# Gain insight into data privacy

## Cloud Manager 3.7

NetApp
June 06, 2022

# Table of Contents

# Gain insight into data privacy

## Learn about Cloud Compliance

Cloud Compliance is a data privacy and compliance service for Cloud Volumes ONTAP in AWS and Azure. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data across Cloud Volumes ONTAP systems.

Cloud Compliance is currently available as a Controlled Availability release.

Learn about the use cases for Cloud Compliance.

### Features

Cloud Compliance provides several tools that can help you with your compliance efforts. You can use Cloud Compliance to:

- Identify Personal Identifiable Information (PII)
- Identify a wide scope of sensitive information as required by GDPR, CCPA, PCI, and HIPAA privacy regulations
- Respond to Data Subject Access Requests (DSAR)

### Cost

Cloud Compliance is an add-on service for Cloud Volumes ONTAP provided by NetApp at no extra cost. Activating Cloud Compliance requires deploying a cloud instance, which you will be charged for by your cloud provider. There are no charges for data ingress or egress because data doesn't flow outside of the network.

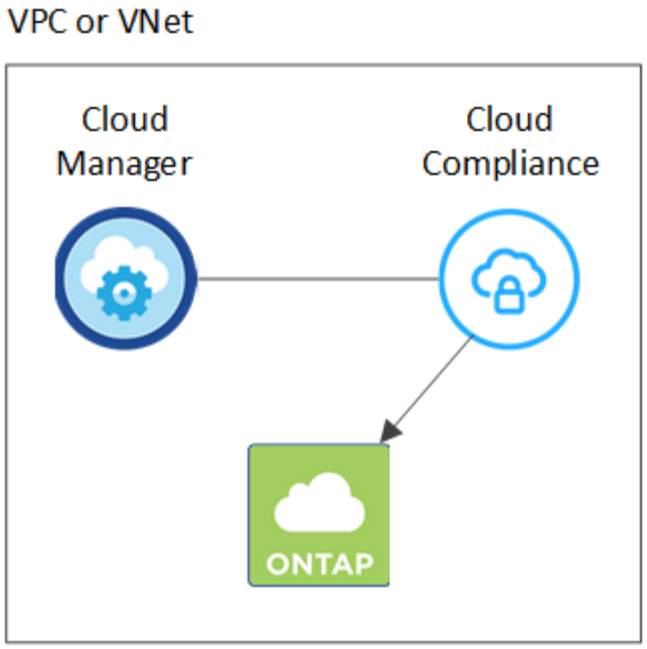
### How Cloud Compliance works

At a high-level, Cloud Compliance works like this:

1. You enable Cloud Compliance on one or more Cloud Volumes ONTAP systems.
2. Cloud Compliance scans the data using an AI learning process.
3. In Cloud Manager, you click **Compliance** and use the provided dashboard and reporting tools to help you in your compliance efforts.

### The Cloud Compliance instance

When you enable Cloud Compliance on one or more Cloud Volumes ONTAP systems, Cloud Manager deploys a Cloud Compliance instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request.




Note the following about the instance:

- In Azure, Cloud Compliance runs on a Standard_D16s_v3 VM with a 512 GB disk.
- In AWS, Cloud Compliance runs on an m5.4xlarge instance with a 500 GB io1 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

- The instance is named *CloudCompliance* with a generated hash (UUID) concatenated to it. For example: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Only one Cloud Compliance instance is deployed per Cloud Manager system.
- Upgrades of Cloud Compliance software is automated—you don't need to worry about it.

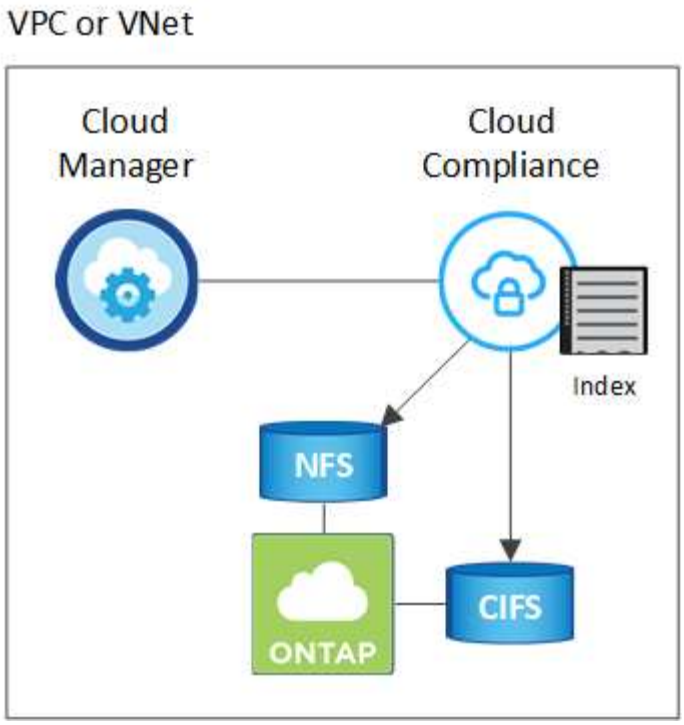
The instance should remain running at all times because Cloud Compliance continuously scans the data on Cloud Volumes ONTAP systems.

## How scans work

After you enable Cloud Compliance, it immediately starts scanning your data to identify personal and sensitive data.

Cloud Compliance connects to Cloud Volumes ONTAP like any other client by mounting NFS and CIFS volumes. NFS volumes are automatically accessed as read-only, while you need to provide Active Directory credentials to scan CIFS volumes.

Cloud Compliance scans the unstructured data on each volume for a range of personal information. It maps your organizational data, categorizes each file, and identifies and extracts entities and predefined patterns in the data. The result of the scan is an index of personal information, sensitive personal information, and data categories.




After the initial scan, Cloud Compliance continuously scans each volume to detect incremental changes (this is why it's important to keep the instance running).

You can turn scans on and off at the working environment level, but not at the volume level. Learn how.

## Information that Cloud Compliance indexes

Cloud Compliance collects, indexes, and assigns categories to unstructured data (files). The data that Cloud Compliance indexes includes the following:

**Standard metadata**

Cloud Compliance collects standard metadata about files: the file type, its size, creation and modification dates, and so on.

**Personal data**

Personally identifiable information such as email addresses, identification numbers, or credit card numbers. Learn more about personal data.

