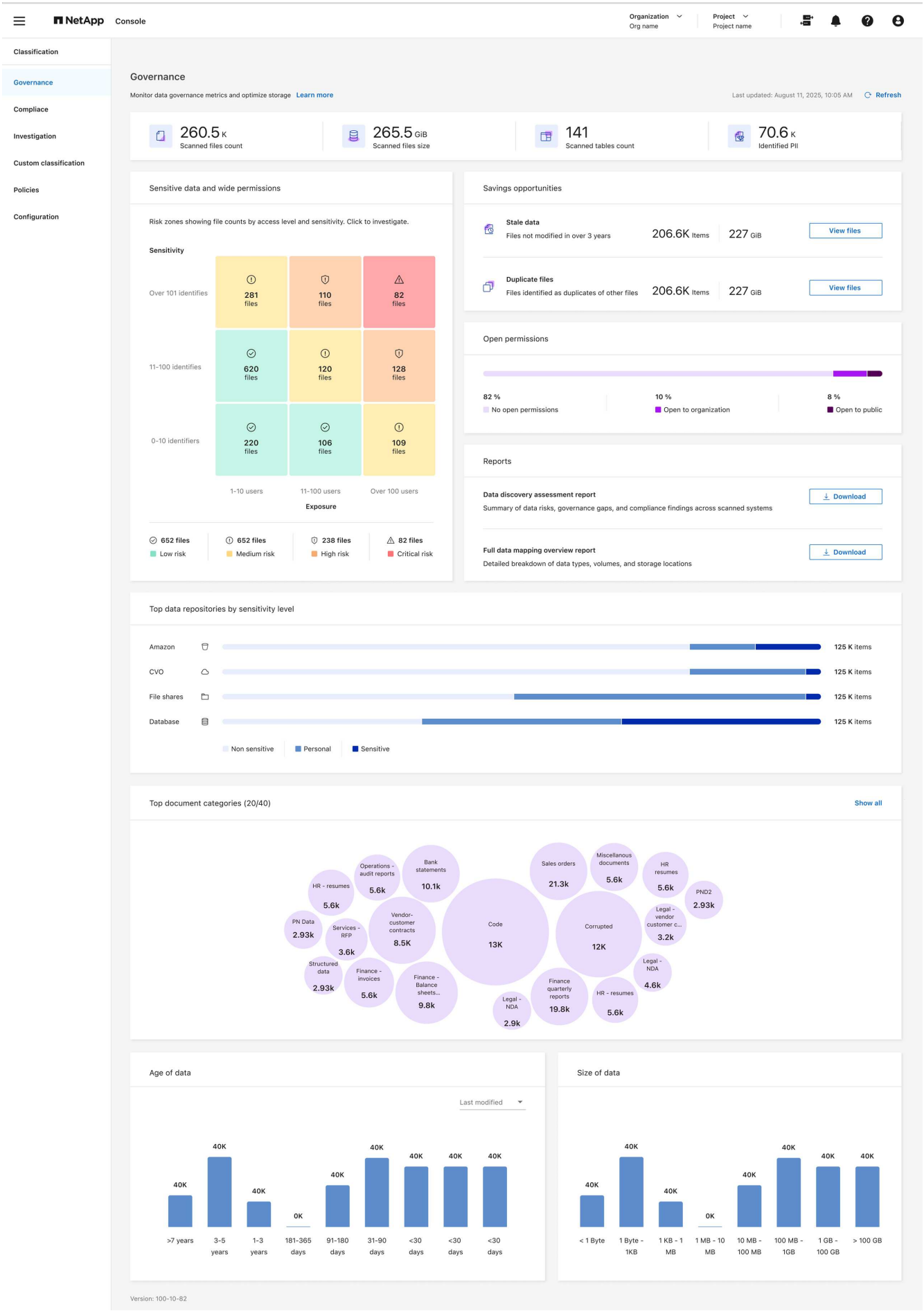
Gain control of the costs related to the data on your organization's storage resources. NetApp Data Classification identifies the amount of stale data, duplicate files, and very large files in your systems so you can decide whether you want to remove or tier some files to less expensive object storage.

This is where you should begin your research. From the Governance dashboard, you can select an area for further investigation.

Additionally, if you're planning to migrate data from on-premises locations to the cloud, you can view the size of the data and whether any of the data contains sensitive information before moving it.

Review the Governance dashboard

The Governance dashboard provides information so that you can increase the efficiency and control the costs related to the data stored on your storage resources.


NetApp Console
Organization
Org name
Project
Project name
Classification
Governance
Compliace
Investigation
Custom classification
Policies
Configuration
Governance
Monitor data governance metrics and optimize storage Learn more
Last updated: August 11, 2025, 10:05 AM
Refresh
260.5 K
Scanned files count
265.5 GiB
Scanned files size
141
Scanned tables count
70.6 K
Identified PII
Sensitive data and wide permissions
Risk zones showing file counts by access level and sensitivity. Click to investigate.
Sensitivity
Over 101 identifies
11-100 identifies
0-10 identifiers
281 files
110 files
82 files
620 files
120 files
128 files
220 files
106 files
109 files
1-10 users
11-100 users
Over 100 users
Exposure
652 files
Low risk
652 files
Medium risk
238 files
High risk
82 files
Critical risk
Savings opportunities
Stale data
Files not modified in over 3 years
206.6K Items
227 GiB
View files
Duplicate files
Files identified as duplicates of other files
206.6K Items
227 GiB
View files
Open permissions
82 %
No open permissions
10 %
Open to organization
8 %
Open to public
Reports
Data discovery assessment report
Summary of data risks, governance gaps, and compliance findings across scanned systems
Download
Full data mapping overview report
Detailed breakdown of data types, volumes, and storage locations
Download
Top data repositories by sensitivity level
Amazon
CVO
File shares
Database
125 K items
Non sensitive
Personal
Sensitive
Top document categories (20/40)
Show all
Operations - audit reports 5.6k
Bank statements 10.1k
Sales orders 21.3k
Miscellanous documents 5.6k
HR resumes 5.6k
PND2 2.93k
HR - resumes 5.6k
PN Data 2.93k
Services - RFP 3.6k
Vendor-customer contracts 8.5K
Code 13K
Corrupted 12K
Legal - vendor customer c... 3.2k
Structured data 2.93k
Finance - invoices 5.6k
Finance - Balance sheets... 9.8k
Legal - NDA 2.9k
Finance quarterly reports 19.8k
HR - resumes 5.6k
Legal - NDA 4.6k
Age of data
Last modified
40K
>7 years
40K
3-5 years
40K
1-3 years
0K
181-365 days
40K
91-180 days
40K
31-90 days
40K
<30 days
40K
<30 days
40K
<30 days
Size of data
40K
< 1 Byte
40K
1 Byte - 1KB
40K
1 KB - 1 MB
0K
1 MB - 10 MB
40K
10 MB - 100 MB
40K
100 MB - 1GB
40K
1 GB - 100 GB
40K
> 100 GB
Version: 100-10-82

Steps

1. From the NetApp Console menu, select **Governance > Classification**.
2. Select **Governance**.

   The Governance dashboard appears.

Review savings opportunities

The *Saving Opportunities* component shows data that you can delete or tier to less expensive object storage. The data in *Saving Opportunities* update every 2 hours. You can also manually update the data.

Steps

1. From the Data Classification menu, select **Governance**.
2. Within each Savings Opportunities tile of the Governance dashboard, select **Optimize Storage** to view the filtered results in the Investigation page. To discover any data you should delete or tier to less expensive storage, investigate the the *Saving Opportunities*.
   - **Stale Data** - By default, data is considered stale if it was last modified over 3 years ago. You can [customize the definition of stale data](task-stale-data.html).
   - **Duplicate Files** - Files that are duplicated in other locations in the data sources you are scanning. See what types of duplicate files are displayed.

If any of your data sources implement data tiering, old data that already resides in object storage can be identified in the *Stale Data* category.

Create the data discovery assessment report

The data discovery assessment report provides a high-level analysis of the scanned environment to show areas of concern and potential remediation steps. The results are based on both mapping and classifying your data. The goal of this report is to raise awareness of three significant aspects of your dataset:

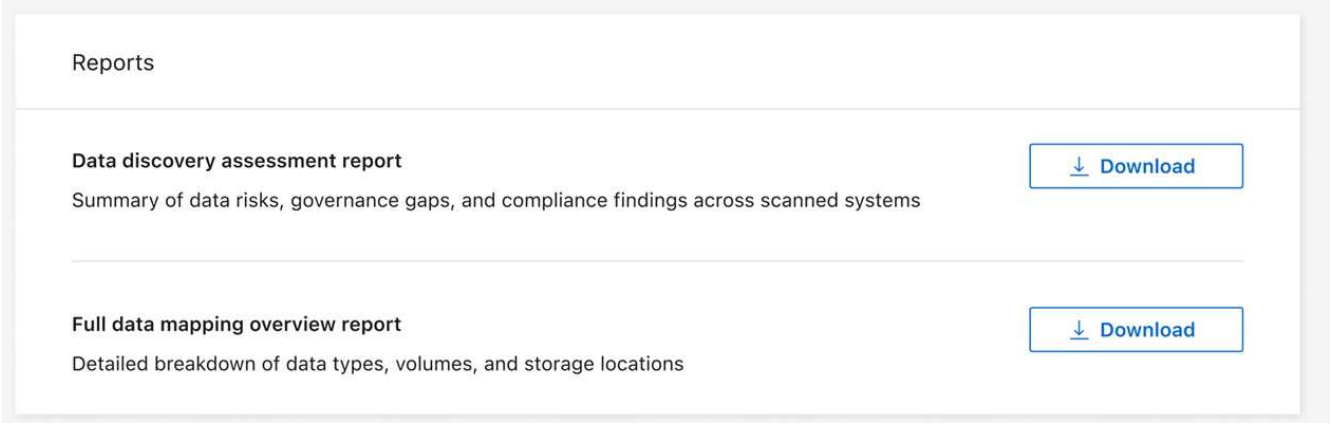
Feature	Description
Data governance concerns	A detailed picture of all the data you own and areas where you may be able to reduce the amount of data to save costs.
Data security exposures	Areas where your data is accessible to internal or external attacks because of broad access permissions.
Data compliance gaps	Where your personal or sensitive personal information is located for both security and for DSARs (data subject access requests).

With the report, you can take the following actions:

- Reduce storage costs by changing your retention policy, or by moving or deleting certain data (stale or duplicate data).
- Protect your data that has broad permissions by revising global group management policies.
- Protect your data that has personal or sensitive personal information by moving PII to more secure data stores.

Steps

1. From Data Classification, select **Governance**.
2. In the reports tile, select **Data Discovery Assessment Report**.



Result

Data Classification generates a PDF report that you can review and share.

Create the data mapping overview report

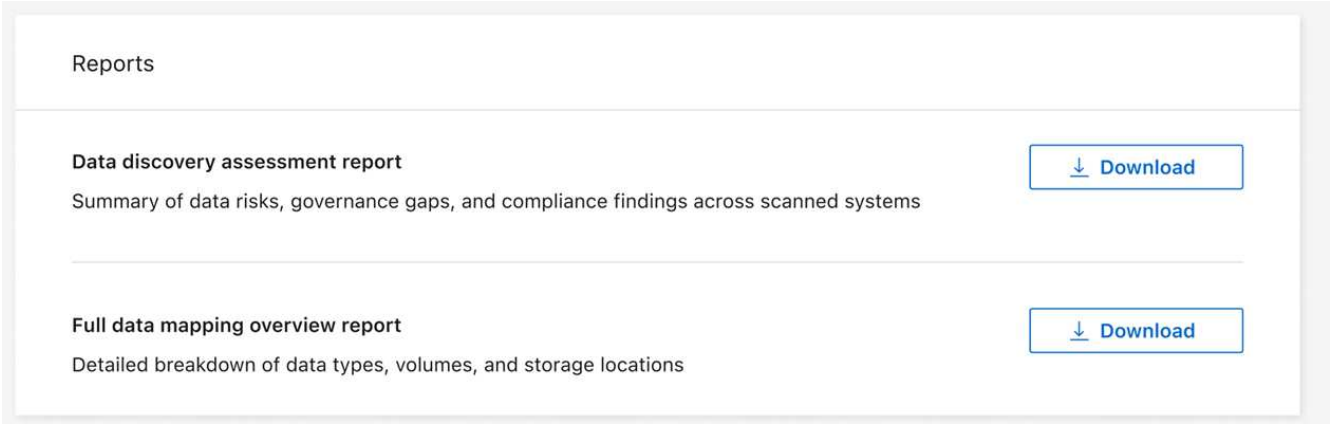
The data mapping overview report provides an overview of the data being stored in your corporate data sources to assist you with decisions of migration, back up, security, and compliance processes. The report summarizes all systems and data sources. It also provides an analysis for each system.

The report includes the following information:

Category	Description
Usage Capacity	For all systems: Lists the number of files and the used capacity for each system. For single systems: Lists the files that are using the most capacity.
Age of Data	Provides three charts and graphs for when files were created, last modified, or last accessed. Lists the number of files, and their used capacity, based on certain date ranges.
Size of Data	Lists the number of files that exist within certain size ranges in your systems.

Steps

1. From Data Classification, select **Governance**.
2. In the reports tile, select **Full data mapping overview report**.



Result

Data Classification generates a PDF report that you can review and send to other groups as needed.

If the report is larger than 1 MB, the PDF file is retained on the Data Classification instance and you'll see a pop-up message about the exact location. When Data Classification is installed on a Linux machine on your premises, or on a Linux machine you deployed in the cloud, you can navigate directly to the PDF file. When Data Classification is deployed in the cloud, you need to authorize with SSH to the Data Classification instance to download the PDF file.

Review the top data repositories listed by data sensitivity

The *Top Data Repositories by Sensitivity Level* area of the Data Mapping Overview report lists the top four data repositories (systems and data sources) that contain the most sensitive items. The bar chart for each system is divided into:

- Non-sensitive data
- Personal data
- Sensitive personal data

This data refreshes every two hours and can be manually refreshed.

Steps

1. To see the total number of items in each category, position your cursor over each section of the bar.
2. To filter results that will appear in the Investigation page, select each area in the bar and investigate further.

Review sensitive data and wide permissions

The *Sensitive Data and Wide Permissions* area of the Governance dashboard shows the counts for files that contain sensitive data and have wide permissions. The table shows the following types of permissions:

- From the most restrictive permissions to the most permissive restrictions on the horizontal axis.
- From the least sensitive data to the most sensitive data on the vertical axis.

Steps

1. To see the total number of files in each category, position your cursor over each box.
2. To filter results that will appear in the Investigation page, select a box and investigate further.

Review data listed by types of open permissions

The *Open Permissions* area of the Data Mapping Overview report shows the percentage for each type of permissions that exist for all files that are being scanned. The chart shows the following types of permissions:

- No Open Permissions
- Open to Organization
- Open to Public
- Unknown Access

Steps

1. To see the total number of files in each category, position your cursor over each box.
2. To filter results that will appear in the Investigation page, select a box and investigate further.

Review the age and size of data

You can investigate the items in the *Age* and *Size* graphs of the Data Mapping Overview report to see if there is any data you should delete or tier to less expensive object storage.

Steps

1. In the Age of Data chart, to see details about the age of the data, position your cursor over a point in the chart.
2. To filter by an age or size range, select that age or size.
    - **Age of Data graph** - Categorizes data based on the time it was created, the last time it was accessed, or the last time it was modified.
    - **Size of Data graph** - Categorizes data based on size.

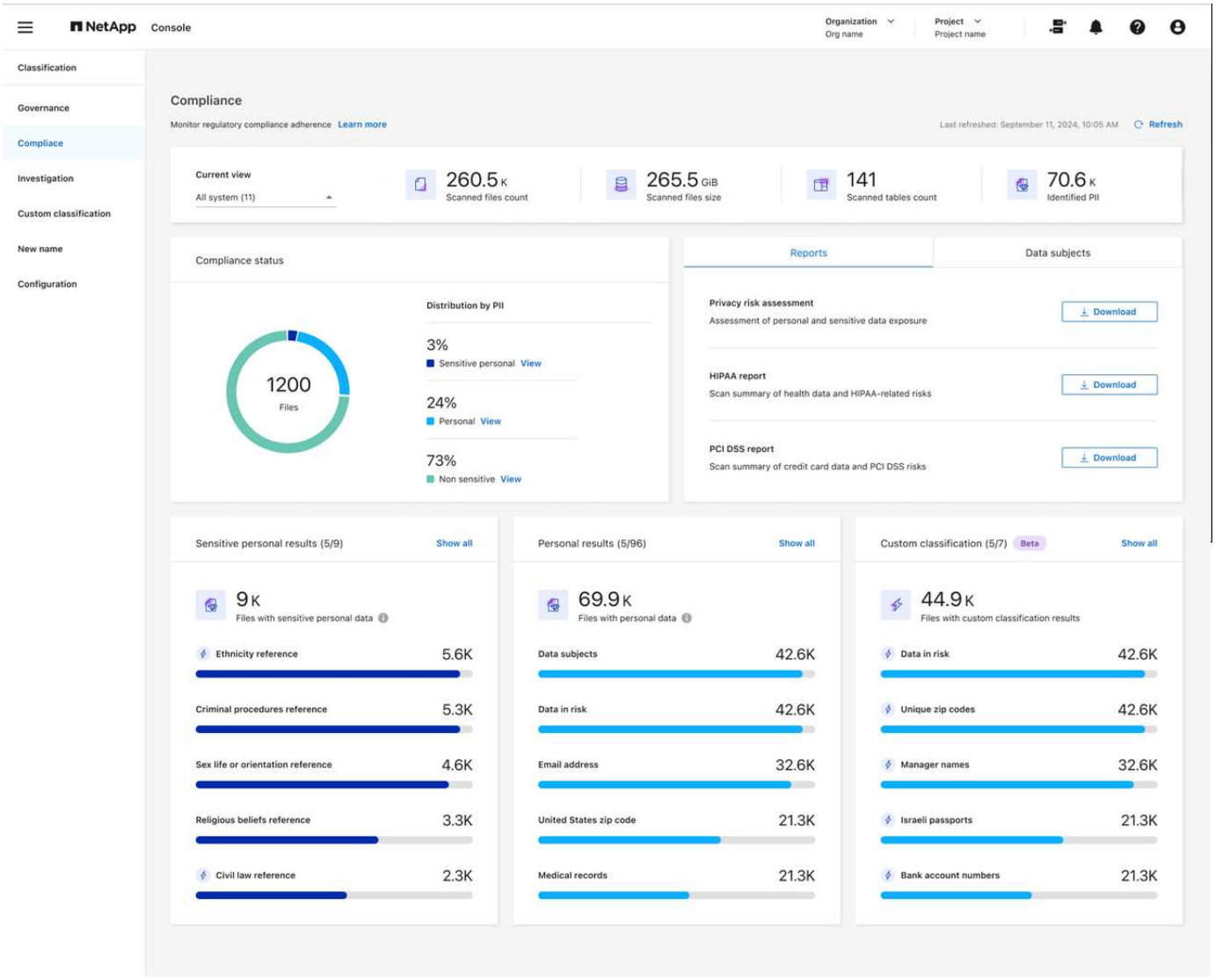
> If any of your data sources implement data tiering, old data that already resides in object storage might be identified in the *Age of Data* graph.