**Sensitive personal data**

Special types of sensitive information, such as health data, ethnic origin, or political opinions, as defined by GDPR and other privacy regulations. Learn more about sensitive personal data.

**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. Learn more about categories.

**Name entity recognition**

Cloud Compliance uses AI to extract natural persons' names from documents. Learn about responding to Data Subject Access Requests.

## Networking overview

Cloud Manager deploys the Cloud Compliance instance with a private IP address and a security group that enables inbound HTTP connections from Cloud Manager. This connection enables you to access the Cloud Compliance dashboard from the Cloud Manager interface.

Outbound rules are completely open. The instance connects to Cloud Volumes ONTAP systems and to the internet through a proxy from Cloud Manager. Internet access is needed to upgrade the Cloud Compliance software and to send usage metrics.

If you have strict networking requirements, learn about the endpoints that Cloud Compliance contacts.

The indexed data never leaves the Cloud Compliance instance—the data isn't relayed outside of your virtual network and it isn't sent to Cloud Manager.

## User access to compliance information

Cloud Manager Admins can view compliance information for all working environments.

Workspace Admins can view compliance information only for systems that they have permissions to access. If a Workspace Admin can't access a working environment in Cloud Manager, then they can't see any compliance information for the working environment in the Compliance tab.

Learn more about Cloud Manager roles.

# Getting started with Cloud Compliance for Cloud Volumes ONTAP

Complete a few steps to get started with Cloud Compliance for Cloud Volumes ONTAP in AWS or Azure.

## Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details.

**Verify that your configuration can meet the requirements**

- Ensure that the Cloud Compliance instance will have outbound internet access.

  Cloud Manager deploys the instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request.

- Ensure that users can access the Cloud Manager interface from a host that has a direct connection to AWS or Azure, or from a host that's inside the same network as the Cloud Compliance instance (the instance will have a private IP address).
- Ensure that you can keep the Cloud Compliance instance running.

**Enable Cloud Compliance on Cloud Volumes ONTAP**

- New working environments: Be sure to keep Cloud Compliance enabled when you create the working environment (it's enabled by default).
- Existing working environments: Click **Compliance**, optionally edit the list of working environments, and click **Show Compliance Dashboard**.

**Ensure access to volumes**

Now that Cloud Compliance is enabled, ensure that it can access volumes.

- The Cloud Compliance instance needs a network connection to each Cloud Volumes ONTAP subnet.
- Security groups for Cloud Volumes ONTAP must allow inbound connections from the Cloud Compliance instance.
- NFS Volume export policies must allow access from the Cloud Compliance instance.
- Cloud Compliance needs Active Directory credentials to scan CIFS volumes.

  Click **Compliance** > **CIFS Scan Status** > **Edit CIFS Credentials** and provide the credentials. The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read data that requires elevated permissions.

**Ensure connectivity between Cloud Manager and Cloud Compliance**

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.
- If your AWS network doesn't use a NAT or proxy for internet access, then the security group for Cloud Manager must allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance. You'll need to ensure connectivity between components after you enable Cloud Compliance. That's covered below.

### Enable outbound internet access

Cloud Compliance requires outbound internet access. If your virtual network uses a proxy server for internet access, ensure that the Cloud Compliance instance has outbound internet access to contact the following endpoints:

| Endpoints | Purpose |
|---|---|
| https://cloudmanager.cloud.netapp.com | Communication with the Cloud Manager service, which includes Cloud Central accounts. |
| https://netapp-cloud-account.auth0.com | Communication with NetApp Cloud Central for centralized user authentication. |

| Endpoints | Purpose |
| --- | --- |
| https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com<br>https://hub.docker.com | Provides access to software images, manifests, and templates. |
| https://kinesis.us-east-1.amazonaws.com | Enables NetApp to stream data from audit records. |
| https://cognito-idp.us-east-1.amazonaws.com<br>https://cognito-identity.us-east-1.amazonaws.com | Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics. |

**Verify web browser connectivity to Cloud Compliance**

The Cloud Compliance instance uses a private IP address to ensure that the indexed data isn't accessible to the internet. As a result, the web browser that you use to access Cloud Manager must have a connection to that private IP address. That connection can come from a direct connection to AWS or Azure (for example, a VPN), or from a host that's inside the same network as the Cloud Compliance instance.

If you're accessing Cloud Manager from a public IP address, then your web browser probably isn't running on a host inside the network.

**Keep Cloud Compliance running**

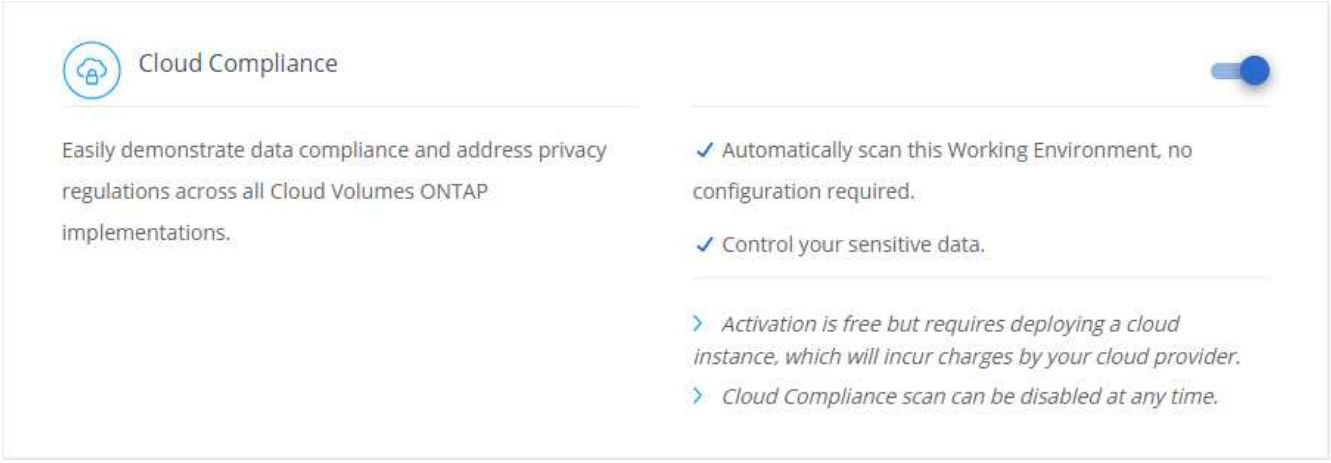
The Cloud Compliance instance needs to stay on to continuously scan your data.

## Enabling Cloud Compliance on a new working environment

Cloud Compliance is enabled by default in the working environment wizard. Be sure to keep the option enabled.

**Steps**

1. Click **Create Cloud Volumes ONTAP**.
2. Select Amazon Web Services or Microsoft Azure as the cloud provider and then choose a single node or HA system.
3. Fill out the Details & Credentials page.
4. On the Services page, leave Cloud Compliance enabled and click **Continue**.




5. Complete the pages in the wizard to deploy the system.

For help, see Launching Cloud Volumes ONTAP in AWS and Launching Cloud Volumes ONTAP in Azure.

**Result**

Cloud Compliance is enabled on the Cloud Volumes ONTAP system. If this the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider. As soon as the instance is available, it starts scanning data as its written to each volume that you create.

## Enabling Cloud Compliance on existing working environments

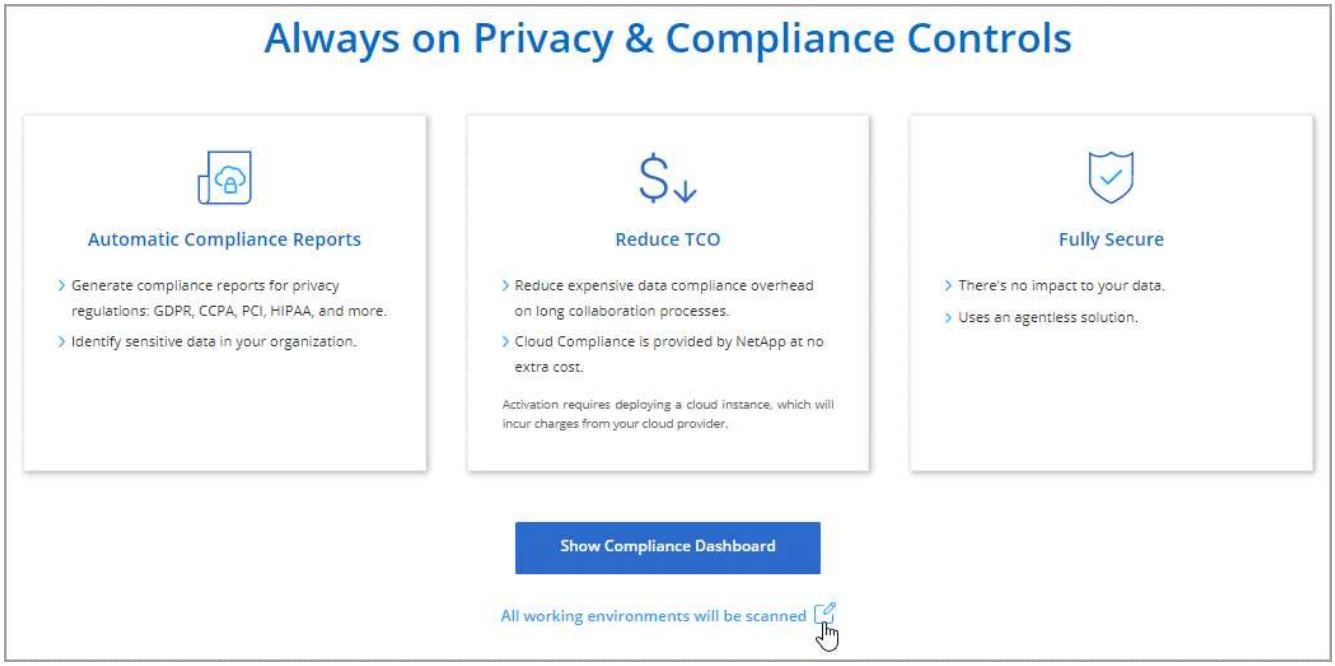
Enable Cloud Compliance on your existing Cloud Volumes ONTAP systems from the **Compliance** tab in Cloud Manager.

Another option is to enable Cloud Compliance from the **Working Environments** tab by selecting each working environment individually. That'll take you longer to complete, unless you have just one system.

**Steps for multiple working environments**

1. At the top of Cloud Manager, click **Compliance**.
2. If you want to enable Cloud Compliance on specific working environments, click the edit icon.

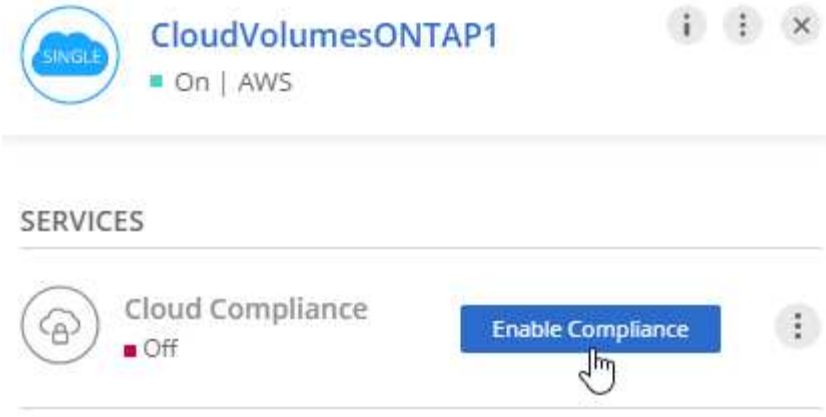
   Otherwise, Cloud Manager is set to enable Cloud Compliance on all working environments to which you have access.




3. Click **Show Compliance Dashboard**.

**Steps for a single working environment**

1. At the top of Cloud Manager, click **Working Environments**.
2. Select a working environment.
3. In the pane on the right, click **Enable Compliance**.




**Result**

If this the first time that you enabled Cloud Compliance, Cloud Manager deploys the Cloud Compliance instance in your cloud provider.

Cloud Compliance starts scanning the data on each working environment. Data will be available in the Compliance dashboard as soon as Cloud Compliance finishes the initial scans. The time that it takes depends on the amount of data—it could be a few minutes or hours.

## Verifying that Cloud Compliance has access to volumes

Make sure that Cloud Compliance can access volumes on Cloud Volumes ONTAP by checking your networking, security groups, and export policies. You'll need to provide Cloud Compliance with CIFS credentials so it can access CIFS volumes.