View compliance details about the private data stored in your organization with NetApp Data Classification

Gain control of your private data by viewing details about the personal data (PII) and sensitive personal data (SPII) in your organization. You can also gain visibility by reviewing the categories and file types that NetApp Data Classification found in your data.

> File-level compliance details are only available if you perform a full classification scan. Mapping-only scans don’t yield file-level details.

By default, the Data Classification dashboard displays compliance data for all systems and databases. To see data for only some of the systems, select them.



You can 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.

View files that contain personal data

Data Classification automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, credit card numbers, social security numbers, bank account numbers, passwords, and more. Data Classification identifies this type of information in individual files, in files within directories (shares and folders), and in database tables.

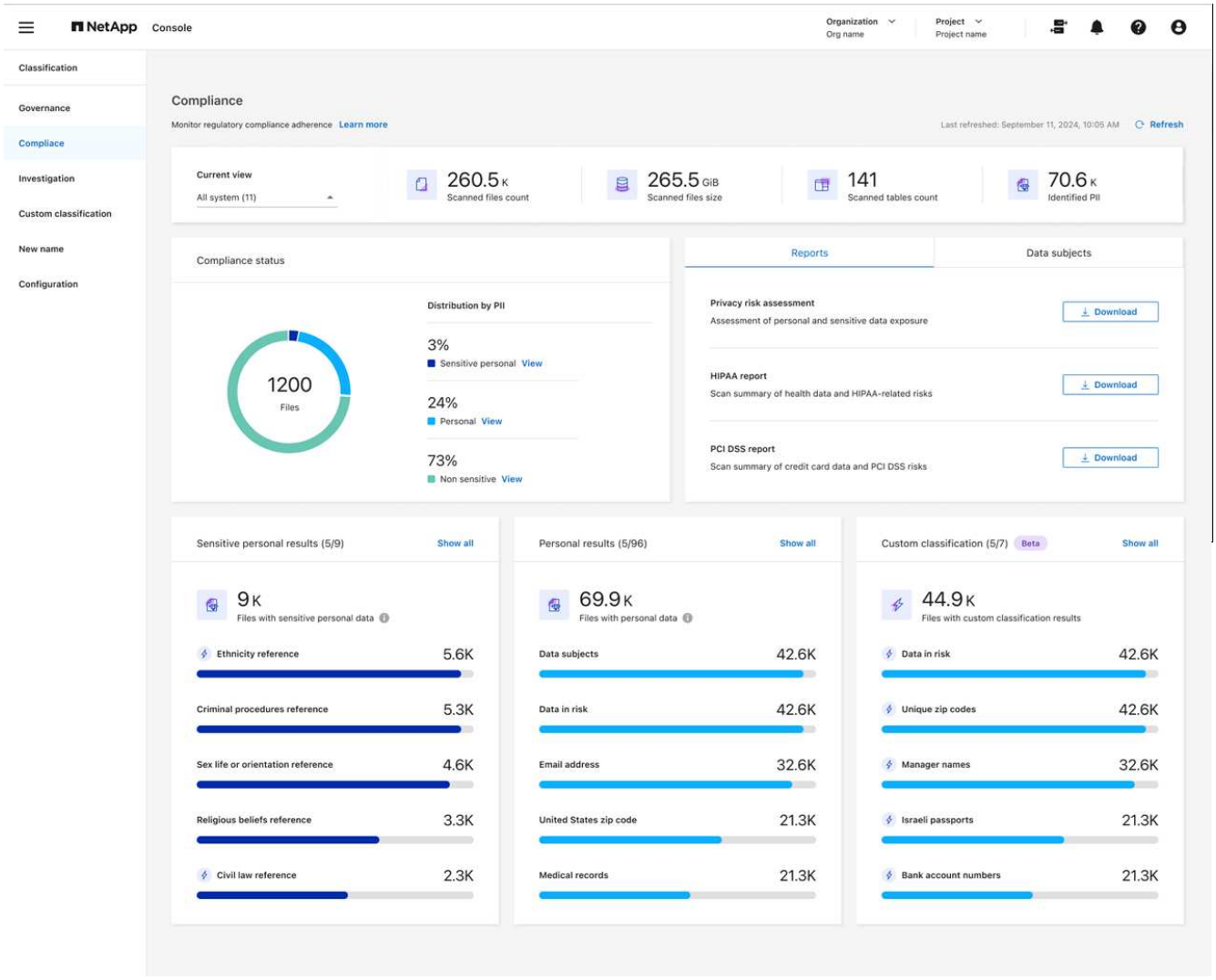
You can also create custom search terms to identify personal data specific to your organization. For more information, see Create a custom classification.

For some types of personal data, Data Classification 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, Data Classification identifies a U.S. social security number (SSN) as an SSN if it sees a proximity word next to it—for example, *SSN* or *social security*. The table of personal data shows when Data Classification uses proximity validation.

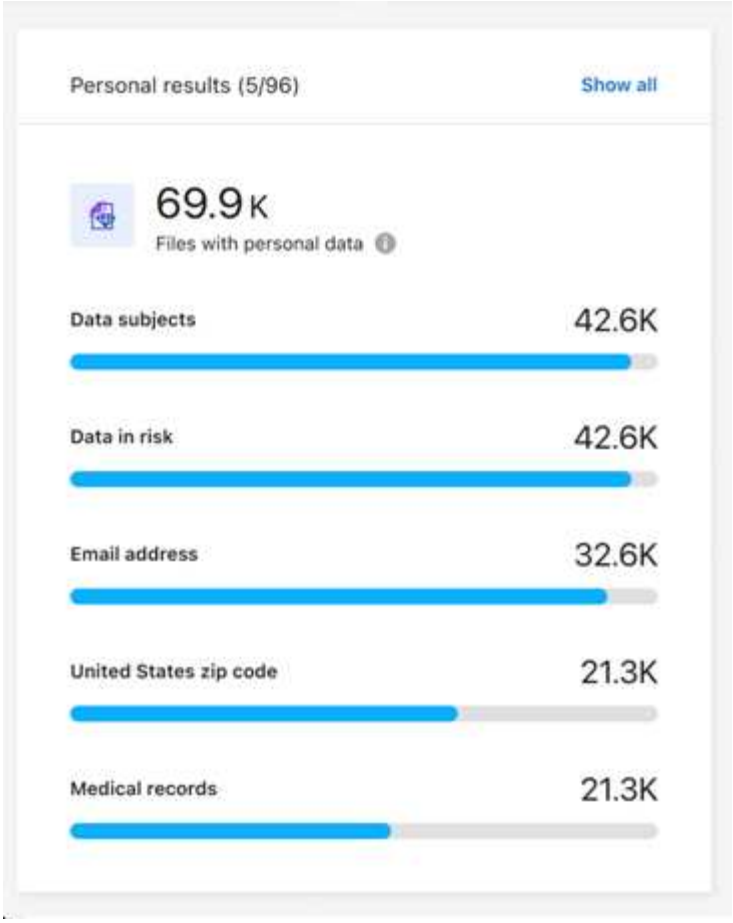
Steps

1. From the Data Classification menu, select the **Compliance** tab.

2. To investigate the details for all personal data, select the icon next to the personal data percentage.

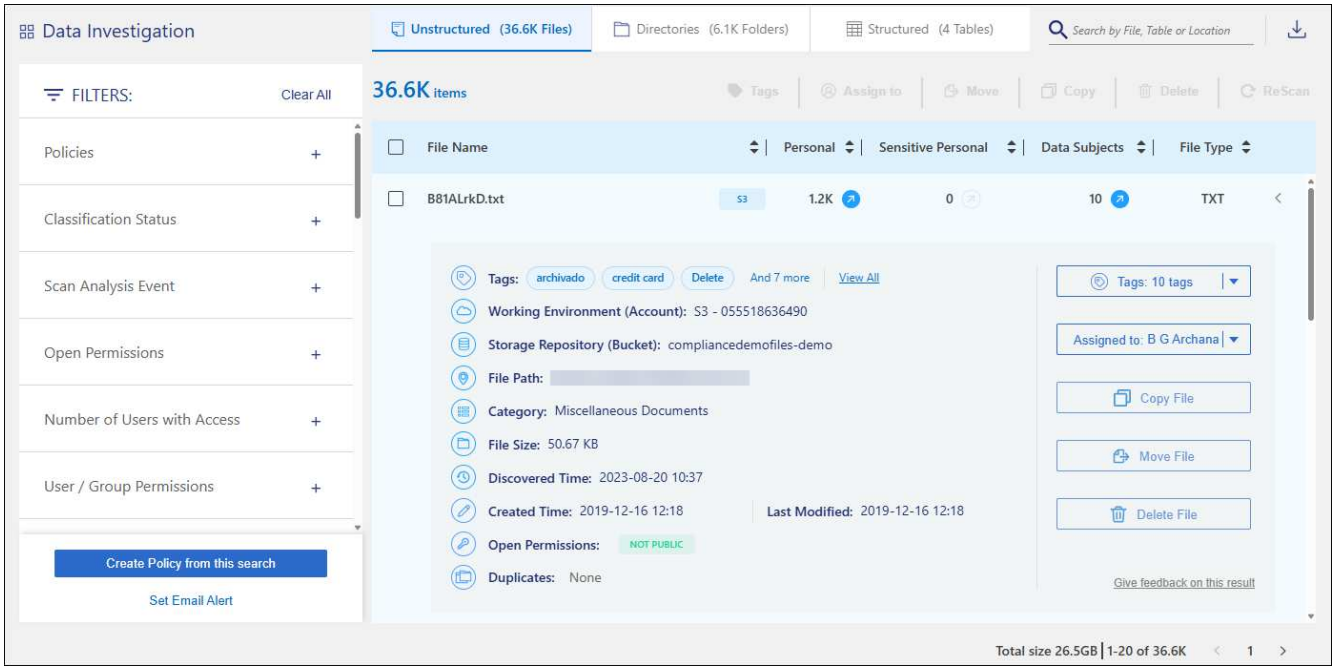


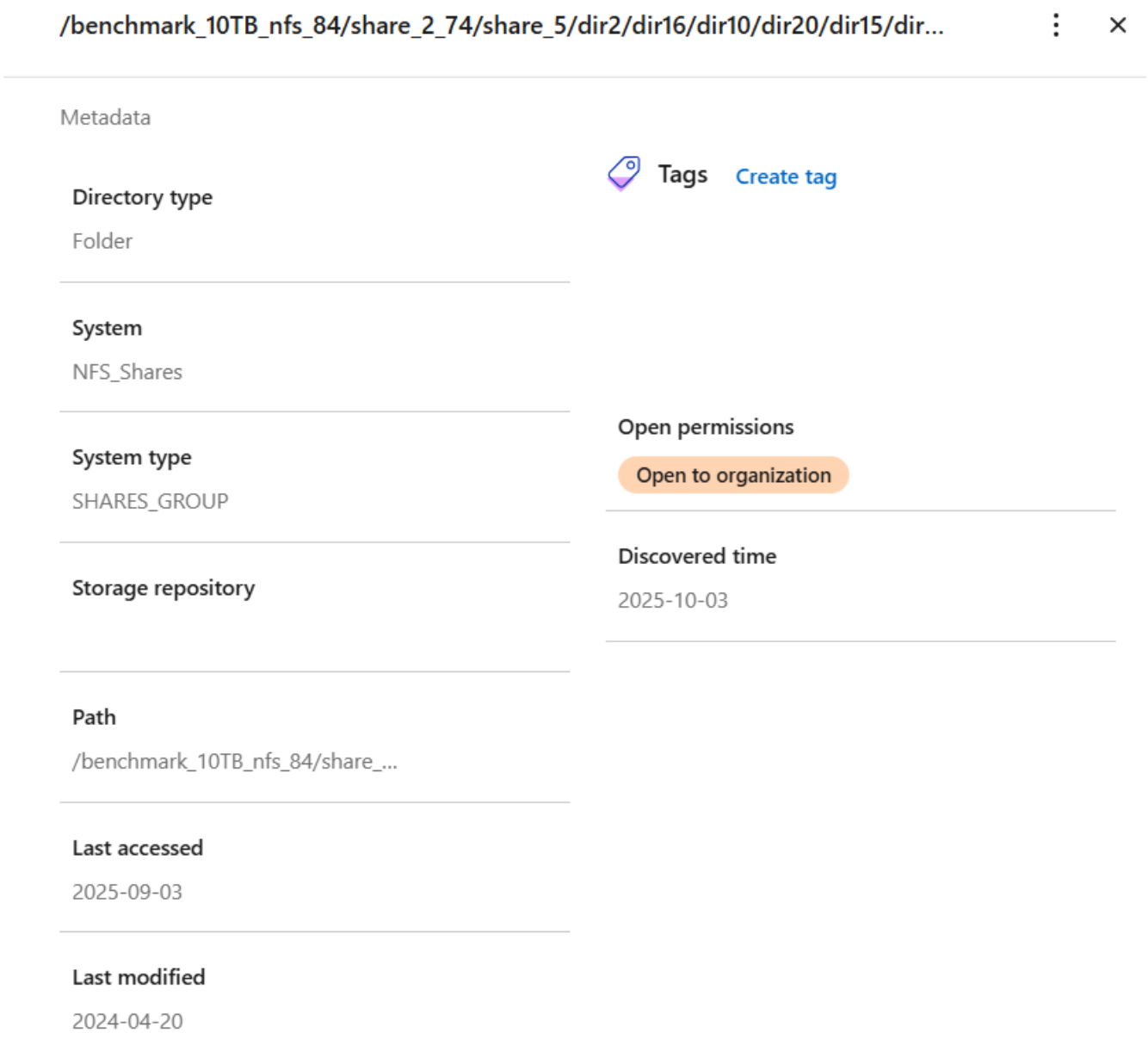
3. To investigate the details for a specific type of personal data, select **View All** and then select the **Investigate Results** arrow icon for a specific type of personal data, for example, email addresses.



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

   The following images show personal data found in a directory (shares and folders). In the **Structured** tab, you view personal data found in databases. In the **Unstructured** tab, you can view file-level data.





View files that contain sensitive personal data

Data Classification 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. Data Classification identifies this type of information in individual files, in files within directories (shares and folders), and in database tables.

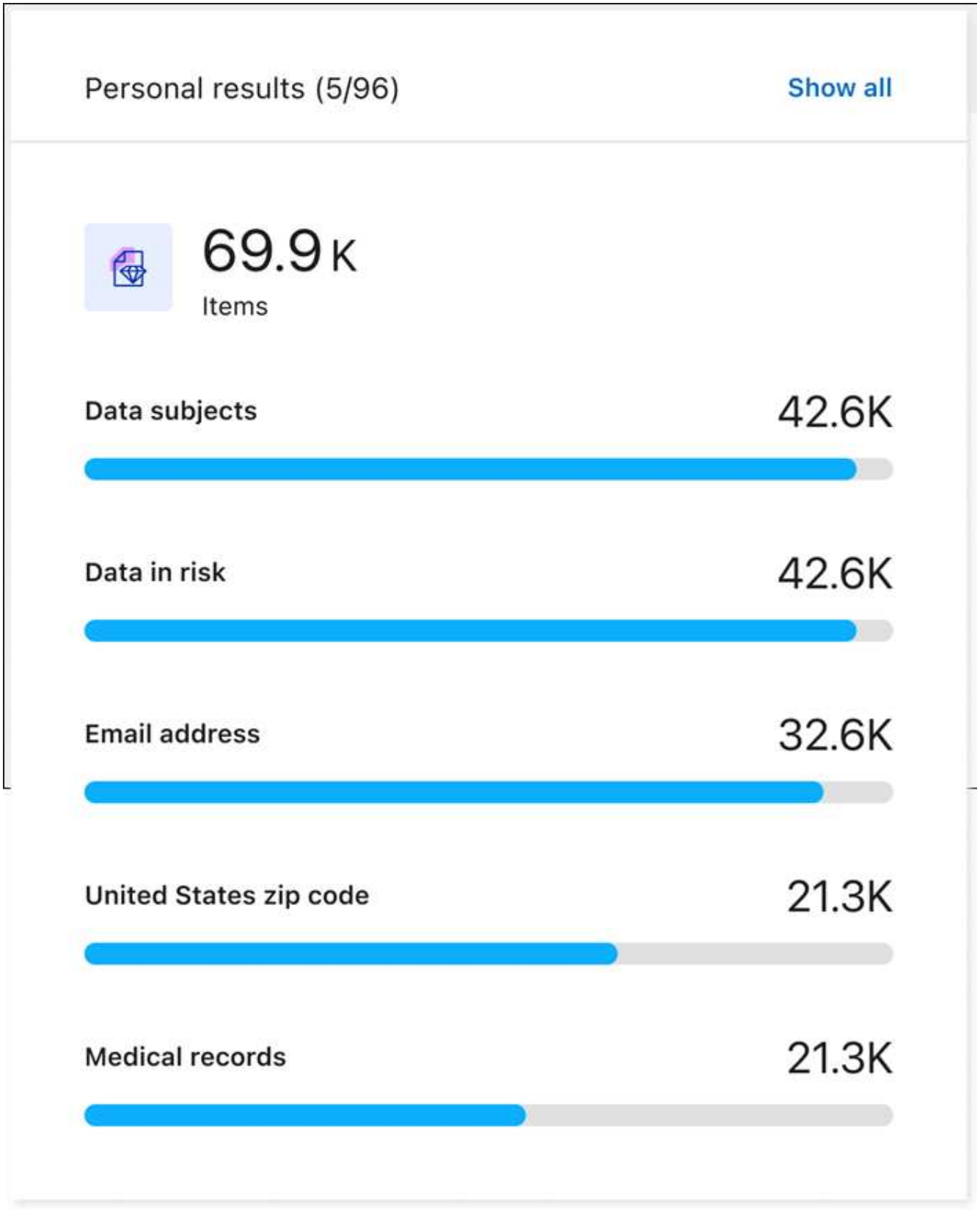
Data Classification uses AI, natural language processing (NLP), machine learning (ML), and cognitive computing (CC) to understand the meaning of the content that it scans in order to extract entities and categorize it accordingly.

For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, Data Classification 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.

Steps

1. From the Data Classification menu, select **Compliance**.
2. To investigate the details for all sensitive personal data, locate the **Sensitive personal results** card then select **Show all**.



.

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

Categories of private data in NetApp Data Classification

There are many types of private data that NetApp Data Classification can identify in your volumes and databases.

Data Classification identifies two types of personal data:

- **Personally identifiable information (PII)**
- **Sensitive personal information (SPII)**

If you need Data Classification to identify other private data types, such as additional national ID numbers or healthcare identifiers, contact your account manager.

Types of personal data

The personal data, or *personally identifiable information* (PII), found in files can be general personal data or national identifiers. The third column in the table below identifies whether Data Classification uses proximity validation to validate its findings for the identifier.

The languages in which these items can be recognized are identified in the table.