**Steps**

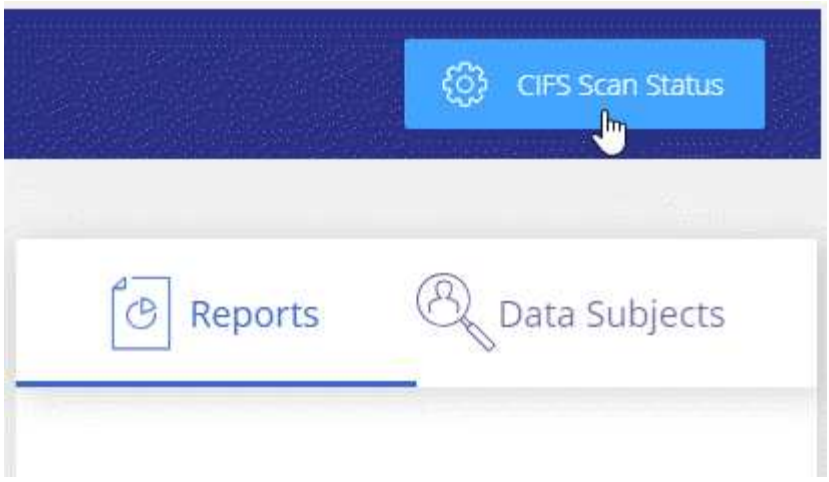
1. Make sure that there's a network connection between the Cloud Compliance instance and each Cloud Volumes ONTAP subnet.

   Cloud Manager deploys the Cloud Compliance instance in the same VPC or VNet as the first Cloud Volumes ONTAP system in the request. So this step is important if some Cloud Volumes ONTAP systems are in different subnets or virtual networks.

2. Ensure that the security group for Cloud Volumes ONTAP allows inbound traffic from the Cloud Compliance instance.

   You can either open the security group for traffic from the IP address of the Cloud Compliance instance, or you can open the security group for all traffic from inside the virtual network.

3. Ensure that NFS volume export policies include the IP address of the Cloud Compliance instance so it can access the data on each volume.
4. If you use CIFS, provide Cloud Compliance with Active Directory credentials so it can scan CIFS volumes.
   a. At the top of Cloud Manager, click **Compliance**.
   b. In the top right, click **CIFS Scan Status**.




c. For each Cloud Volumes ONTAP system, click **Edit CIFS Credentials** and enter the user name and password that Cloud Compliance needs to access CIFS volumes on the system.

   The credentials can be read-only, but providing admin credentials ensures that Cloud Compliance can read any data that requires elevated permissions. The credentials are stored on the Cloud Compliance instance.

   After you enter the credentials, you should see a message that all CIFS volumes were authenticated successfully.


## Verifying that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and Cloud Compliance so you can view the compliance insights that Cloud Compliance found.

**Steps**

1. Make sure that the security group for Cloud Manager allows inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

   This connection enables you to view information in the Compliance tab.

2. If your AWS network doesn't use a NAT or proxy for internet access, modify the security group for Cloud Manager to allow inbound traffic over TCP port 3128 from the Cloud Compliance instance.

   This is required because the Cloud Compliance instance uses Cloud Manager as a proxy to access the internet.

   This port is open by default on all new Cloud Manager instances, starting with version 3.7.5. It's not open on Cloud Manager instances created prior to that version.

# Gaining visibility and control of private data

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.

## Personal data

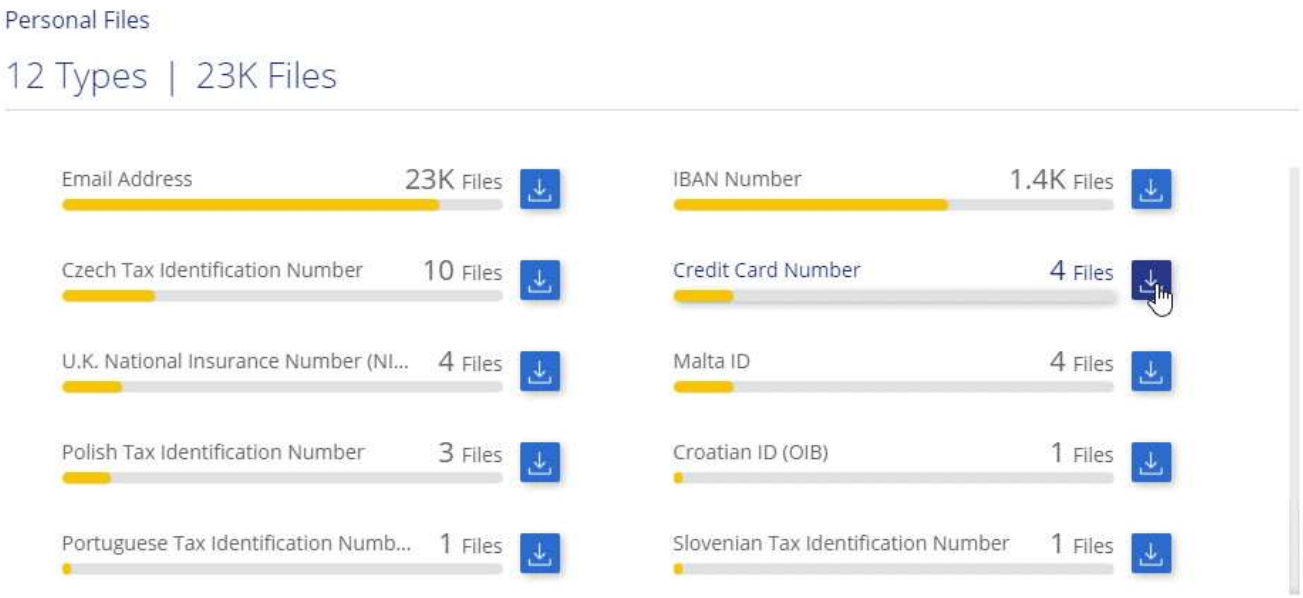
Cloud Compliance automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, Personal Identification Information (PII), credit card numbers, social security numbers, bank account numbers, and more. See the full list.

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 list below shows when Cloud Compliance uses proximity validation.

### Viewing files that contain personal data

#### Steps

1. At the top of Cloud Manager, click **Compliance**.
2. Download the details for one of the top 2 file types directly from the main screen, or click **View All** and then download the list for any of the personal data types that were found.




### Types of personal data

The personal data found in files can be general personal data or national identifiers. The third column identifies whether Cloud Compliance uses proximity validation to validate its findings for the identifier.

| Type | Identifier | Proximity validation? |
|---|---|---|
| General | Email address | No |
| | Credit card number | No |
| | IBAN number (International Bank Account Number) | No |
| | IP address | Yes |
| National Identifiers | Belgian ID (Numero National) | Yes |
| | Bulgarian ID (Unified Civil Number) | Yes |
| | Cyprus Tax Identification Number (TIC) | Yes |
| | Danish Tax Identification Number (CPR) | Yes |
| | Estonian ID (Isikukood) | Yes |
| | Finnish ID (henkilötunnus) | Yes |
| | French Tax Identification Number (SPI) | Yes |
| | German Tax Identification Number (Steuerliche Identifikationsnummer) | Yes |
| | Hungarian Tax Identification Number (Adóazonosító jel) | Yes |
| | Irish ID (PPS) | Yes |
| | Israeli ID | Yes |
| | Italian ID (Codice Fiscale) | Yes |
| | Latvian Tax Identification Number | Yes |
| | Lithuanian ID (Asmens kodas) | Yes |
| | Luxembourg ID | Yes |
| | Malta ID | Yes |
| | Netherlands ID (BSN) | Yes |
| | Polish Tax Identification Number | Yes |
| | Portuguese Tax Identification Number (NIF) | Yes |
| | Romanian Tax Identification Number | Yes |
| | Slovakian Tax Identification Number | Yes |
| | Slovenian Tax Identification Number | Yes |
| | South African ID | Yes |
| | Spanish Tax Identification Number | Yes |
| | Swedish Tax Identification Number | Yes |
| | U.K. National Insurance Number (NINO) | Yes |
| | USA Social Security Number (SSN) | Yes |

## 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.

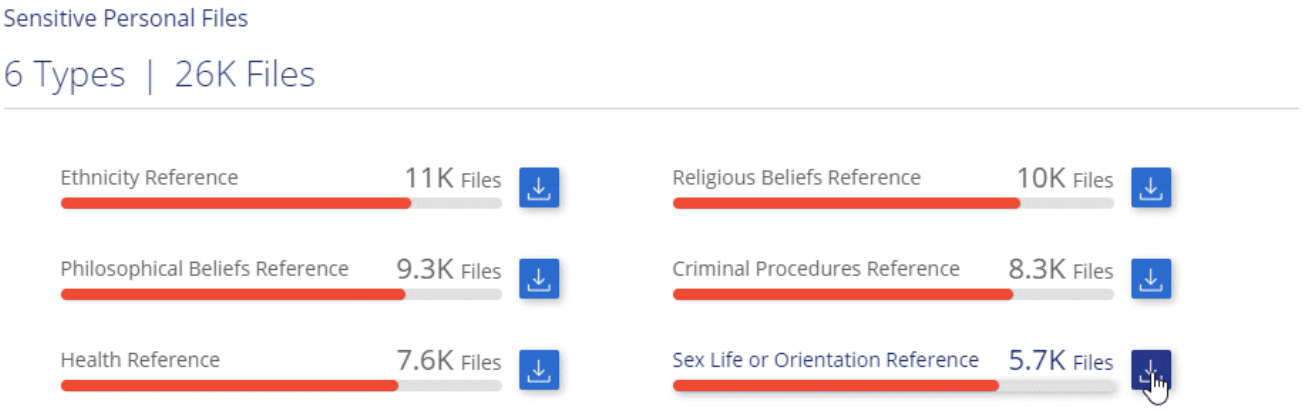
For example, one sensitive GDPR data category is ethnic origin. Because of its NLP abilities, Cloud Compliance can distinguish the difference between a sentence that reads "George is Mexican" (indicating sensitive data as specified in article 9 of the GDPR), versus "George is eating Mexican food."

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. Download the details for one of the top 2 file types directly from the main screen, or click **View All** and then download the list for any of the sensitive personal data types that were found.




### Types of sensitive personal data

The sensitive personal data that Cloud Compliance can find in files includes the following:

**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.

**Philosophical Beliefs Reference**

Data concerning a natural person's philosophical beliefs.

**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.

## 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.

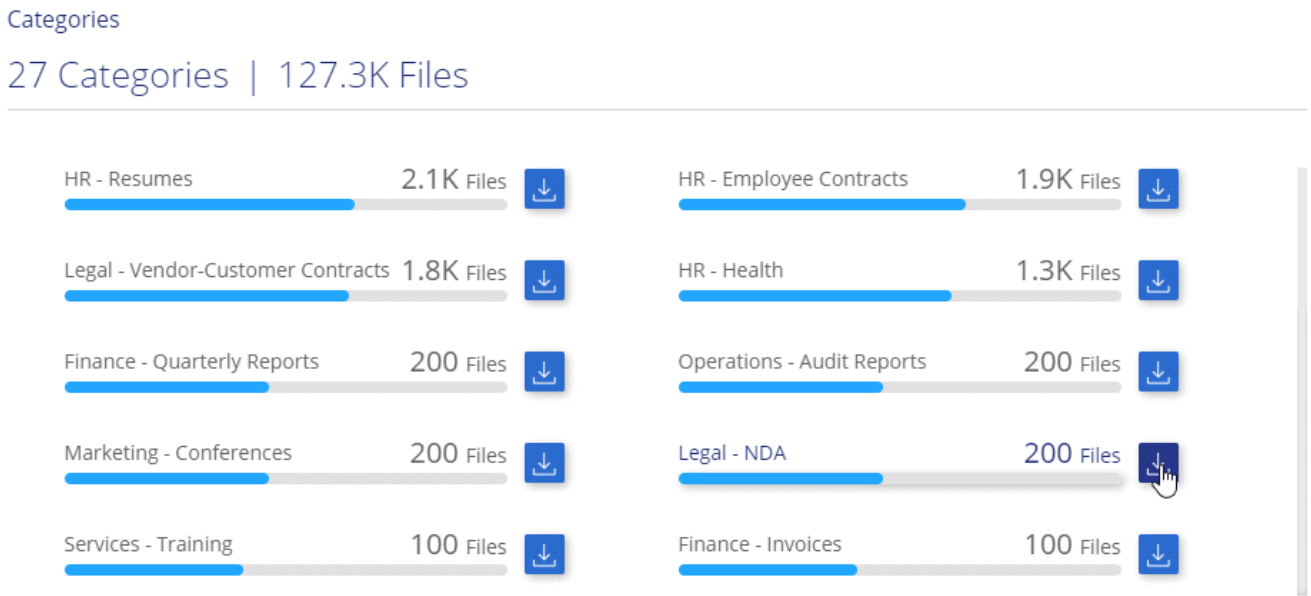
Categories can help you understand what's happening with your data by showing you the type of information that you have. For example, a category like resumes or employee contracts can include sensitive data. When you download the CSV report, you might find that employee contracts are stored in an unsecure 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

1. At the top of Cloud Manager, click **Compliance**.
2. Download the details for one of the top 4 file types directly from the main screen, or click **View All** and then download the list for any of the categories.