Type	Identifier	Proximity validation?	English	German	Spanish	French	Japanese
General	Credit card number	Yes	✓	✓	✓		✓
	Data Subjects	No	✓	✓	✓		
	Email Address	No	✓	✓	✓		✓
	IBAN Number (International Bank Account Number)	No	✓	✓	✓		✓
	IP Address	No	✓	✓	✓		✓
	Password	Yes	✓	✓	✓		✓

Type	Identifier	Proximity validation?	English	German	Spanish	French	Japanese
National Identifiers							

Type	Identifier	Proximity validation?	English	German	Spanish	French	Japanese

Type	Identifier	Proximity validation?	English	German	Spanish	French	Japanese

Type	Identifier	Proximity validations?	English	German	Spanish	French	Japanese
	Corporate)						
	Latvian ID	Yes	✓	✓	✓		
	Lithuanian ID	Yes	✓	✓	✓		
	Luxembourg ID	Yes	✓	✓	✓		
	Maltese ID	Yes	✓	✓	✓		
	National Health Service (NHS) Number	Yes	✓	✓	✓		
	New Zealand Bank Account	Yes	✓	✓	✓		
	New Zealand Driver's License	Yes	✓	✓	✓		
	New Zealand IRD Number (Tax ID)	Yes	✓	✓	✓		
	New Zealand NHI (National Health Index) Number	Yes	✓	✓	✓		
	New Zealand Passport Number	Yes	✓	✓	✓		
	Polish ID (PESEL)	Yes	✓	✓	✓		
	Portuguese Tax Identification Number (NIF)	Yes	✓	✓	✓		
	Romanian ID (CNP)	Yes	✓	✓	✓		
	Singapore National Registration Identity Card (NRIC)	Yes	✓	✓	✓		
	Slovenian ID (EMSO)	Yes	✓	✓	✓		
	South African ID	Yes	✓	✓	✓		
	Spanish Tax Identification Number	Yes	✓	✓	✓		
	Swedish ID	Yes	✓	✓	✓		
	UK ID (NINO)	Yes	✓	✓	✓		
	USA California Driver's License	Yes	✓	✓	✓		
	USA Indiana Driver's License	Yes	✓	✓	✓		
	USA New York Driver's License	Yes	✓	✓	✓		
	USA Texas Driver's License	Yes	✓	✓	✓		
	USA Social Security Number (SSN)	Yes	✓	✓	✓		

Types of sensitive personal data

Data Classification can find the following sensitive personal information (SPII) in files.

The following SPII can currently only be recongized in English:

- **Criminal Procedures Reference**: Data concerning a natural person's criminal convictions and offenses.
- **Ethnicity Reference**: Data concerning a natural person's racial or ethnic origin.
- **Health Reference**: Data concerning a natural person's health.
- **ICD-9-CM Medical Codes**: Codes used in the medical and health industry.
- **ICD-10-CM Medical Codes**: Codes used in the medical and health industry.

- **Philosophical Beliefs Reference**: Data concerning a natural person's philosophical beliefs.
- **Political Opinions Reference**: Data concerning a natural person's political opinions.
- **Religious Beliefs Reference**: Data concerning a natural person's religious beliefs.
- **Sex Life or Orientation Reference**: Data concerning a natural person's sex life or sexual orientation.

Types of categories

Data Classification categorizes your data as follows.

Most of these categories can be recognized in English, German, and Spanish.

Category	Type	English	German	Spanish
Finance	Balance Sheets	✓	✓	✓
	Purchase Orders	✓	✓	✓
	Invoices	✓	✓	✓
	Quarterly Reports	✓	✓	✓
HR	Background Checks	✓		✓
	Compensation Plans	✓	✓	✓
	Employee Contracts	✓		✓
	Employee Reviews	✓		✓
	Health	✓		✓
	Resumes	✓	✓	✓
Legal	NDAs	✓	✓	✓
	Vendor-Customer contracts	✓	✓	✓
Marketing	Campaigns	✓	✓	✓
	Conferences	✓	✓	✓
Operations	Audit Reports	✓	✓	✓
Sales	Sales Orders	✓	✓	
Services	RFI	✓		✓
	RFP	✓		✓
	SOW	✓	✓	✓
	Training	✓	✓	✓
Support	Complaints and Tickets	✓	✓	✓

The following metadata is also categorized and identified in the same supported languages:

- Application Data
- Archive Files

- Audio
- Breadcrumbs from Data Classification Business Application Data
- CAD Files
- Code
- Corrupted
- Database and index files
- Design Files
- Email Application Data
- Encrypted (files with a high entropy score)
- Executables
- Financial Application Data
- Health Application Data
- Images
- Logs
- Miscellaneous Documents
- Miscellaneous Presentations
- Miscellaneous Spreadsheets
- Miscellaneous "Unknown"
- Password Protected files
- Structured Data
- Videos
- Zero-Byte Files

Types of files

Data Classification scans all files for category and metadata insights and displays all file types in the file types section of the dashboard. When Data Classification detects Personal Identifiable Information (PII) or when it performs a DSAR search, only the following file formats are supported:

`.CSV, .DCM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides`

Accuracy of information found

NetApp can't guarantee 100% accuracy of the personal data and sensitive personal data that Data Classification identifies. You should always validate the information by reviewing the data.

Based on our testing, the table below shows the accuracy of the information that Data Classification finds. We break it down by *precision* and *recall*:

Precision

The probability that what Data Classification finds has been identified correctly. For example, a precision rate of 90% for personal data means that 9 out of 10 files identified as containing personal information,

actually contain personal information. 1 out of 10 files would be a false positive.

Recall

The probability for Data Classification to find what it should. For example, a recall rate of 70% for personal data means that Data Classification can identify 7 out of 10 files that actually contain personal information in your organization. Data Classification would miss 30% of the data and it won't appear in the dashboard.

We are constantly improving the accuracy of our results. Those improvements will be automatically available in future Data Classification releases.

Type	Precision	Recall
Personal data - General	90%-95%	60%-80%
Personal data - Country identifiers	30%-60%	40%-60%
Sensitive personal data	80%-95%	20%-30%
Categories	90%-97%	60%-80%

Create a custom classification in NetApp Data Classification

NetApp Data Classification enables you to create custom categories or personal identifiers to identify data specific to your organization's regulatory and compliance requirements.

Data Classification supports two types of custom classifiers: categories and personal identifiers. Custom categories are created based on a set of files you upload from which Data Classification creates an AI model to identify similar data in your organization (for example, a health research firm might create a clinical analysis category). Custom personal identifiers are created using keyword lists or a regular expression (regex) to identify information specific to your organization that can pose a compliance risk.

All custom classifications are available in the Custom classification dashboard.

Create a custom personal identifier

Data Classification enables you to create a custom personal identifier using either contextual keywords or a regular expression to identify data unique to your organization.

Requirements for keywords

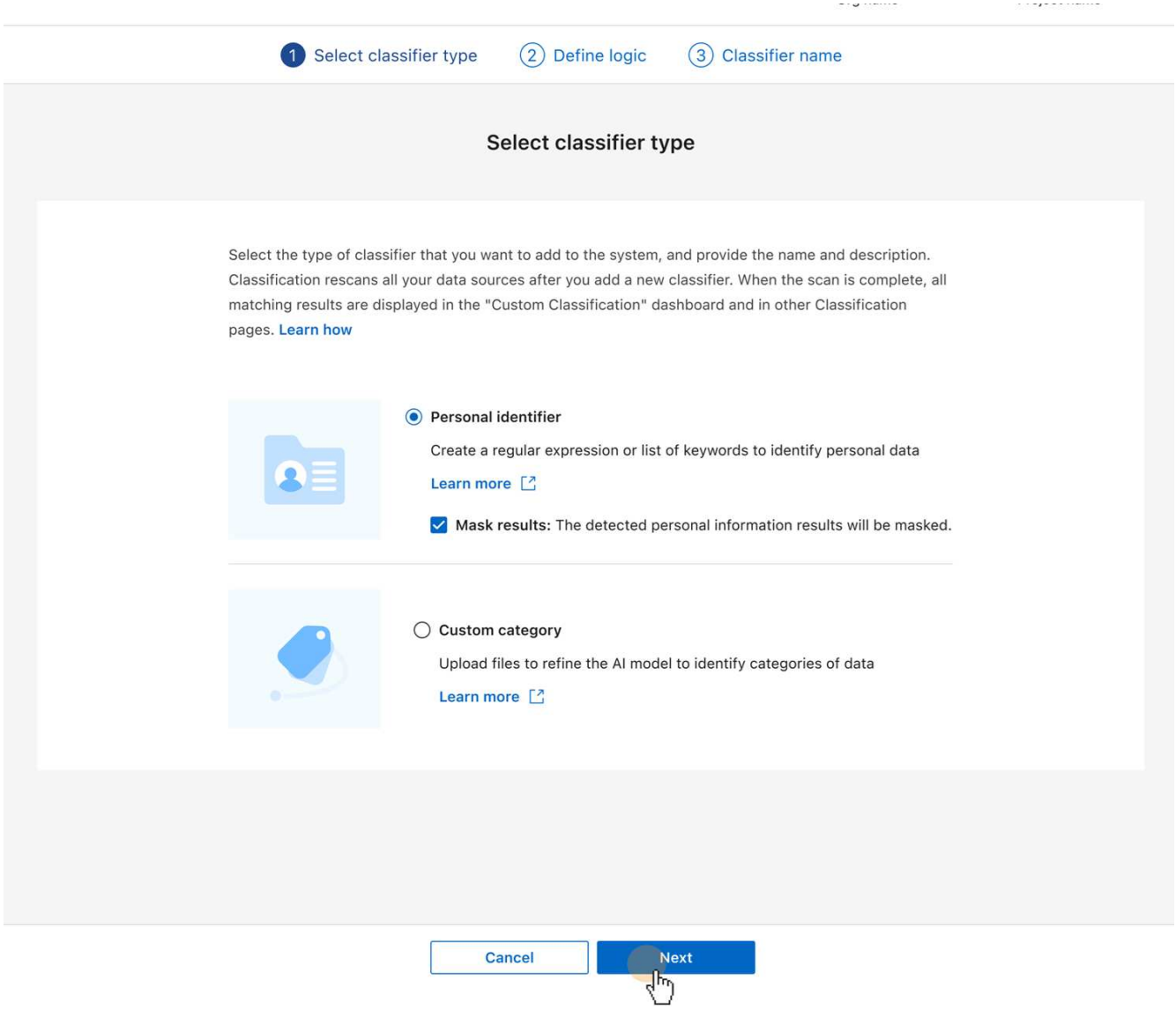
If you're creating your personal identifier with a keyword list, the list must meet the following requirements:

- Keyword entries are case insensitive.
- Keywords must be at least three characters. Any words shorter than three characters are ignored.
- Duplicate words are only added once.
- The total list of keywords can't exceed 500,000 characters. The list must include at least one keyword.

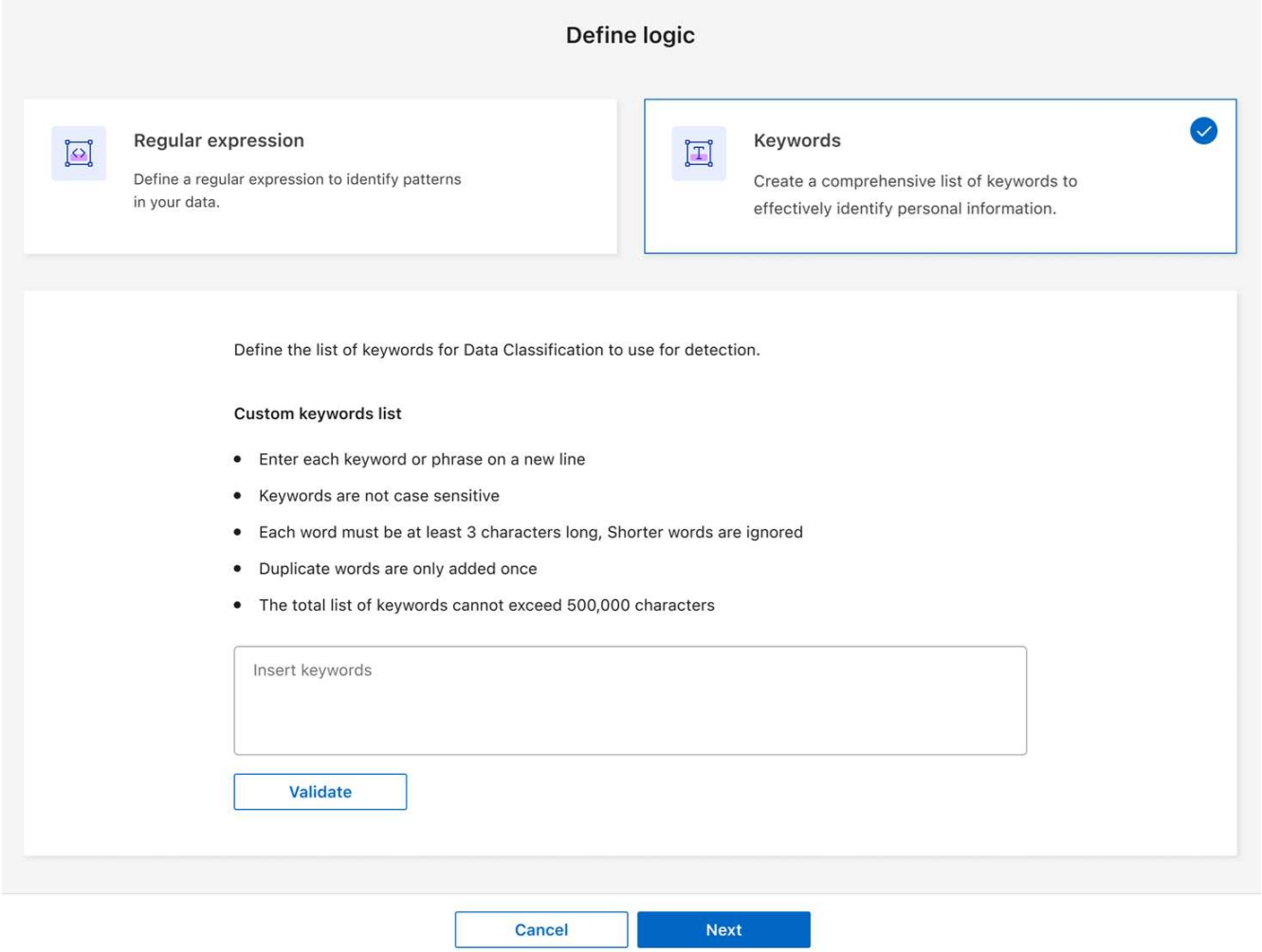
Steps

1. Select the **Custom classification** tab.
2. Select **+ New Classifier** to create the custom classifier.

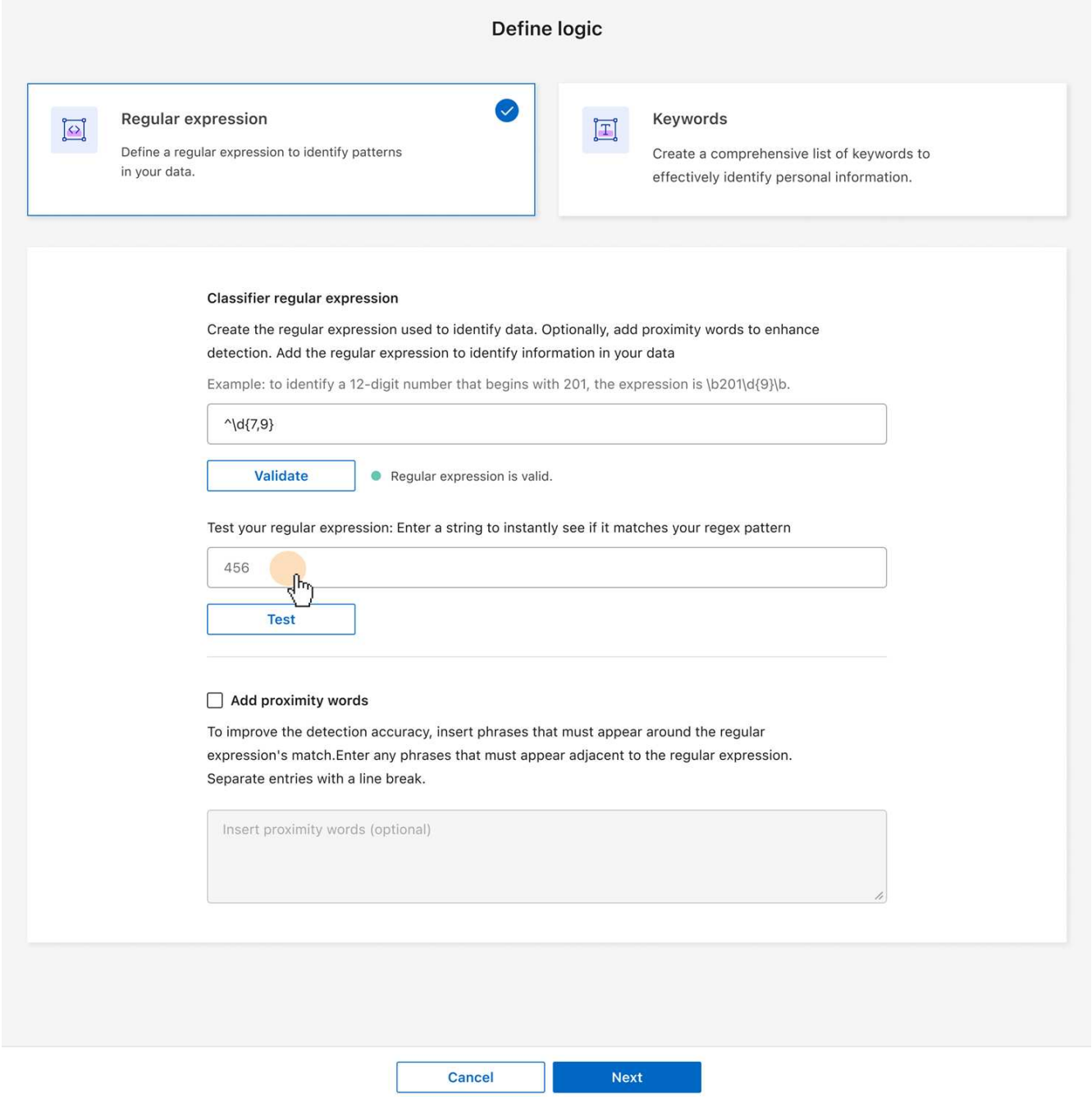
3. Select **Personal identifier**. Optionally, select **Mask results** to mask detected personal data.
4. Select **Next**.



5. To add the classifier with keywords, select **Keywords**. Enter a list of keywords, with each entry on a separate line. Ensure the keywords adhere to the requirements.



To add the classifier as a regular expression, select **Regular expression** then add a pattern to detect the specific information of your data. Select **Validate** to confirm the syntax of your entry.



a. Optionally, enter a sample string that should match your regex pattern then select **Test** to check it.

b. Optionally, add proximity words. If you add proximity words, Data Classification only flags the regex pattern if the proximity words are adjacent to the matching string.

6. Select **Next**.
7. Enter a **Classifier name** and a **Description** to identify the custom category in your dashboard.
8. Select **Save** to create the custom personal identifier.

After you create a custom personal identifier, its results are captured in the next scheduled scan. To capture results sooner, perform an on-demand scan. To view results, see Generate compliance reports.

Create a custom category

With custom categories, you can categorize data specific to your organization. Custom categories are created based on text files that you upload from which Data Classification creates an AI model to identify similar information in other files.

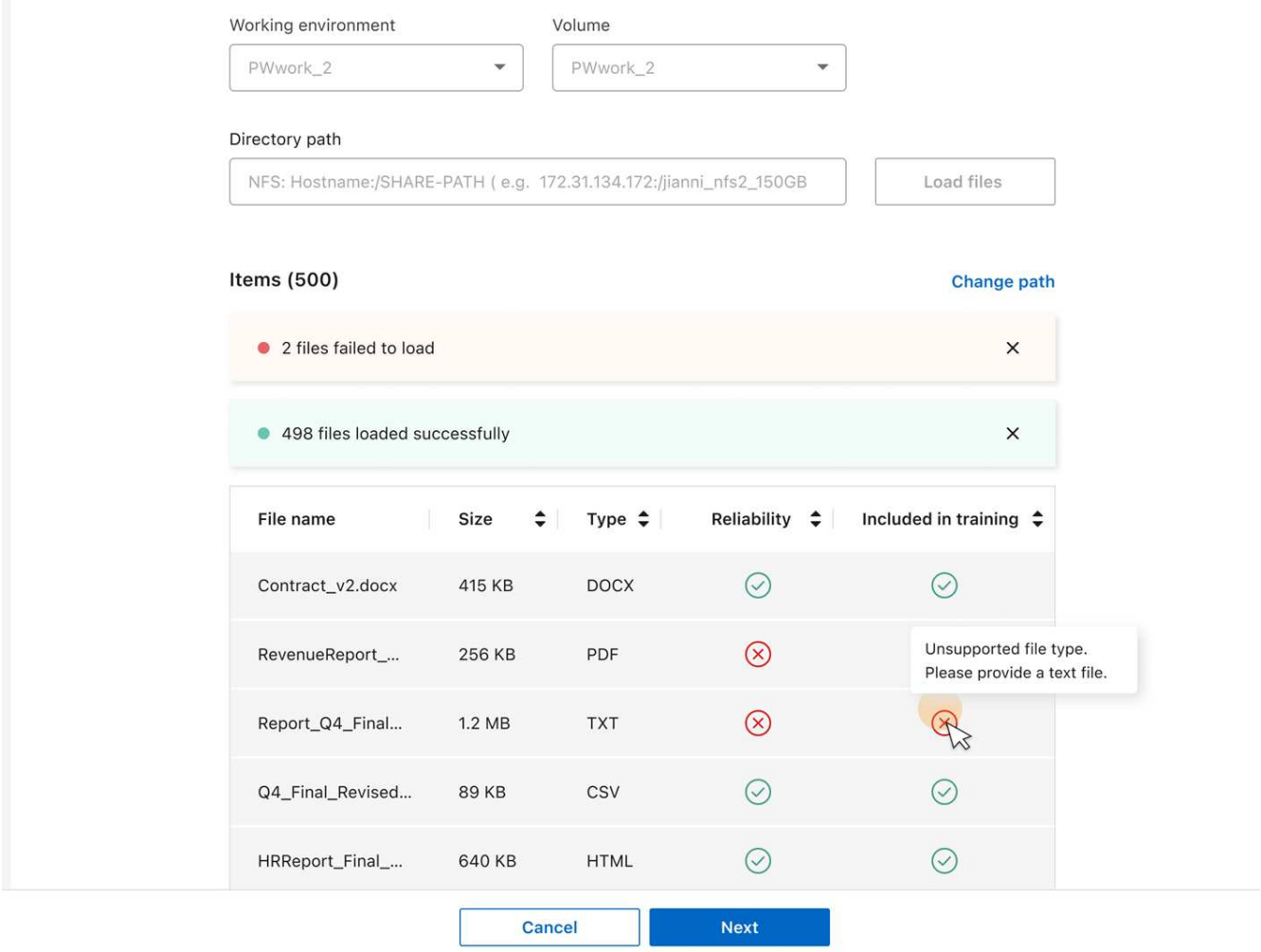
Training data requirements

- The training dataset must contain a minimum of 25 files. The maximum file count is 1,000.
- All files must be located directly in the file path that you provide.
- All files must be larger than 100 bytes.
- Data Classification training data must be one of the following file types: CSV, DOCX, DOC, GZ, JSON, PDF, PPTX, TXT, RTT, XLS, or XLSX. You can upload a combination of all the supported file types.

Steps

1. In NetApp Data Classification, select **Custom classification**.
2. Select **+ New classifier**.
3. Choose **Custom category** as your classifier type then **Next**.
4. Define the logic for your custom category with a collection of text-based files. Provide the IP address of the **Working address** then select the **Volume** from the dropdown menu.

   Enter the **Directory path** for the directory that contains the training data.
5. Select **Load files** for Data Classification to perform a check of the files. You can review the summary of the files, which lists the file name, size, type, and notes if the file was deemed acceptable for training.



a. To change the file path or re-upload files, select **Change path** then enter the data and load the files again.

6. When you're satisfied with the files uploaded, select **Next**.
7. Enter a **Classifier name** and a **Description** to identify the custom category in your dashboard.
8. Select **Save** to create the custom category.

Result

After you create a custom category, its results are captured in the next scheduled scan. To capture results sooner, manually initiate the scan.

Edit a custom classifier

You can modify the logic of a personal identifier after you create it. You can't change the type of the personal identifier or the logic type; for example, you can't change a custom category to a custom personal identifier. You also can't change a keyword-based custom identifier to a regex-based custom identifier.

Steps

1. In NetApp Data Classification, select **Custom classification**.
2. Identify the classifier you want to delete, then select the action menu … at the end of its row.
3. Select **Edit logic**.

4. If you're modifying keywords, add, delete, or edit the appropriate keywords. If you're modifying a regular expression, enter the new regular expression and validate it. Optionally, add proximity keywords.
5. Select **Save** to apply the changes.

Delete a custom classifier

1. In NetApp Data Classification, select **Custom classification**.
2. Identify the classifier you want to delete then select the action menu … at the end of its row.
3. Select **Delete classifier**.

Next steps

- Generate compliance reports

Investigate the data stored in your organization with NetApp Data Classification

The Data Investigation dashboard displays file and directory-level insights into your data, enabling you to sort and filter results. The Data Investigation page presents insights into file and directory metadata and permissions as well as identifying duplicate files. With file-, directory-, and database-level insights, you can take actions to improve the compliance of your organization and save storage space. The Data Investigation page also supports moving, copying, and deleting files.

To gain insights from the Investigation page, you must perform a full classification scan on your data sources. Data sources that have had a mapping-only scan do not show file-level details.

Data investigation structure

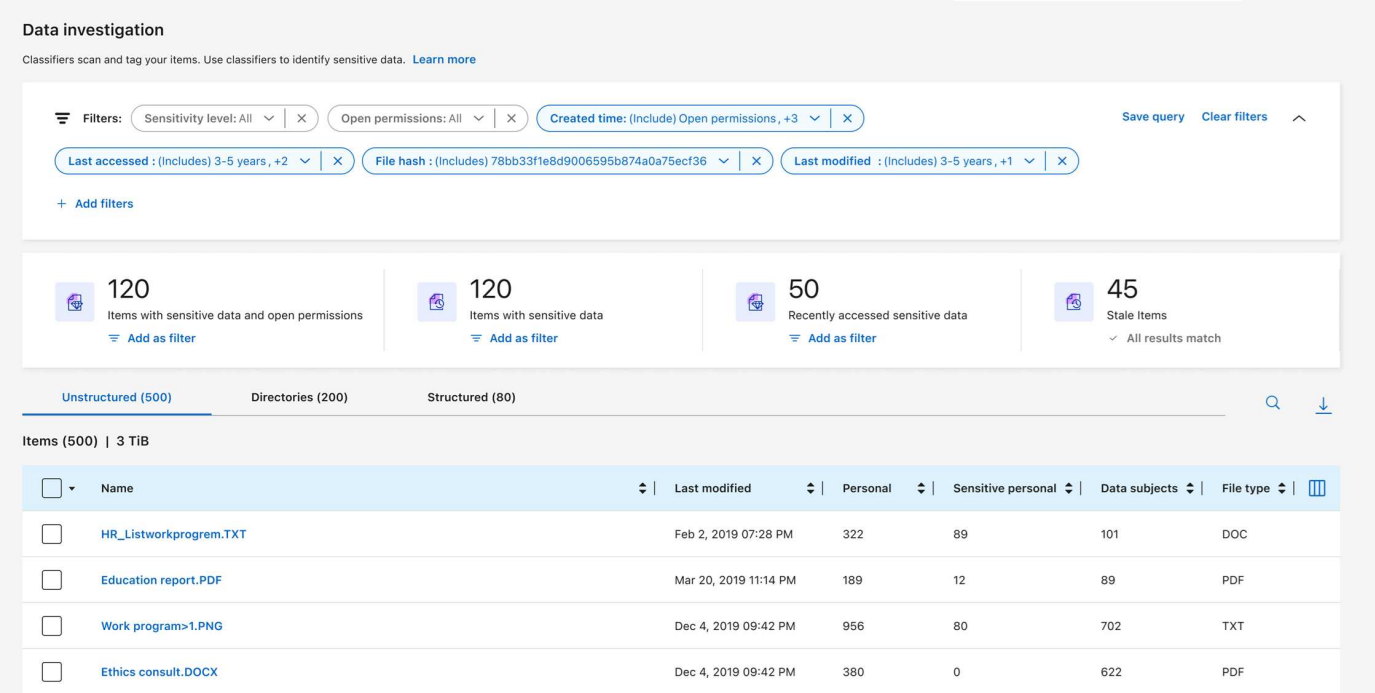
The Data Investigation page sorts data into three tabs:

- **Unstructured data**: file data
- **Directories**: folders and file shares
- **Structured**: database

Data filters

The Data Investigation page provides numerous filters to sort through your data so you can what you need. You can use multiple filters in concert.

To add a filter, select the **Add filter** button.



Filter sensitivity and content

Use the following filters to view how much sensitive information is contained in your data.

Filter	Details
Category	Select the types of categories.
Sensitivity Level	Select the sensitivity level: Personal, Sensitive personal, or Non sensitive.
Number of identifiers	Select the range of detected sensitive identifiers per file. Includes personal data and sensitive personal data. When filtering in Directories, Data Classification totals the matches from all files in each folder (and sub-folders). NOTE: The December 2023 (version 1.26.6) release removed the option to calculate the number of personal identifiable information (PII) data by Directories.
Personal Data	Select the types of personal data.
Sensitive Personal Data	Select the types of sensitive personal data.
Data Subject	Enter a data subject's full name or known identifier. Learn more about data subjects here.

Filter user owner and user permissions

Use the following filters to view file owners and permissions to access your data.

Filter	Details
Open Permissions	Select the type of permissions within the data and within folders/shares.

Filter	Details
User / Group Permissions	Select one or multiple user names and/or group names, or enter a partial name.
File Owner	Enter the file owner name.
Number of users with access	Select one or multiple category ranges to show which files and folders are open to a certain number of users.

Filter chronologically

Use the following filters to view data based on time criteria.

Filter	Details
Created Time	Select a time range when the file was created. You can also specify a custom time range to further refine the search results.
Discovered Time	Select a time range when Data Classification discovered the file. You can also specify a custom time range to further refine the search results.
Last Modified	Select a time range when the file was last modified. You can also specify a custom time range to further refine the search results.
Last Accessed	Select a time range when the file or directory* was last accessed. You can also specify a custom time range to further refine the search results. For the types of files that Data Classification scans, this is the last time Data Classification scanned the file.

* Last accessed time for a directory is only available for NFS or CIFS shares.

Filter metadata

Use the following filters to view data based on location, size, and directory or file type.

Filter	Details
File Path	Enter up to 20 partial or full paths that you want to include or exclude from the query. If you enter both include paths and exclude paths, Data Classification finds all files in the included paths first, then it removes files from excluded paths, and then it displays the results. Note that using "*" in this filter has no effect, and that you can’t exclude specific folders from the scan - all the directories and files under a configured share will be scanned.
Directory Type	Select the directory type; either "Share" or "Folder".
File Type	Select the types of files.
File Size	Select the file size range.
File Hash	Enter the file’s hash to find a specific file, even if the name is different.

Filter storage type

Use the following filters to view data by storage type.

Filter	Details
System type	Select the type of system.
System environment name	Select specific systems.
Storage Repository	Select the storage repository, for example, a volume or a schema.

Filter query

Use the following filter to view data by saved queries.

Filter	Details
Saved query	Select one saved query or multiples. Go to the saved queries tab to view the list of existing saved queries and create new ones.
Tags	Select the tag or tags that are assigned to your files.

Filter analysis status

Use the following filter to view data by the Data Classification scan status.

Filter	Details
Analysis Status	Select an option to show the list of files that are Pending First Scan, Completed being scanned, Pending Rescan, or that have Failed to be scanned.
Scan Analysis Event	Select whether you want to view files that were not classified because Data Classification couldn't revert last accessed time, or files that were classified even though Data Classification couldn't revert last accessed time.

See details about the "last accessed time" timestamp for more information about the items that appear in the Investigation page when filtering using the Scan Analysis Event.

Filter data by duplicates

Use the following filter to view files that are duplicated in your storage.

Filter	Details
Duplicates	Select whether the file is duplicated in the repositories.

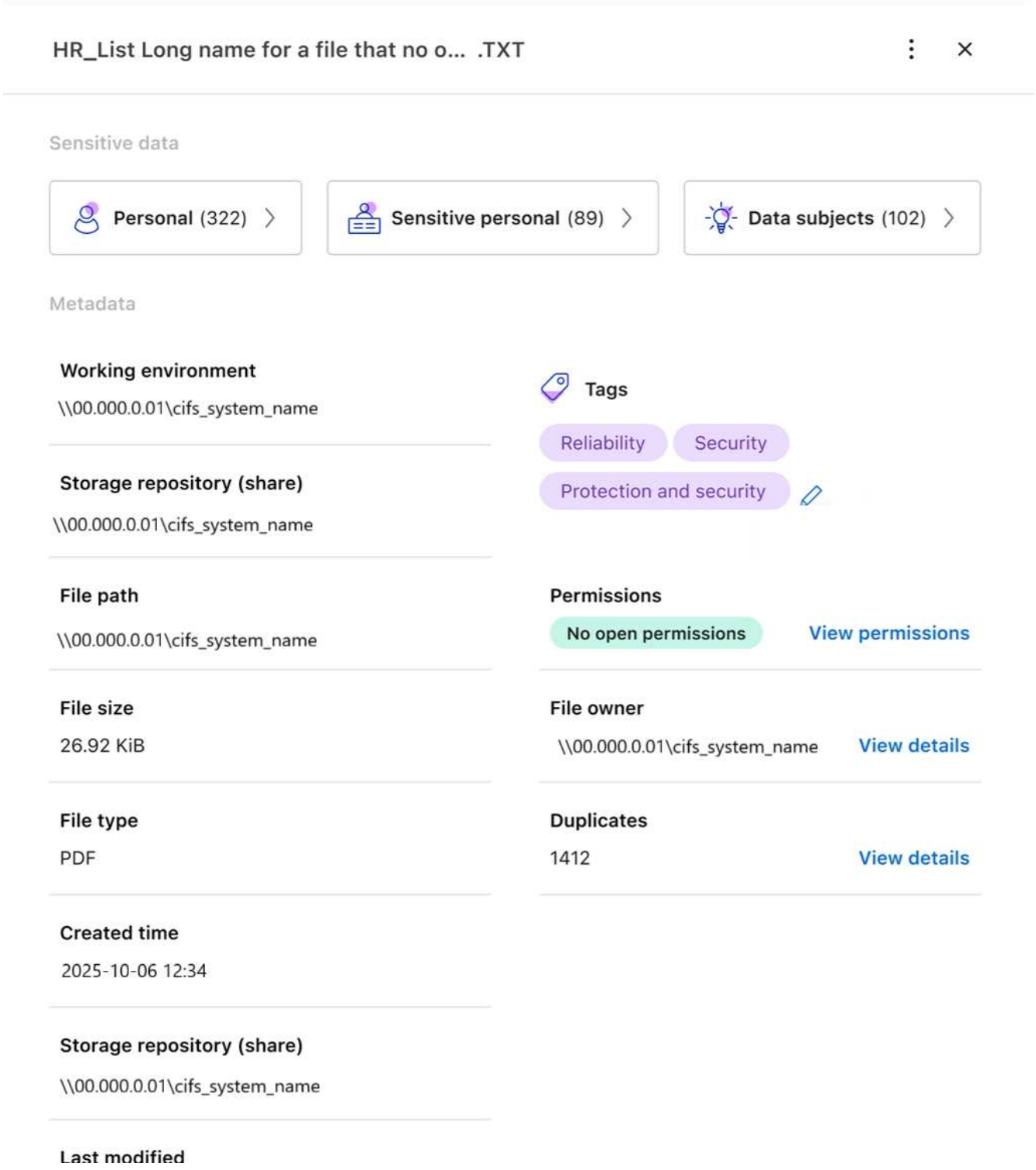
View file metadata

In addition to showing you the system and volume where the file resides, the metadata shows much more information, including the file permissions, file owner, and whether there are duplicates of this file. This information is useful if you're planning to create saved queries because you can see all the information that you can use to filter your data.

The availability of information depends on the data source. For example, volume name and permissions are not shared for database files.

Steps

1. From the Data Classification menu, select **Investigation**.
2. In the Data Investigation list on the right, select the down-caret on the right for any single file to view the file metadata.



3. Optionally, you can create or add a tag to the file with the **Create tag** button. Select an existing tag from the dropdown menu or add a new tag with the **+ Add** button. Tags can be used to filter data.

View user permissions for files and directories

To view a list of all users or groups who have access to a file or to a directory and the types of permissions they have, select **View all Permissions**. This option is available only for data in CIFS shares.

If you security identifiers (SIDs) instead of user and group names, you should integrate your Active Directory into Data Classification. For more information, see add Active Directory to Data Classification.

Steps

1. From the Data Classification menu, select **Investigation**.
2. In the Data Investigation list on the right, select the down-caret on the right for any single file to view the file metadata.
3. To view a list of all users or groups who have access to a file or to a directory and the types of permissions they have, in the Open Permissions field, select **View all Permissions**.

   Data Classification shows up to 100 users in the list.

4. Select the down-caret button for any group to see the list of users who are part of the group.

   You can expand one level of the group to see the users who are part of the group.

5. Select the name of a user or group to refresh the Investigation page so you can see all the files and directories that the user or group has access to.