### Types of categories

Cloud Compliance categorizes your data as follows:

**Finance**

- Balance Sheets
- Purchase Orders
- Invoices
- Quarterly Reports

**HR**

- Background Check
- Compensation Plans
- Employee Contracts
- Employee Review
- Health
- Resumes

**Legal**

- NDA
- Vendor-Customer contracts

**Marketing**

- Campaigns
- Conferences

**Operations**

- Audit Reports

**Sales**

- Sales Orders

**Services**

- RFI
- RFP
- Training

**Support**

- Complaints and Tickets

**Other**

- Archive Files
- Audio
- CAD Files
- Code
- Executables
- Images

## File types

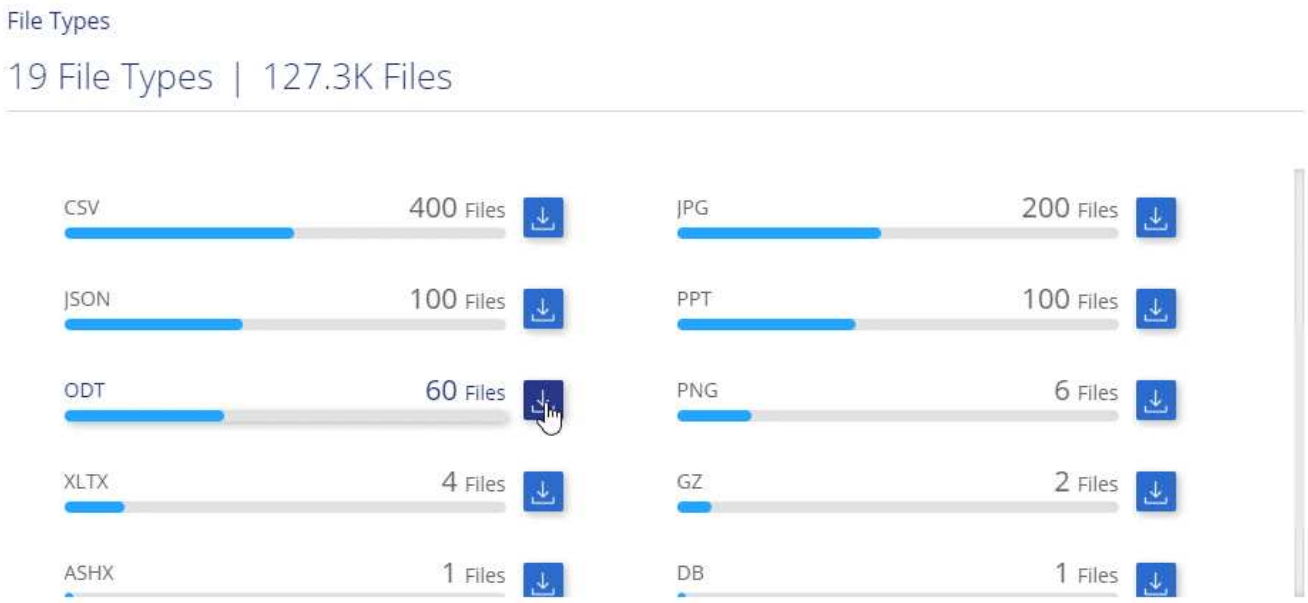
Cloud Compliance takes the data that it scanned and breaks it down by file type. Cloud Compliance can display all file types found in the scans.

Reviewing your file types can help you control your sensitive data because you might find that certain file types are not stored correctly. 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

1. At the top of Cloud Manager, click **Compliance**.
2. Download the details for one of the top 4 file types directly from the main screen, or click **View All** and then download the list for any of the file types.




## Accuracy of information found

NetApp can't guarantee 100% accuracy of the personal data and sensitive personal data that Cloud Compliance 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 Cloud Compliance finds. We break it down by *precision* and *recall*:

**Precision**

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

Cloud Compliance is in a Controlled Availability release and we are constantly improving the accuracy of our results. Those improvements will be automatically available in future Cloud Compliance 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% |

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

The dashboard enables you 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 (support for more will be added later).

Each file list includes the following information:

- File name
- Location type
- Location
- File path
- File type
- 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. The files only appear in the CSV reports.

# Viewing the 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.

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

The report includes the following information:

**Compliance status**

A severity score (see below for more details) 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**

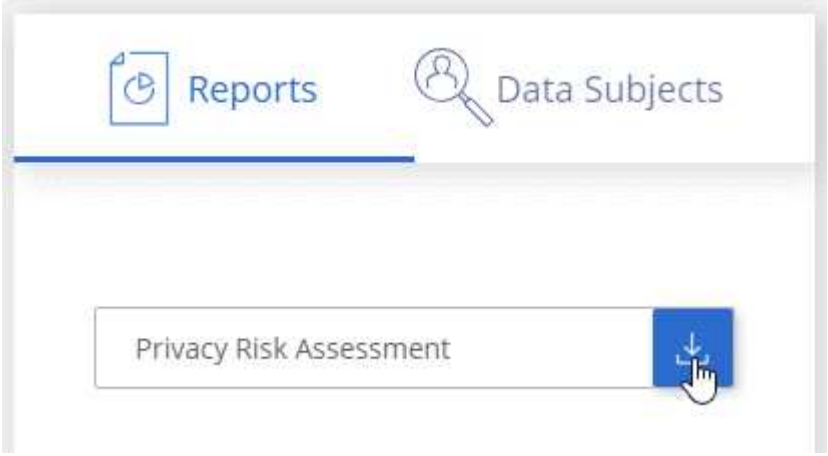
The number of people by location for which national identifiers were found.