Check for duplicate files in your storage systems

You can check whether duplicate files are being stored in your storage systems. This is useful if you want to identify areas where you can save storage space. It's also good to ensure certain files that have specific permissions or sensitive information are not unnecessarily duplicated in your storage systems.

Data Classification compares all files (excluding databases) for duplicates if they are:

- 1 MB or lager
- Or contain personal or sensitive personal information

Data Classification uses hashing technology to determine duplicate files. If any file has the same hash code as another file, the files are exact duplicates even if the file names are different.

Steps

1. From the Data Classification menu, select **Investigation**.
2. In Filter pane, select "File Size" along with "Duplicates" ("Has duplicates") to see which files of a certain size range are duplicated in your environment.
3. Optionally, download the list of duplicate files and send it to your storage administrator so they can decide which files, if any, can be deleted.
4. Optionally, you can delete, tag, or move the duplicate files. Select the files you want to perform an action on, then select the appropriate action.

View if a specific file is duplicated

You can see if a single file has duplicates.

Steps

1. From the Data Classification menu, select **Investigation**.
2. In the Data Investigation list, select ⌄ on the right for any single file to view the file metadata.

   If duplicates exist for a file, this information appears next to the *Duplicates* field.
3. To view the list of duplicate files and where they are located, select **View Details**.
4. In the next page select **View Duplicates** to view the files in the Investigation page.
5. Optionally, you can delete, tag, or move the duplicate files. Select the files you want to perform an action on, then select the appropriate action.

> You can use the "file hash" value provided in this page and enter it directly in the Investigation page to search for a specific duplicate file at any time - or you can use it in a saved query.

Download your report

You can download your filtered results in a CSV or JSON format.

There can be up to three report files downloaded if Data Classification is scanning files (unstructured data), directories (folders and file shares), and databases (structured data).

The files are split into files with a fixed number of rows or records:

- JSON: 100,000 records per report that takes about 5 minutes to generate
- CSV: 200,000 records per report that takes about 4 minutes to generate

> You can download a version of the CSV file to view in this browser. This version is limited to 10,000 records.

What's included in the downloadable report

The **Unstructured Files Data Report** includes the following information about your files:

- File name
- Location type
- System name
- Storage repository (for example, a volume, bucket, shares)
- Repository type
- File path
- File type
- File size (in MB)
- Created time
- Last modified
- Last accessed
- File owner
  - File owner data encompasses account name, SAM account name, and e-mail address when Active

Directory is configured.

- Category
- Personal information
- Sensitive personal information
- Open permissions
- Scan Analysis Error
- Deletion detection date

  The 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 don't contribute to the file number count that appears in the dashboard or on the Investigation page. The files only appear in the CSV reports.

The **Unstructured Directories Data Report** includes the following information about your folders and file shares:

- System type
- System name
- Directory name
- Storage repository (for example, a folder or file shares)
- Directory owner
- Created time
- Discovered time
- Last modified
- Last accessed
- Open permissions
- Directory type

The **Structured Data Report** includes the following information about your database tables:

- DB Table name
- Location type
- System name
- Storage repository (for example, a schema)
- Column count
- Row count
- Personal information
- Sensitive personal information

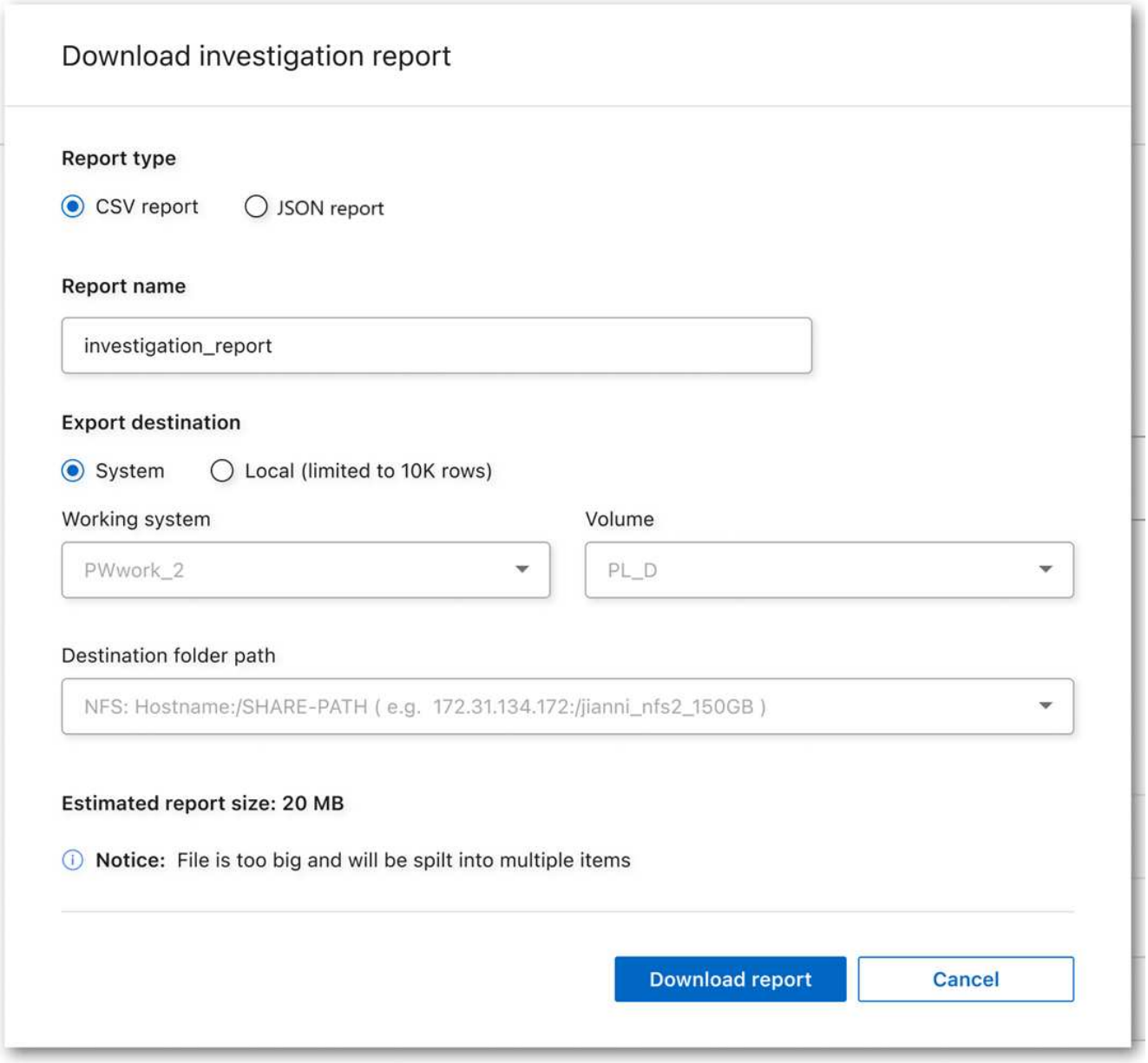
Steps to generate the report

1. From the Data Investigation page, select the button on the top, right of the page.
2. Choose the report type: CSV or JSON.
3. Enter a **Report name**.

4. To download the complete report, select **System** then choose the **System** and **Volume** from the respective dropdown menus. Provide a **Destination folder path**.

   To download the report in the browser, select **Local** . Note this option limits the report to the first 10,000 rows and is limited to the **CSV** format. You don't need to complete any other fields if you select **Local**.

5. Select **Download Report**.



Result

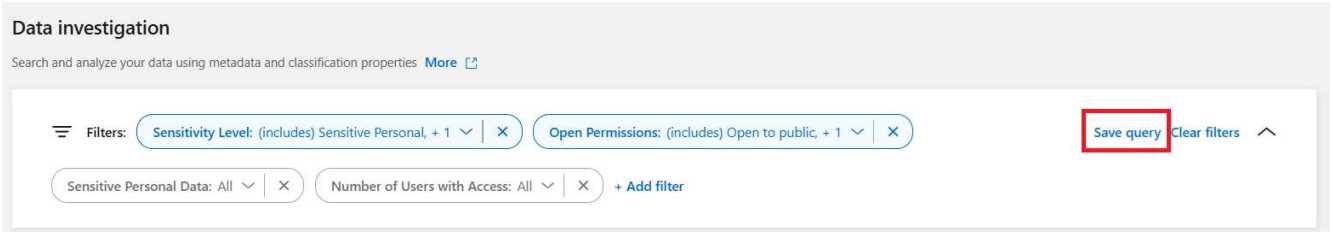
A dialog displays a message that the reports are being downloaded.

Create a saved query based on selected filters

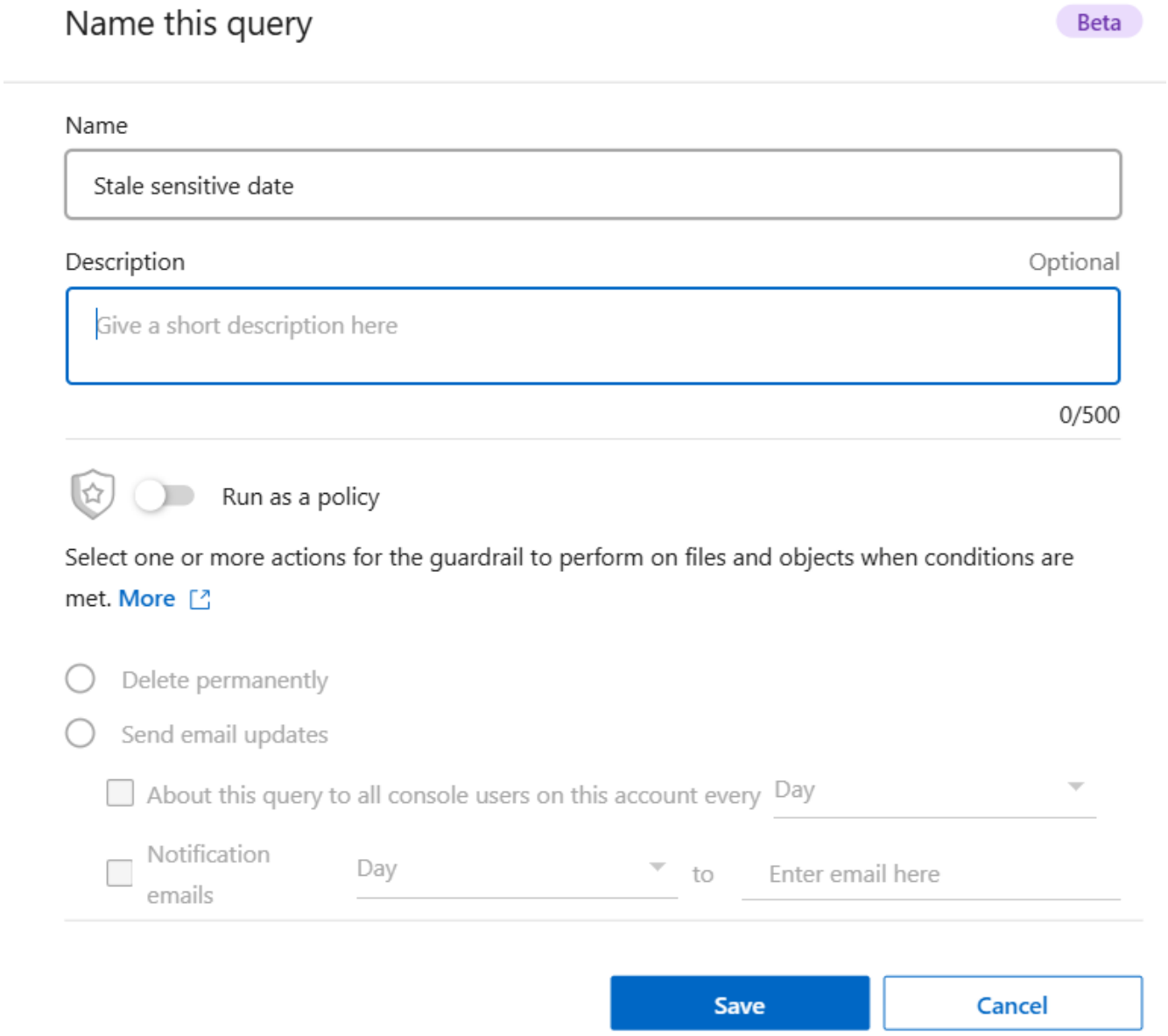
Steps

1. In the Investigation tab, define a search by selecting the filters you want to use. See Filtering data in the Investigation page for details.

2. Once you have all the filter characteristics set to your liking, select **Save query**.



3. Name the saved query and add a description. The name must be unique.
4. You can optionally save the query as policy:
   a. To save the query as a policy, switch the **Run as a policy** toggle.
   b. Choose to **Delete permanently** or **Send email updates**. If you choose email updates, you can email the query results to *all* Console users at daily, weekly, or monthly. Alternately, you can send the notification to specific email address at the same frequencies.
5. Select **Save**.



Once you've created the search or policy, you can view it in the **Saved queries** tab.

It can take up to 15 minutes for the results to appear on the Saved Queries page.

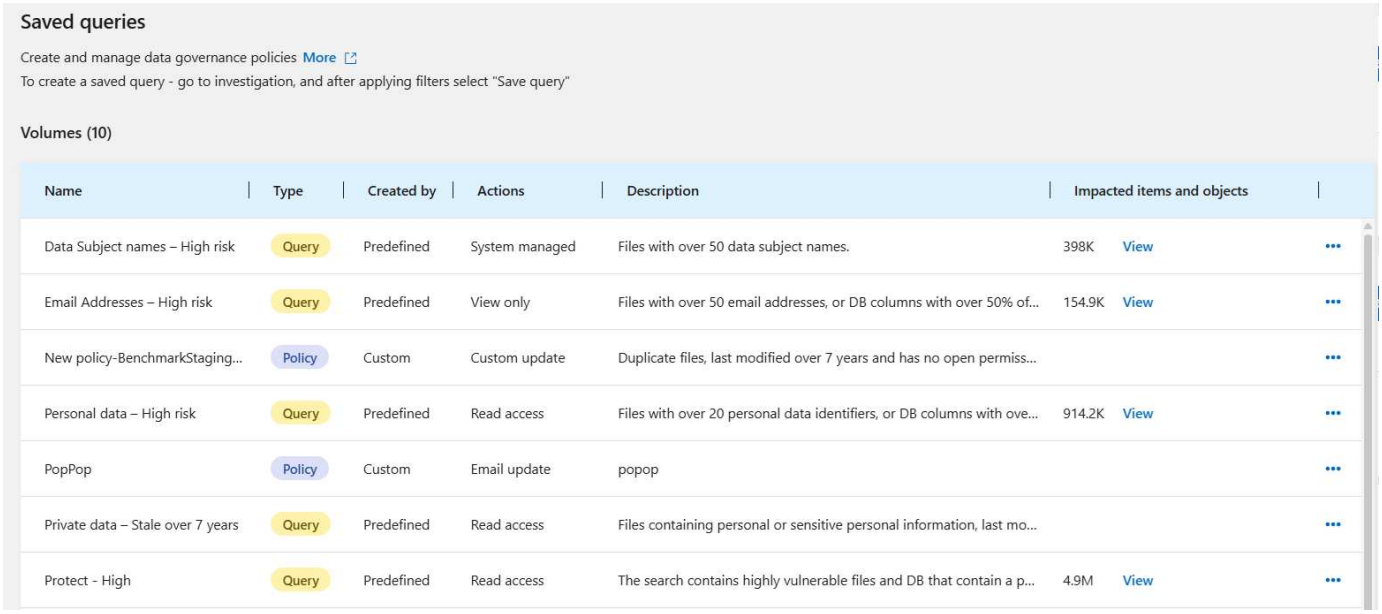
Manage saved queries with NetApp Data Classification

NetaApp Data Classification supports saving your search queries. With a saved query, you can create custom filters to sort through frequent queries of your data Investigation page. Data Classification also includes predefined saved queries based on common requests.

The **Saved queries** tab in the Compliance dashboard lists all the predefined and custom saved queries available on this instance of Data Classification.

Saved queries can also be saved as **policies**. Whereas queries filter data, policies allow you to act on the data. With a policy: you can delete discovered data or send email updates about the discovered data.

Saved queries also appear in the list of filters in the Investigation page.



View saved queries results in the Investigation page

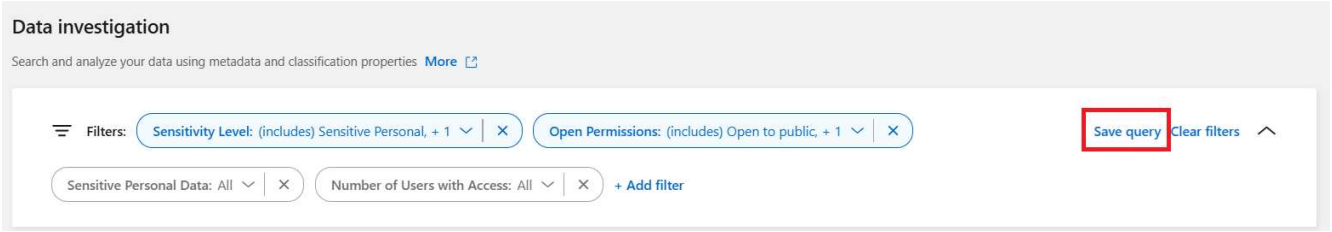
To display the results for a saved query in the Investigation page, select the button for a specific search then select **Investigate Results**.

Create saved queries and policies

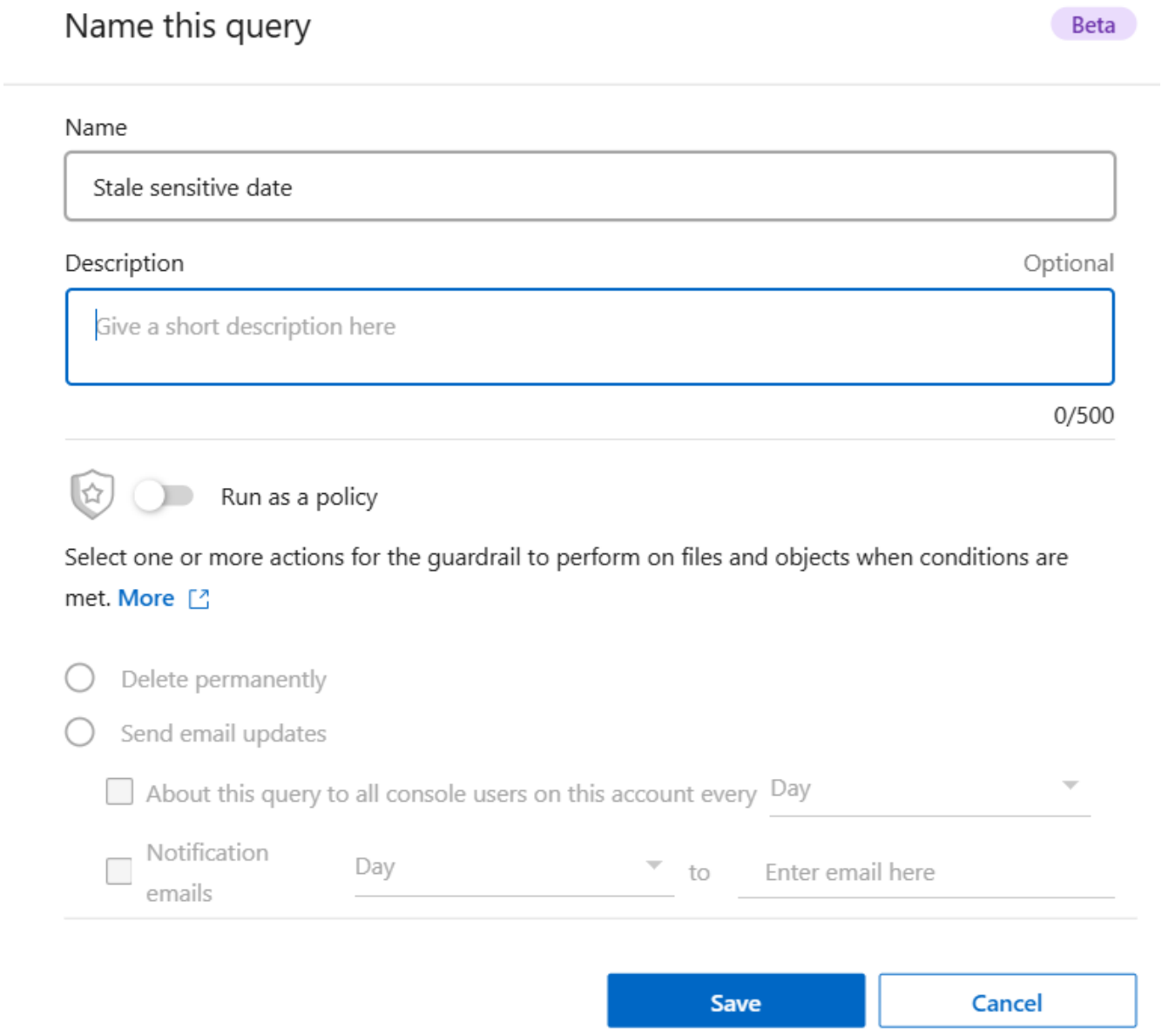
You can create your own custom saved queries that provide results for queries specific to your organization. Results are returned for all files and directories (shares and folders) that match the search criteria.

Steps

1. In the Investigation tab, define a search by selecting the filters you want to use. See Filtering data in the Investigation page for details.
2. Once you have all the filter characteristics set to your liking, select **Save query**.



3. Name the saved query and add a description. The name must be unique.
4. You can optionally save the query as policy:
   a. To save the query as a policy, switch the **Run as a policy** toggle.
   b. Choose to **Delete permanently** or **Send email updates**. If you choose email updates, you can email the query results to *all* Console users at daily, weekly, or monthly. Alternately, you can send the notification to specific email address at the same frequencies.
5. Select **Save**.



Once you've created the search or policy, you can view it in the **Saved queries** tab.

Edit saved queries or policies

You can modify the name and description of a saved query. You can also convert a query to a policy and vice

versa.

You cannot modify default saved queries. You cannot modify the filters of a saved query. You can alternately view the investigation results of a saved query, change or modify the filters, then save it as a new query or policy.

Steps

1. From the Saved queries page, select **Edit Search** for the search that you want to change.

2. Make the changes to the name and description fields. To only change the name and description fields.

   You can optionally convert the query to a policy or convert the policy to a saved query. Switch the **Run as a policy** toggle as needed.
   .. If you're converting the query to a policy, choose to **Delete permanently** or **Send email updates**. If you choose email updates, you can email the query results to *all* Console users at daily, weekly, or monthly. Alternately, you can send the notification to specific email address at the same frequencies.

3. Select **Save** to complete the changes.

Delete saved queries

You can delete any custom saved query or policy if you no longer need it. You can't delete default saved queries.

To delete a saved query, select the button for a specific search, select **Delete query**, then select **Delete query** again in the confirmation dialog.

Default queries

Data Classification provides the following system-defined search queries:

- **Data Subject names - High risk**

  Files with more than 50 data subject names

- **Email Addresses - High risk**

  Files with more than 50 email addresses or database columns with more than 50% of their rows containing email addresses

- **Personal data - High risk**

  Files with more than 20 personal data identifiers or database columns with more than 50% of their rows containing personal data identifiers

- **Private data - Stale over 7 years**

  Files containing personal or sensitive personal information, last modified more than 7 years ago

- **Protect - High**

  Files or database columns that contain a password, credit card information, IBAN number, or social security number

- **Protect - Low**

  Files that have not been accessed for more than 3 years

- **Protect - Medium**

  Files that contain files or database columns with personal data identifiers including ID numbers, tax identification numbers, drivers license numbers, medicinal IDs, or passport numbers

- **Sensitive Personal data - High risk**

  Files with more than 20 sensitive personal data identifiers or database columns with greater than 50% of their rows containing sensitive personal data

Change the NetApp Data Classification scan settings for your repositories

You can manage how your data is being scanned in each of your systems and data sources. You can make the changes on a "repository" basis; meaning you can make changes for each volume, schema, user, etc. depending on the type of data source you are scanning.

Some of the things you can change are whether a repository is scanned or not, and whether NetApp Data Classification is performing a mapping scan or a mapping & classification scan. You can also pause and resume scanning, for example, if you need to stop scanning a volume for a period of time.

View the scan status for your repositories

You can view the individual repositories that NetApp Data Classification is scanning (volumes, buckets, etc.) for each system and data source. You can also see how many have been "Mapped", and how many have been "Classified". Classification takes longer because the full AI identification is being performed on all data.

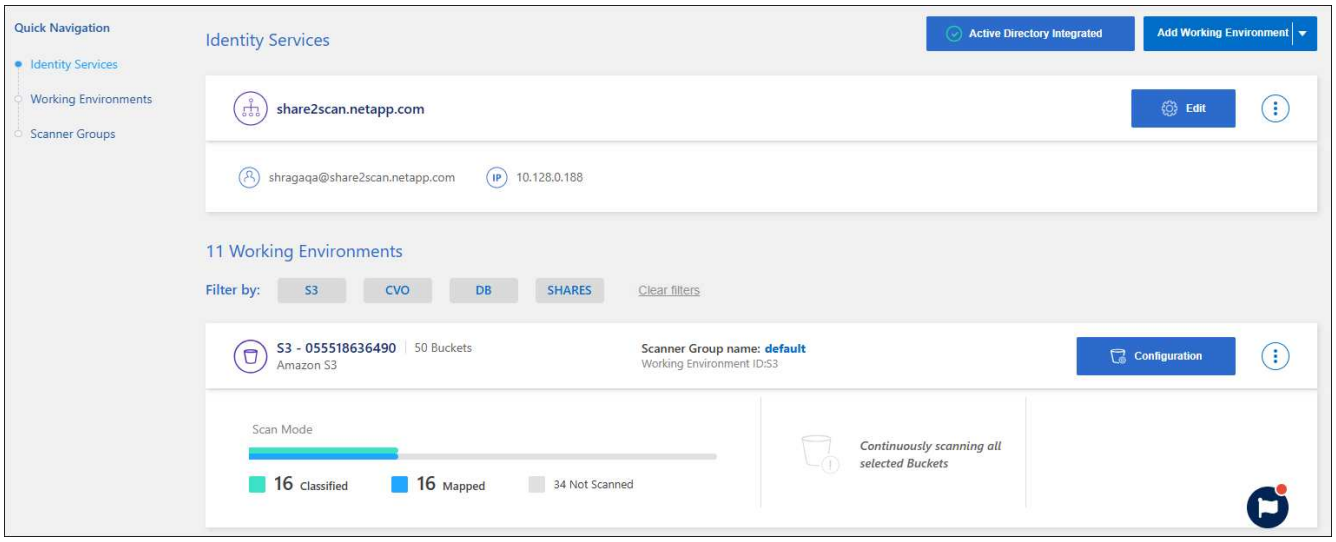
You can view the scanning status of each work environment on the Configuration page:

- **Initializing** (light blue dot): The map or classify configuration is activated. This appears briefly before transitioning to the "pending queue" status.
- **Pending queue** (orange dot): The scan task is waiting to be listed in the scanning queue.
- **Queued** (orange dot): The task was successfully added to the scanning queue. The system will start mapping or classifying the volume when its turn in the queue arrives.
- **Running** (green dot): The scan task, which was in the queue, is actively in progress on the selected storage repository.
- **Finished** (green dot): The scan of the storage repository is complete.
- **Paused** (gray dot): You paused scanning. Although the changes in the volume are not displayed in the system, the scanned insights remain available.

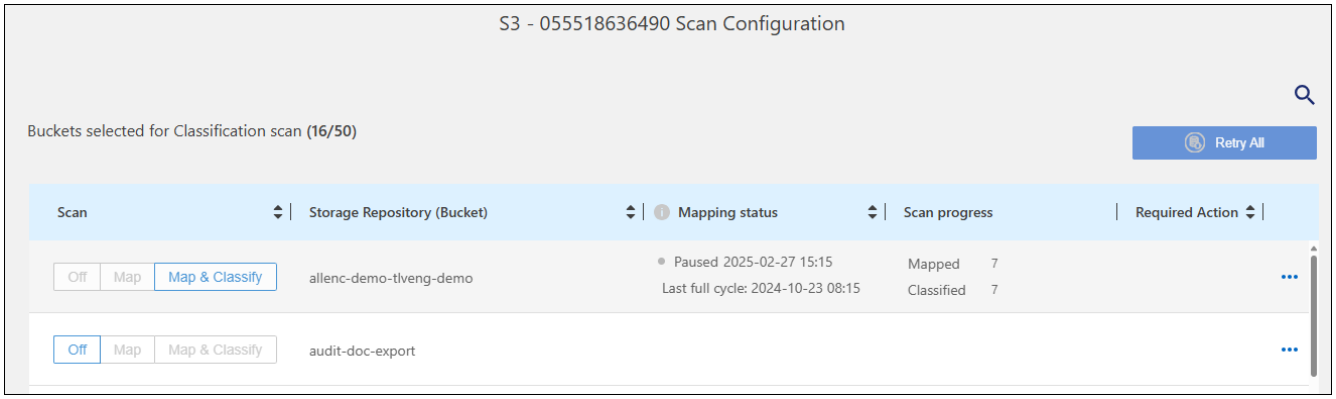
- **Error** (red dot): The scan cannot complete because it has encountered issues. If you need to complete an action, the error appears in the tooltip under the “Required action” column. Otherwise, the system shows an “error” status and tries to recover. When it finishes, the status changes.
- **Not scanning**: The volume configuration of "Off" was selected and the system is not scanning the volume.

Steps

1. From the Data Classification menu, select **Configuration**.



2. From the Configuration tab, select the **Configuration** button for the system.
3. In the Scan Configuration page, view the scan settings for all repositories.



4. During a scan, hover your cursor over the progress bar in the *Mapping status* column to view the number of files in the queue to be mapped or classified for that repository.

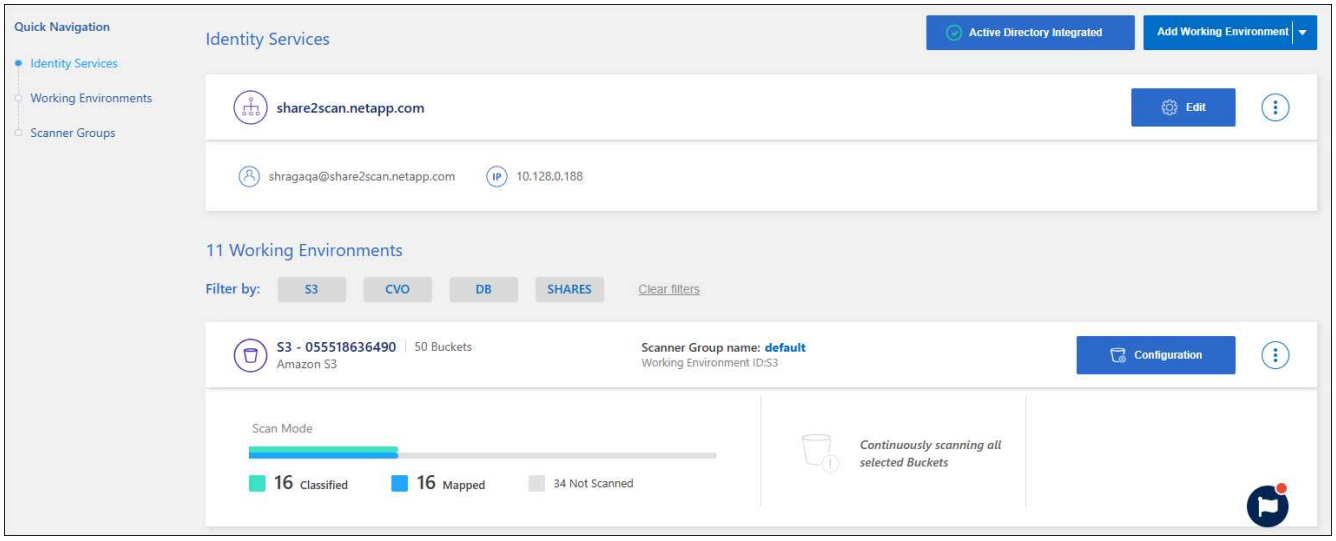
Change the type of scanning for a repository

You can start or stop mapping-only scans, or mapping and classification scans, in a system at any time from the Configuration page. You can also change from mapping-only scans to mapping and classification scans, and vice-versa.

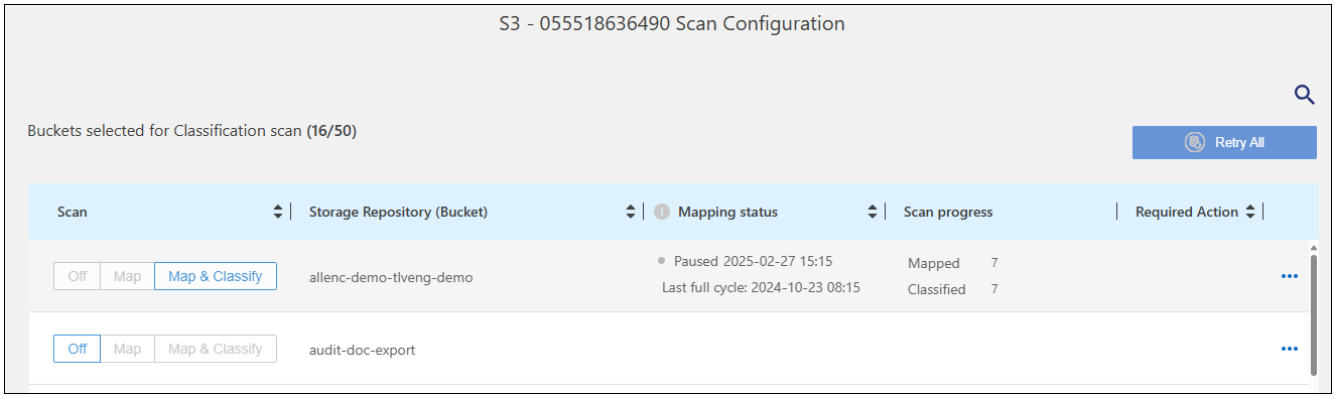
Databases can’t be set to mapping-only scans. Database scanning can be Off or On; where On is equivalent to Map & Classify.

Steps

1. From the Data Classification menu, select **Configuration**.
2. From the Configuration tab, select the **Configuration** button for the system.

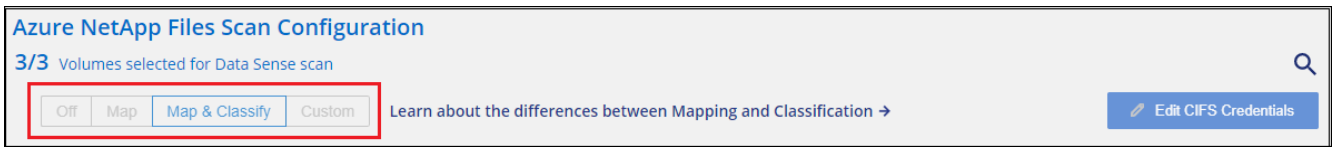


3. In the Scan Configuration page, change any of the repositories (buckets in this example) to perform **Map** or **Map & Classify** scans.



Certain types of systems enable you to change the type of scanning globally for all repositories using a button bar at the top of the page. This is valid for Cloud Volumes ONTAP, on-premises ONTAP, Azure NetApp Files, and Amazon FSx for ONTAP systems.

The example below shows this button bar for an Azure NetApp Files system.



Prioritize scans

You can prioritize the most important mapping-only scans or map & classify scans to ensure high priority scans are completed first.

By default, scans are queued based on the order in which they are initiated. With the ability to prioritize scans, you can move scans to the front of the queue. Multiple scans can be prioritized. Priority is designated in a first-

in, first-out order, meaning the first scan you prioritize moves to the front of the queue; the second scan you prioritize becomes second in the queue, and so forth.

Priority is granted on a one-time basis. Automatic rescans of mapping data occur in the default order.

Steps

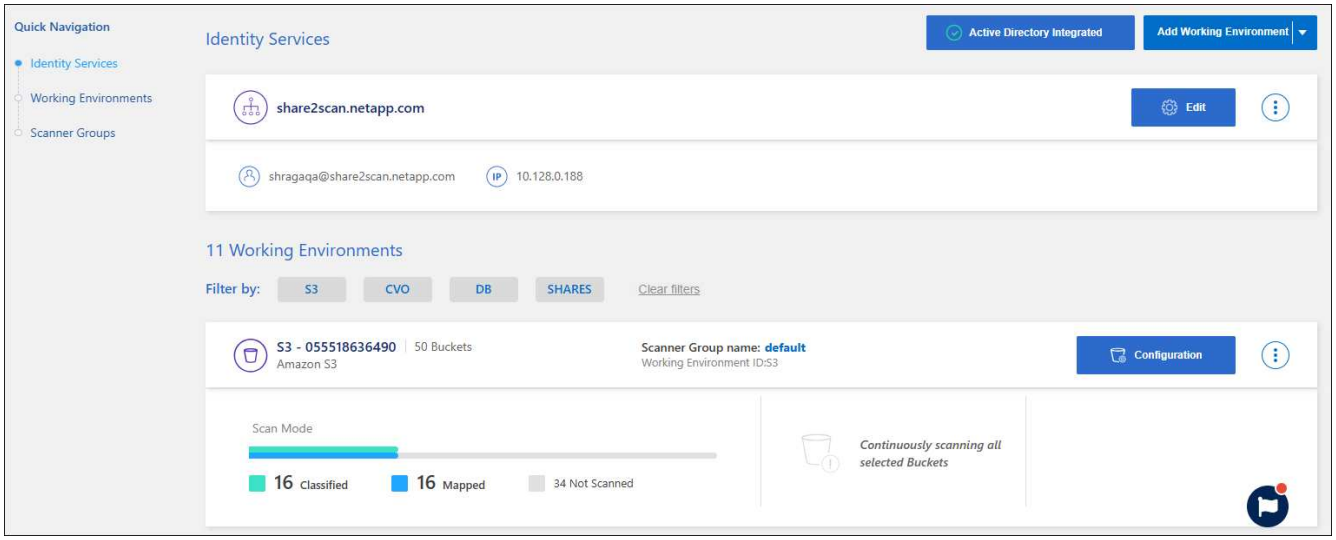
1. From the Data Classification menu, select **Configuration**.
2. Select the resources you want to prioritize.
3. From the Actions … option, select **Prioritize scan**.