## Generating the Privacy Risk Assessment Report

Go to the Compliance tab to generate the report.

**Steps**

1. At the top of Cloud Manager, click **Compliance**.
2. Under **Reports**, click the download icon next to **Privacy Risk Assessment**.




**Result**

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

## Severity score

Cloud Compliance 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% |

| Severity score | Logic |
| --- | --- |
| 4 | Three of the variables are larger than 3% |
| 5 | One of the variables are larger 6% |
| 6 | Two of the variables are larger 6% |
| 7 | Three of the variables are larger 6% |
| 8 | One of the variables are larger 15% |
| 9 | Two of the variables are larger 15% |
| 10 | Three of the variables are larger 15% |

# Responding to a Data Subject Access Request

Respond to a Data Subject Access Request (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.

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

## What is a Data Subject Access Request?

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.

## How can Cloud Compliance help you respond to a DSAR?

When you perform a data subject search, Cloud Compliance finds all of the files that has that person's name or identifier in it. Cloud Compliance 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 or 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.

## Searching for data subjects and downloading 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.

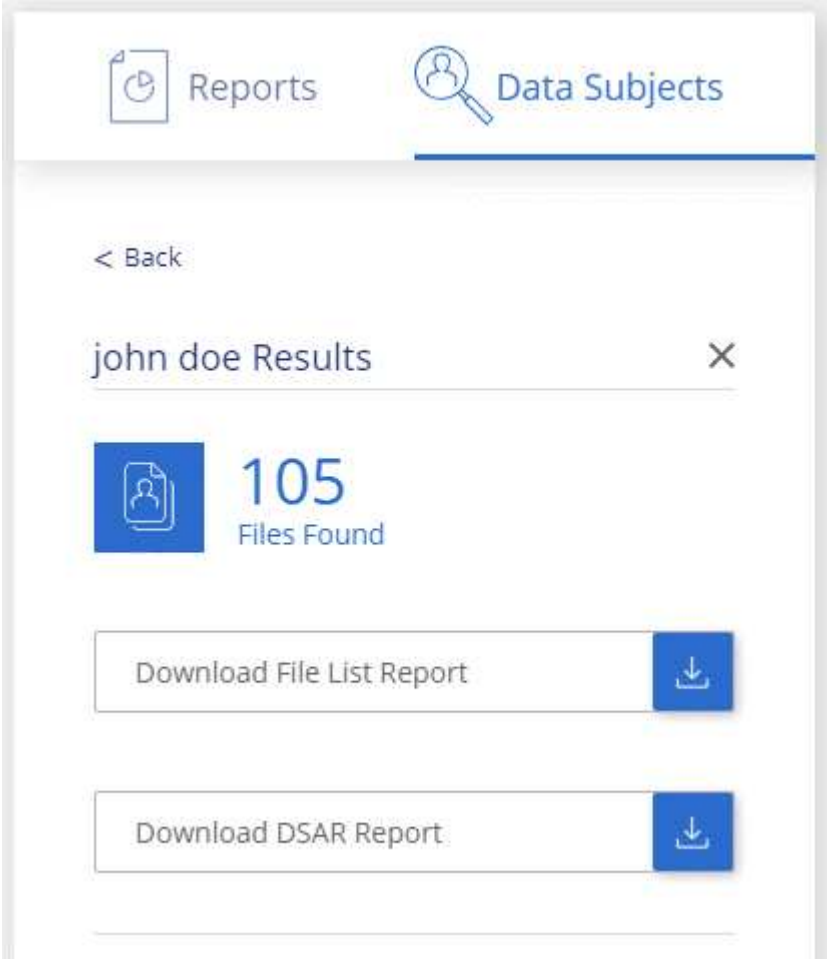
Only English is supported when searching for the names of data subjects. Support for more languages will be added later.

**Steps**

1. At the top of Cloud Manager, click **Compliance**.

2. Click **Data Subjects**.
3. Search for the data subject's full name or known identifier.

   Here's an example that shows a search for the name *john doe*:




4. Choose one of the available options:
   - **Download File List Report**: A list of the files that contain information on the data subject.

     If there are more than 10,000 results, only the top 10,000 appear in the report (support for more will be added later).

   - **Download DSAR Report**: A formal response to the access request that you can send to the data subject. This report contains automatically-generated information based on data that Cloud Compliance found on the data subject and is designed to be used as a template. You should complete the form and review it internally before sending it to the data subject.

# Disabling Cloud Compliance

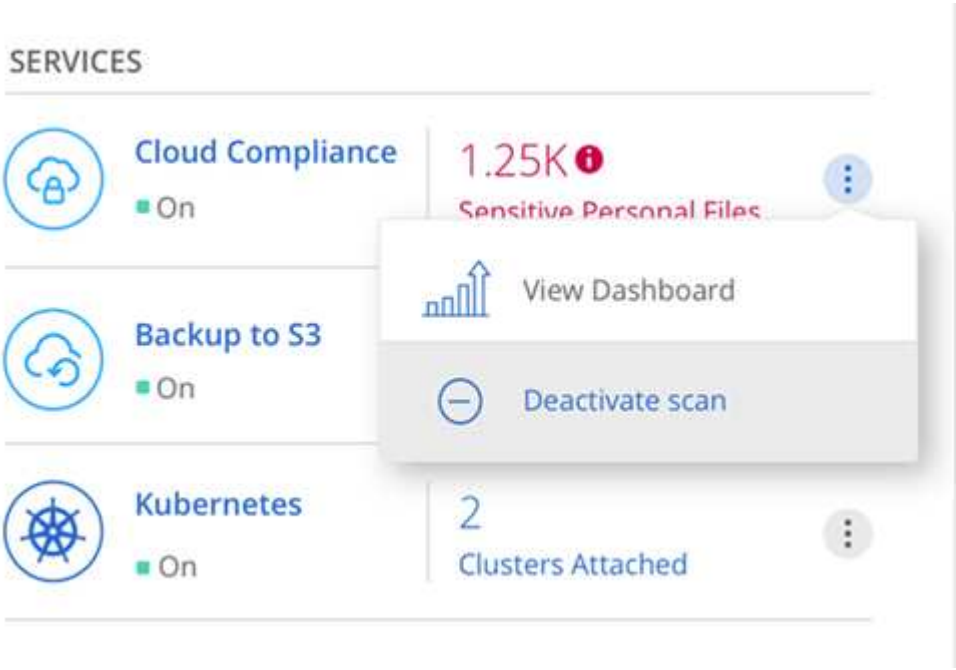
If you need to, you can stop Cloud Compliance from scanning one or more working environments. You can also delete the Cloud Compliance instance if you no longer want to use Cloud Compliance with your Cloud Volumes ONTAP systems.