Stop scanning for a repository

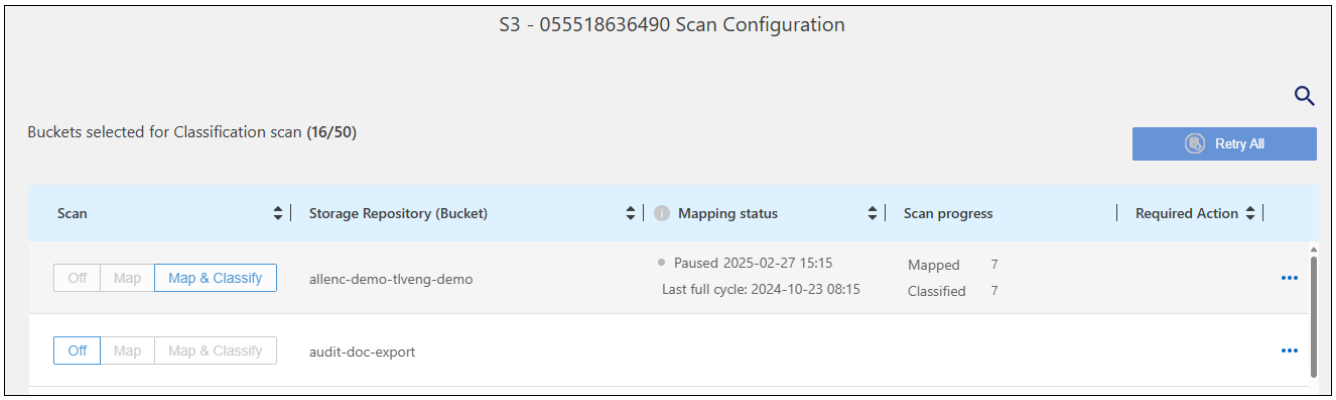
You can stop scanning a repository (for example, a volume) if you no longer need to monitor it for compliance. You do this by turning scanning "off". When scanning is turned off, all the indexing and information about that volume is removed from the system, and charging for scanning the data is stopped.

Steps

1. From the Data Classification menu, select **Configuration**.
2. From the Configuration tab, select the **Configuration** button for the system.



3. In the Scan Configuration page select **Off** to stop scanning for a particular bucket.



Pause and resume scanning for a repository

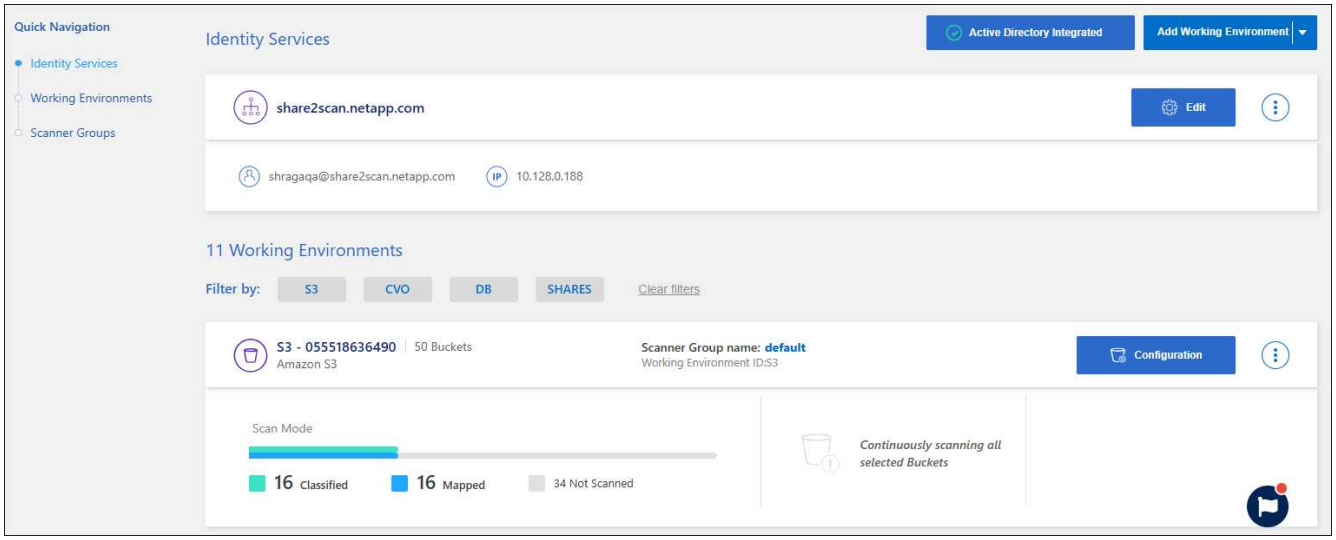
You can "pause" scanning on a repository if you want to temporarily stop scanning certain content. Pausing scanning means that Data Classification won't perform any future scans for changes or additions to the repository. All current scan results remain accessible in Data Classification.

If you pause scans, it does not eliminate billing charges because the data is still on the system.

You can resume scanning at any time.

Steps

1. From the Data Classification menu, select **Configuration**.
2. From the Configuration tab, select the **Configuration** button for the system.



3. In the Scan Configuration page, select the Actions ••• icon.
4. Select **Pause** to pause scanning for a volume, or select **Resume** to resume scanning for a volume that had been previously paused.

View NetApp Data Classification compliance reports

NetApp Data Classification provides reports that you can use to better understand the status of your organization's data privacy program.

By default, the Data Classification dashboards display compliance and governance data for all systems, databases, and data sources. If you want to view reports that contain data for only some of the systems, you can filter to see just them.

- Compliance reports are only available if you perform a full classification scan on your data sources. Data sources that have had a mapping-only scan can only generate the Data Mapping Report.
- NetApp cannot guarantee 100% accuracy of the personal data and sensitive personal data that Data Classification identifies. You should always validate the information by reviewing the data.

The following reports are available for Data Classification:

- **Data discovery assessment report**: Provides a high-level analysis of the scanned environment to highlight the system's findings and to show areas of concern and potential remediation steps. This report is available in the Governance dashboard.
- **Full data mapping overview report**: Provides information about the size and number of files in your systems. This includes usage capacity, age of data, size of data, and file types. This report is available in the Governance dashboard.
- **Data Subject Access Request report**: Enables you to extract a report of all files that contain information regarding a data subject's specific name or personal identifier. This report is available in the Compliance dashboard.
- **HIPAA report**: Helps you identify the distribution of health information across your files. This report is available in the Compliance dashboard.
- **PCI DSS report**: Helps you identify the distribution of credit card information across your files. This report is available in the Compliance dashboard.
- **Privacy risk assessment report**: Provides privacy insights from your data and a privacy risk score. This report is available in the Compliance dashboard.
- **Reports on a specific information type**: Reports are available that include details about the identified files that contain personal data and sensitive personal data. You can also see files broken down by category and file type.

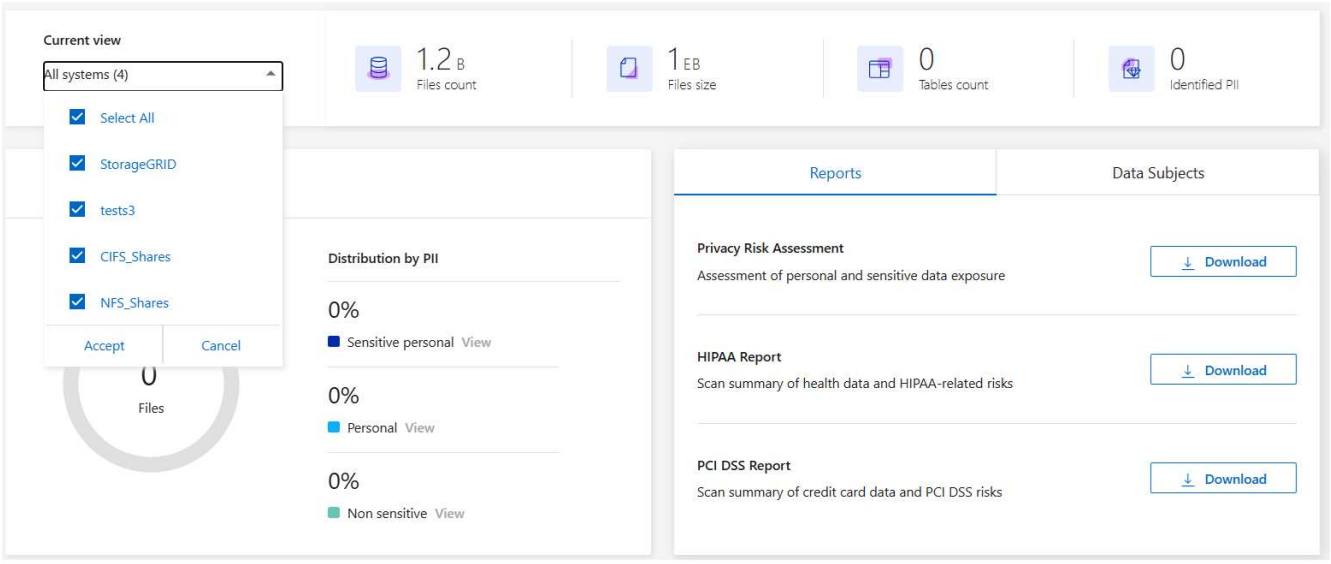
Select the systems for reports

You can filter the contents of the Data Classification Compliance dashboard to see compliance data for all systems and databases, or for just specific systems.

When you filter the dashboard, Data Classification scopes the compliance data and reports to just those systems that you selected.

Steps

1. From the Data Classification menu, select **Compliance**.
2. Select the systems filter drop-down then select the systems.
3. Select **Accept** to confirm your selection.



Data Subject Access Request Report

Privacy regulations such as the European GDPR grant data subjects (such as customers or employees) the right to access their personal data. When a data subject requests this information, this is known as a DSAR (data subject access request). Organizations are required to respond to these requests "without undue delay", and at the latest within one month of receipt.

You can respond to a DSAR by searching for a subject's full name or known identifier (such as an email address) and then downloading a report. The report is designed to aid in your organization's requirement to comply with GDPR or similar data privacy laws.

How can Data Classification help you respond to a DSAR?

When you perform a data subject search, Data Classification finds all of the files that have that person's name or identifier in it. Data Classification checks the latest pre-indexed data for the name or identifier. It doesn't initiate a new scan.

After the search is complete, you can then download the list of files for a Data Subject Access Request report. The report aggregates insights from the data and puts it into legal terms that you can send back to the person.

Data subject search is not currently supported within databases.

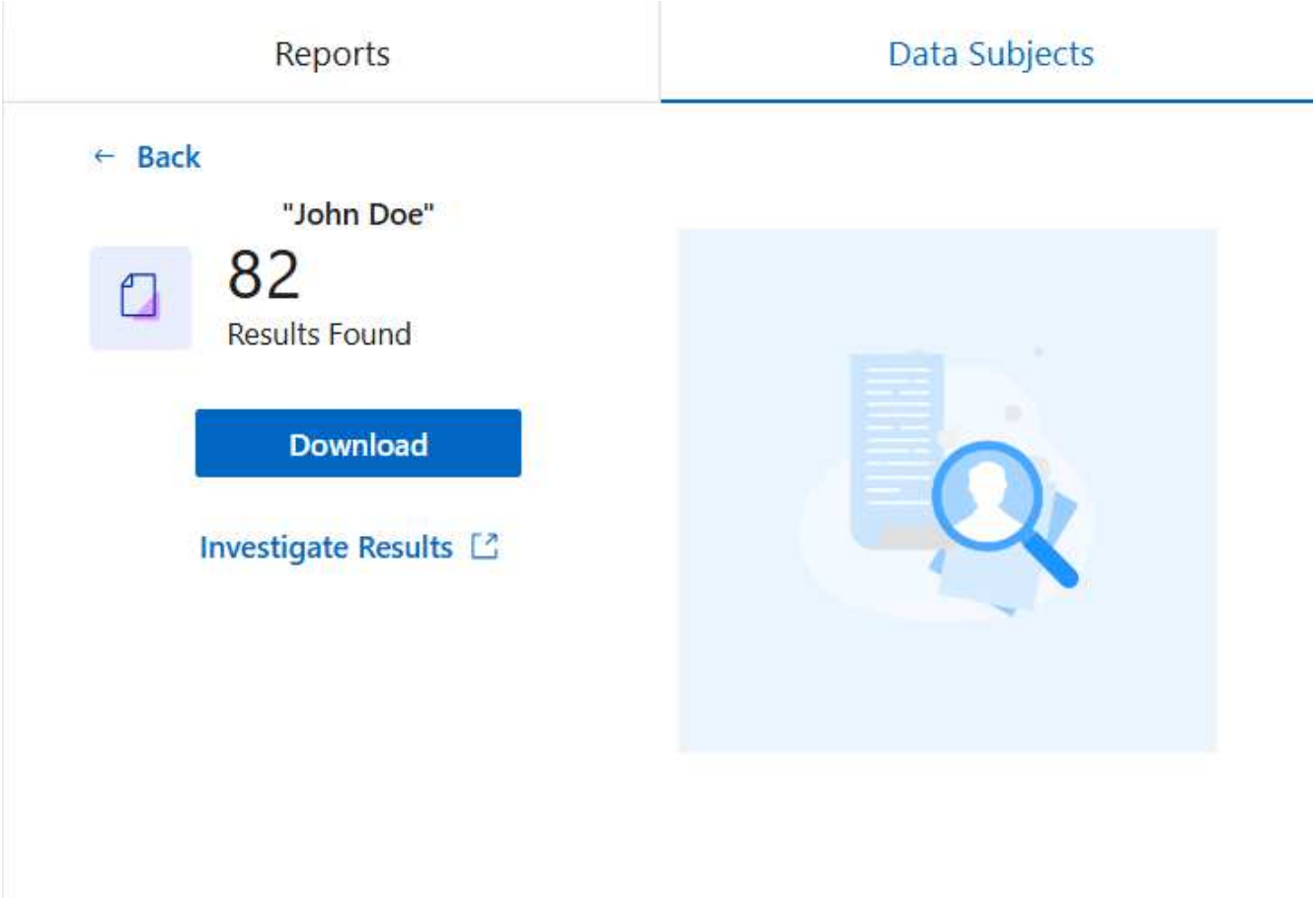
Search for data subjects and download reports

Search for the data subject's full name or known identifier and then download a file list report or DSAR report. You can search by any personal information type.

English, German, Japanese, and Spanish are supported when searching for the names of data subjects. Support for more languages will be added later.

Steps

1. From the Data Classification menu, select **Compliance**.
2. From the Compliance page, locate the **Data Subjects** tab.
3. In the **Data Subjects** section, enter a name or known identifier then select **Search**.
4. When the search completes, select **Download** to access the data subject access request response. Select **Investigate Results** to view more information in the Data Investigation page.

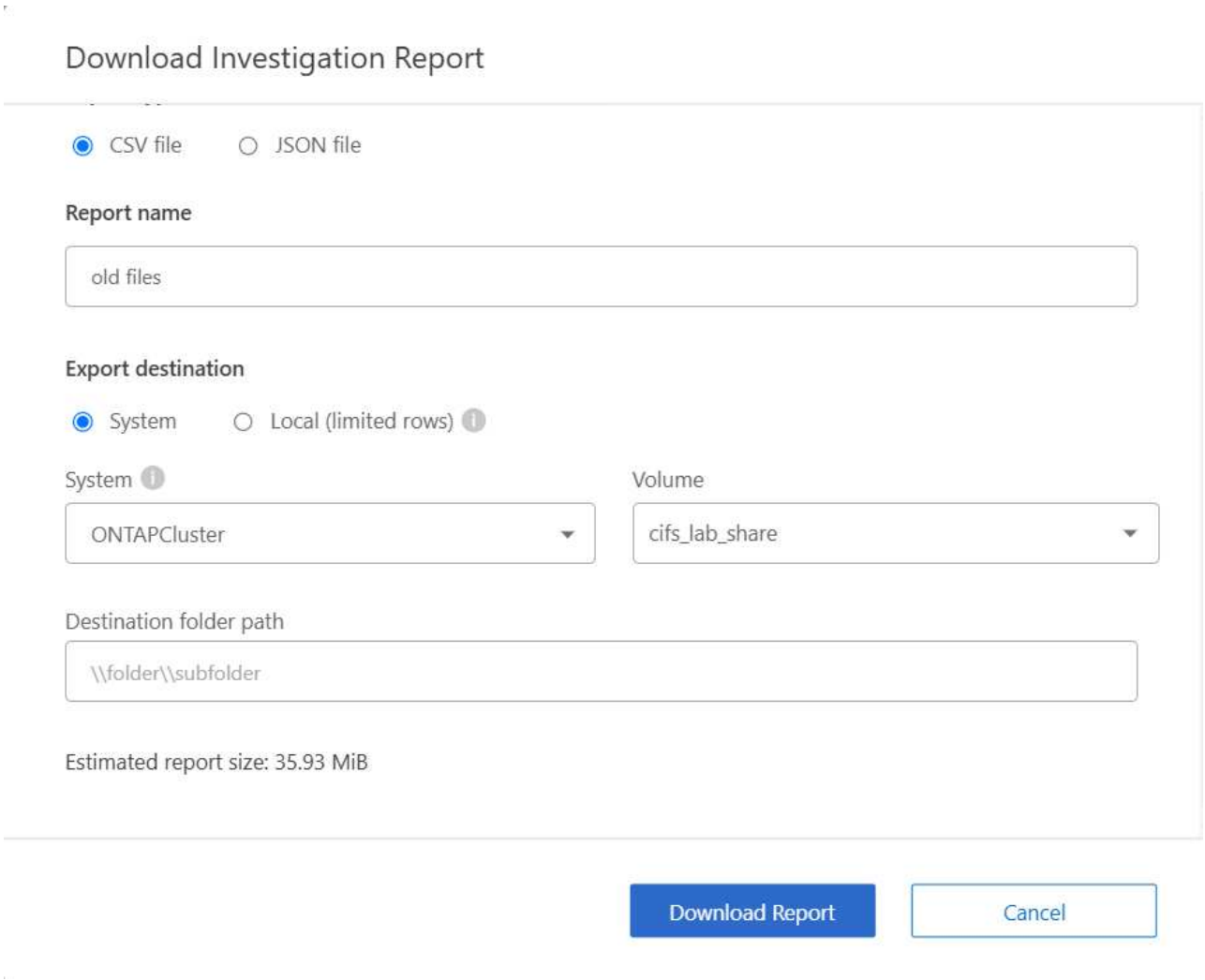


5. Review the results in Data Classification or download them as a report by selecting the download icon.
   a. When you select the download icon, configure your download settings:
      - Choose the film format: CSV or JSON
      - Enter a **Report name**
      - Choose the export destination: **System** or your **Local** machine.

        If you choose system, all data downloads. You must also select the **System**, **Volume**, and **Destination folder path**.

        If you choose **Local**, it limits the report to the first 10,000 rows of unstructured data; 5,000 rows of unstructured data, and 1,000 rows of structured data.

   b. Select **Download Report** to initiate the download.



Health Insurance Portability and Accountability Act (HIPAA) Report

The Health Insurance Portability and Accountability Act (HIPAA) Report can help you identify files containing health information. It is designed to aid in your organization's requirement to comply with HIPAA data privacy laws. The information Data Classification looks for includes:

- Health reference pattern
- ICD-10-CM Medical code
- ICD-9-CM Medical code
- HR - Health category
- Health Application Data category

The report includes the following information:

- Overview: How many files contain health information and in which systems.
- Encryption: The percentage of files containing health information that are on encrypted or unencrypted systems. This information is specific to Cloud Volumes ONTAP.
- Ransomware Protection: The percentage of files containing health information that are on systems that do or don't have ransomware protection enabled. This information is specific to Cloud Volumes ONTAP.
- Retention: The timeframe in which the files were last modified. This is helpful because you shouldn't keep

health information for longer than you need to process it.

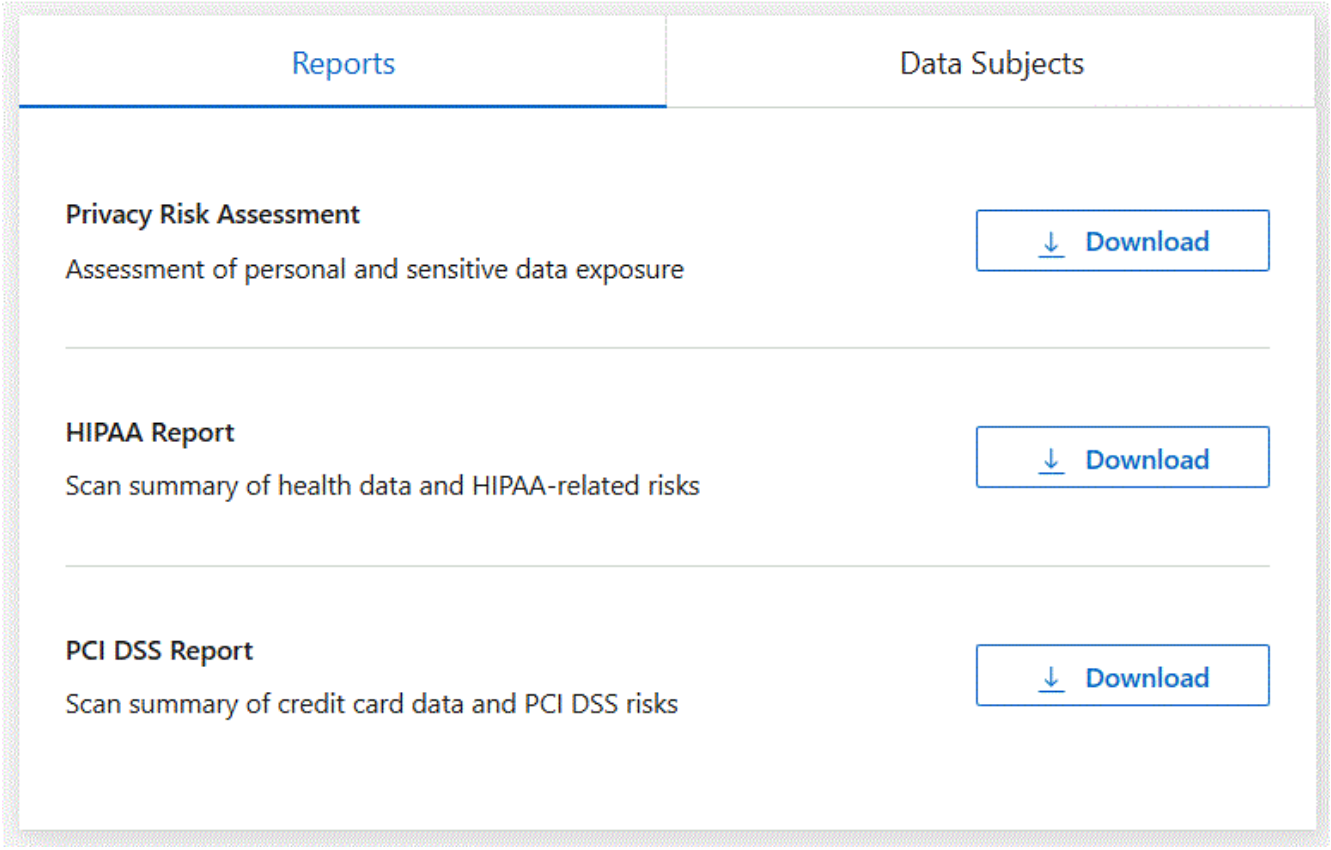
- Distribution of Health Information: The systems where the health information was found and whether encryption and ransomware protection are enabled.

Generate the HIPAA Report

Go to the Compliance tab to generate the report.

Steps

1. From the Data Classification menu, select **Compliance**.
2. Locate the **Reports pane**. Select the download icon next to **HIPAA Report**.



Result

Data Classification generates a PDF report.

Payment Card Industry Data Security Standard (PCI DSS) report

The Payment Card Industry Data Security Standard (PCI DSS) report can help you identify the distribution of credit card information across your files.

The report includes the following information:

- Overview: How many files contain credit card information and in which systems.
- Encryption: The percentage of files containing credit card information that are on encrypted or unencrypted systems. This information is specific to Cloud Volumes ONTAP.
- Ransomware Protection: The percentage of files containing credit card information that are on systems that

do or don't have ransomware protection enabled. This information is specific to Cloud Volumes ONTAP.

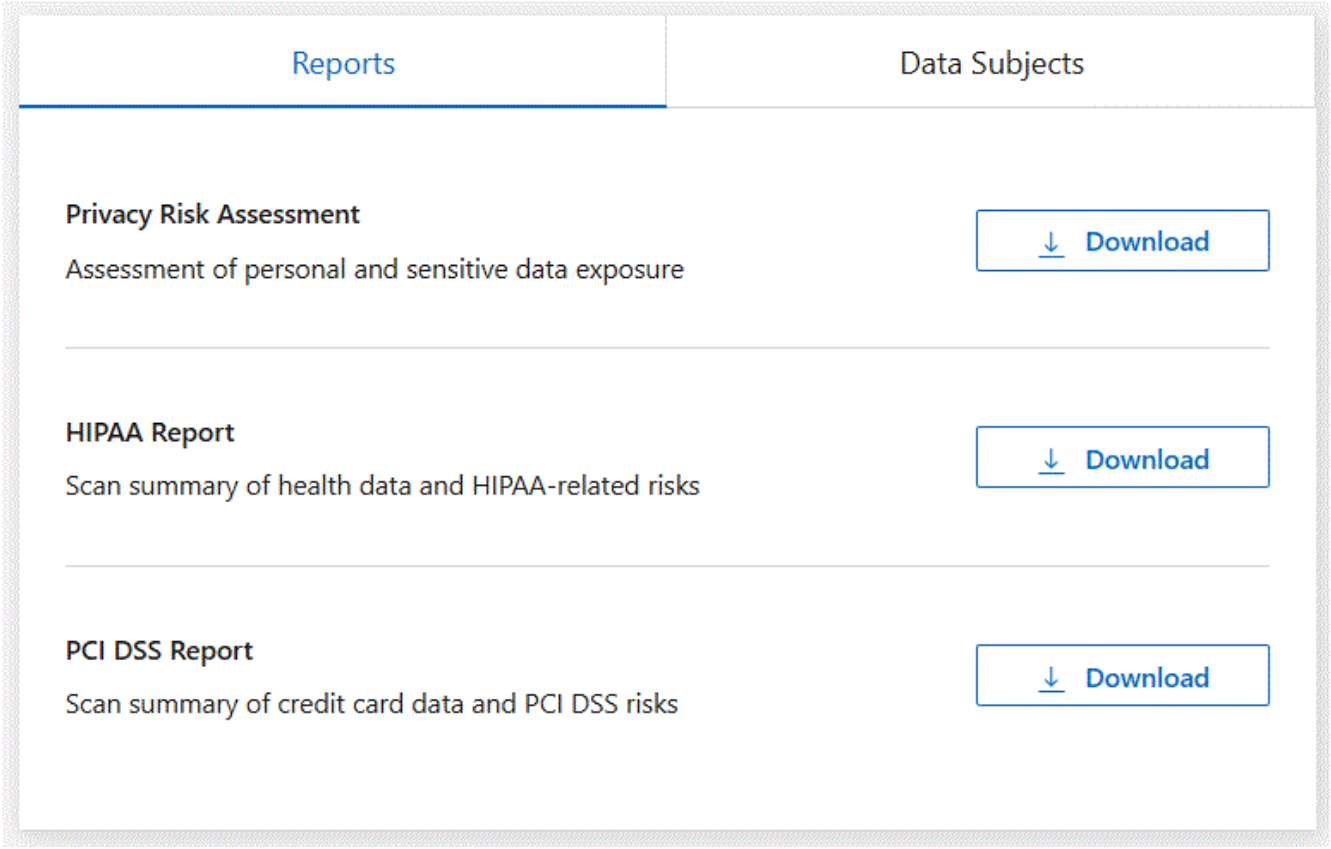
- Retention: The timeframe in which the files were last modified. This is helpful because you shouldn't keep credit card information for longer than you need to process it.
- Distribution of Credit Card Information: The systems where the credit card information was found and whether encryption and ransomware protection are enabled.

Generate the PCI DSS Report

Go to the Compliance tab to generate the report.

Steps

1. From the Data Classification menu, select **Compliance**.
2. Locate the **Reports pane**. Select the download icon next to **PCI DSS Report**.



Result

Data Classification generates a PDF report that you can review and send to other groups as needed.

Privacy Risk Assessment Report

The Privacy Risk Assessment Report provides an overview of your organization's privacy risk status, as required by privacy regulations such as GDPR and CCPA.

The report includes the following information:

- Compliance status: A severity score and the distribution of data, whether it's non-sensitive, personal, or sensitive personal.

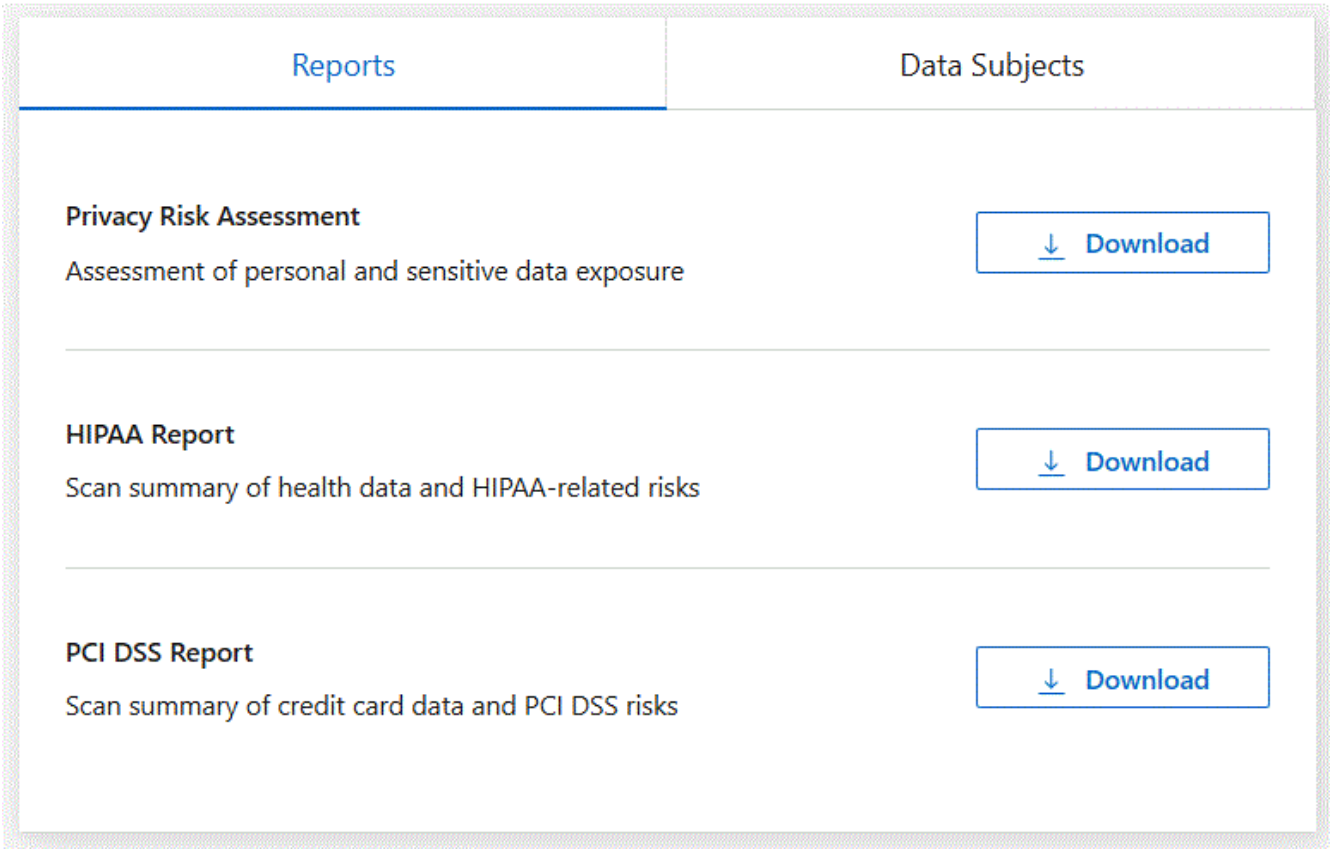
- Assessment overview: A breakdown of the types of personal data found, as well as the categories of data.
- Data subjects in this assessment: The number of people, by location, for which national identifiers were found.

Generate the Privacy Risk Assessment Report

Go to the Compliance tab to generate the report.

Steps

1. From the Data Classification menu, select **Compliance**.
2. Locate the **Reports pane**. Select the download icon next to **Privacy Risk Assessment Report**.



Result

Data Classification generates a PDF report that you can review and send to other groups as needed.

Severity score

Data Classification calculates the severity score for the Privacy Risk Assessment Report on the basis of three variables:

- The percentage of personal data out of all data.
- The percentage of sensitive personal data out of all data.
- The percentage of files that include data subjects, determined by national identifiers such as national IDs, Social Security numbers, and tax ID numbers.

The logic used to determine the score is as follows:

Severity score	Logic
0	All three variables are exactly 0%
1	One of the variables are larger than 0%
2	One of the variables are larger than 3%
3	Two of the variables are larger than 3%
4	Three of the variables are larger than 3%
5	One of the variables are larger than 6%
6	Two of the variables are larger than 6%
7	Three of the variables are larger than 6%
8	One of the variables are larger than 15%
9	Two of the variables are larger than 15%
10	Three of the variables are larger than 15%

Monitor health of NetApp Data Classification

:nofooter
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: /tmp/d20260206-1555642-bufybq/source/./../media/

The NetApp Data Classification Health Monitor dashboard provides real-time monitoring and insights into performance. The Health Monitor captures information about your Data Classification infrastructure, system health, usage metrics, and utilization data, enabling you to identify and remediate issues.

Health Monitor insights

The Health Monitor dashboard presents information in four categories.

- **Infrastructure status**

  View information including the version status, system stability, deployment type, and machine scale.

- **Problematic containers**

  Review the problematic containers field for insights into containers that are stopped or restarting frequently. Use this information to investigate the specific containers.

- **System information**

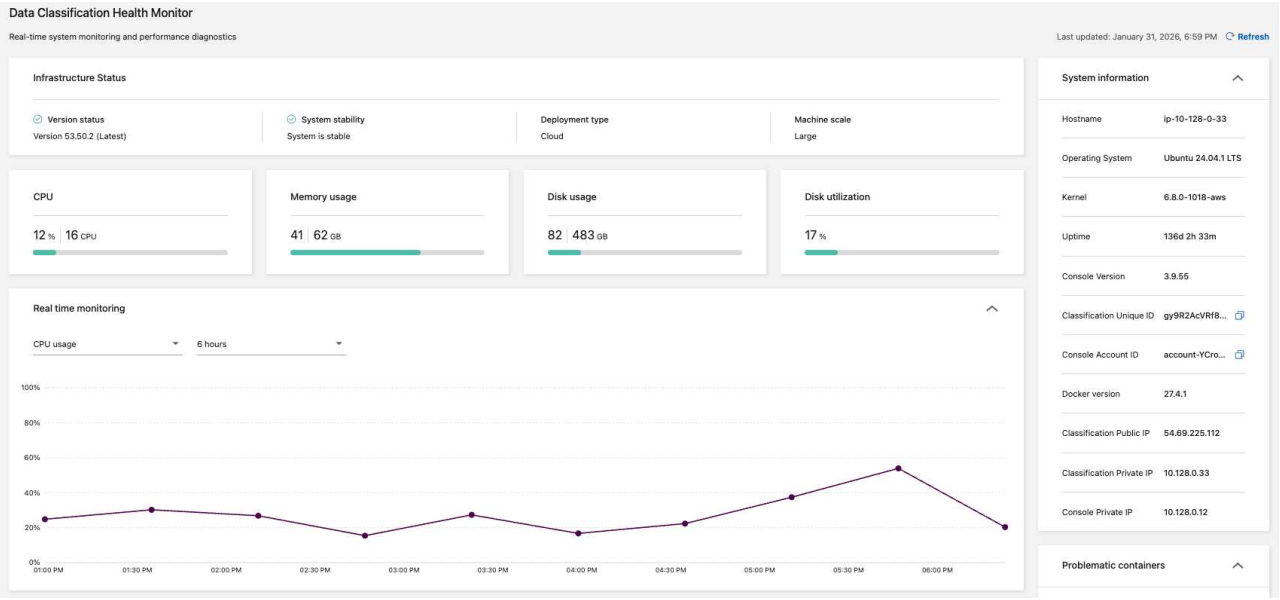
  The system information panel captures critical information about the NetApp Console and Data Classification such as the public and private IP addresses, host name, operating system, Console version, and Console ID.

- **Usage and utilization**

Review the CPU usage, disk utilization, disk usage, and memory usage. These values are displayed in storage units (GB) or percentages of total use. If any fields display a warning, select the warning for information and remediation recommendations.

Access the Health Monitor dashboard

1. In Data Classification, select **Configuration**.
2. Under the **Configuration** heading, select **Data Classification health monitor**.
3. In the Health Monitor dashboard, you can:
   - Review the usage and utilization. If any usage or utilization metrics display warnings, select the warning for recommendations to resolve the issue.
   - Toggle the graph to display CPU usage, disk utilization, disk usage, and memory usage. You can change the x-axis to display content over hours (6, 12, or 24) or days (2, 7, or 14).
   - Refresh the dashboard to view the most recent data metrics.



Copyright information

Trademark information