## Deactivating compliance scans for a working environment

When you deactivate scans, Cloud Compliance no longer scans the data on the system and it removes the indexed compliance insights from the Cloud Compliance instance (the data from the working environment itself isn't deleted).

**Steps**

1. At the top of Cloud Manager, click **Working Environments**.
2. Select the working environment.
3. In the right panel, click the action icon for the Cloud Compliance service and select **Deactivate scan**.




## Deleting the Cloud Compliance instance

You can delete the Cloud Compliance instance if you no longer want to use Cloud Compliance with Cloud Volumes ONTAP. Deleting the instance also deletes the associated disks where the indexed data resides.

**Step**

1. Go to your cloud provider's console and delete the Cloud Compliance instance.

   The instance is named *CloudCompliance* with a generated hash (UUID) concatenated to it. For example: *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

# Frequently asked questions about Cloud Compliance

This FAQ can help if you're just looking for a quick answer to a question.

## What is Cloud Compliance?

Cloud Compliance is a new NetApp cloud offering. Using Artificial Intelligence (AI) driven technology, Cloud Compliance helps organizations understand data context and identify sensitive data across your Cloud

Volumes ONTAP systems hosted in AWS or Azure.

Cloud Compliance provides pre-defined parameters (such as sensitive information types and categories) to address new data compliance regulations for data privacy and sensitivity, such as GDPR, CCPA, and more.

## Why should I use Cloud Compliance?

Cloud Compliance can empower you with data to help you:

- Comply with data compliance and privacy regulations.
- Comply with data retention policies.
- Easily locate and report on specific data in response to data subjects, as required by GDPR, CCPA, and other data privacy regulations.

## What are the common use cases for Cloud Compliance?

- Identify Personal Identifiable Information (PII).
- Identify a wide scope of sensitive information as required by GDPR and CCPA privacy regulations.
- Comply with new and upcoming data privacy regulations.

Learn more about the use cases for Cloud Compliance.

## What types of data can be scanned with Cloud Compliance?

Cloud Compliance supports scanning of unstructured data over NFS and CIFS protocols. Currently Cloud Compliance scans data managed by Cloud Volumes ONTAP.

Learn how scans work.

## Which cloud providers are supported?

Cloud Compliance operates as part of Cloud Manager and currently supports AWS and Azure. This provides your organization with unified privacy visibility across different cloud providers. Support for Google Cloud Platform (GCP) will be added soon.

## How do I access Cloud Compliance?

Cloud Compliance is operated and managed through Cloud Manager. You can access Cloud Compliance features from the **Compliance** tab in Cloud Manager.

## How does Cloud Compliance work?

Cloud Compliance deploys another layer of Artificial Intelligence alongside your Cloud Manager system and Cloud Volumes ONTAP instances. It then scans the data on Cloud Volumes ONTAP and indexes the data insights found.

Learn more about how Cloud Compliance works.

## How much does Cloud Compliance cost?

Cloud Compliance is offered as part of Cloud Volumes ONTAP and doesn't require any additional costs.

Additional costs might be required in the future for customized capabilities.

Cloud Compliance requires deployment of an instance in your cloud provider, for which you'll be charged by your cloud provider.

## How often does Cloud Compliance scan my data?

Data changes frequently, so Cloud Compliance scans your data continuously with no impact to your data. While the initial scan of your data might take longer, subsequent scans only scan the incremental changes, which reduces system scan times.

Learn how scans work.

## Does Cloud Compliance offer reports?

Yes. The information offered by Cloud Compliance can be relevant to other stakeholders in your organizations, so we enable you to generate reports to share the insights.

The following reports are available for Cloud Compliance:

**Privacy Risk Assessment report**

Provides privacy insights from your data and a privacy risk score. Learn more.

**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. Learn more.

**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. Learn more.

## What type of instance or VM is required for Cloud Compliance?

- In Azure, Cloud Compliance runs on a Standard_D16s_v3 VM with a 512 GB disk.
- In AWS, Cloud Compliance runs on an m5.4xlarge instance with a 500 GB io1 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

Learn more about how Cloud Compliance works.

## Does scan performance vary?

Scan performance can vary based on the network bandwidth and the average file size in your cloud environment.

## How do I enable Cloud Compliance?

You can enable Cloud Compliance when you create a new working environment. You can enable it on existing working environments from the **Compliance** tab (on first activation only) or by selecting a specific working environment.

Learn how to get started.

Activating Cloud Compliance results in an immediate initial scan. Compliance results display shortly after.

## How do I disable Cloud Compliance?

You can disable Cloud Compliance from the Working Environments page after you select an individual working environment.

Learn more.

To completely remove the Cloud Compliance instance, you can manually remove the Cloud Compliance instance from your cloud provider's portal.

## What happens if data tiering is enabled on Cloud Volumes ONTAP?

You might want to enable Cloud Compliance on a Cloud Volumes ONTAP system that tiers cold data to object storage. If data tiering is enabled, Cloud Compliance scans all of the data—data that's on disks and cold data tiered to object storage.

The compliance scan doesn't heat up the cold data—it stays cold and tiered to object storage.

## Can I use Cloud Compliance to scan on-premise ONTAP storage?

No. Cloud Compliance is currently available as part of Cloud Manager and supports Cloud Volumes ONTAP. We're planning to support Cloud Compliance with additional cloud offerings such as Cloud Volumes Service and Azure NetApp Files.

## Can Cloud Compliance send notifications to my organization?

No, but you can download status reports that you can share internally in your organization.

## Can I customize the service to my organization's need?

Cloud Compliance provides out-of-the-box insights to your data. These insights can be extracted and used for your organization's needs.

## Can I limit Cloud Compliance information to specific users?

Yes, Cloud Compliance is fully integrated with Cloud Manager. Cloud Manager users can only see information for the working environments they are eligible to view according to their workspace privileges.

Learn more.