



# Gain insight into data privacy

## Cloud Manager

NetApp

June 15, 2020

This PDF was generated from [https://docs.netapp.com/us-en/occm/concept\\_cloud\\_compliance.html](https://docs.netapp.com/us-en/occm/concept_cloud_compliance.html) on June 15, 2020. Always check docs.netapp.com for the latest.

# Table of Contents

- Gain insight into data privacy ..... 1
  - Learn about Cloud Compliance..... 1
  - Get started ..... 5
  - Gaining visibility and control of private data ..... 24
  - Viewing compliance reports ..... 38
  - Responding to a Data Subject Access Request..... 42
  - Disabling Cloud Compliance ..... 44
  - Frequently asked questions about Cloud Compliance ..... 45

# Gain insight into data privacy

## Learn about Cloud Compliance

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

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)

### Supported working environments

Cloud Compliance can scan data from the following types of working environments:

- Cloud Volumes ONTAP in AWS and Azure
- Amazon S3
- Azure NetApp Files

For Azure NetApp Files, Cloud Compliance can scan volumes that are in the same region as Cloud Manager. When you activate compliance scans on an Azure NetApp Files working environment, Cloud Compliance scans *all* of the volumes in the region.

### Cost

The cost to use Cloud Compliance depends on the type of working environment that you're scanning.

#### Cloud Volumes ONTAP and Azure NetApp Files

Cloud Compliance is an add-on service provided by NetApp at no extra cost. Activating Cloud

Compliance requires deploying a cloud instance, which results in charges from your cloud provider.

Data transfer costs depend on your setup. If Cloud Compliance and Cloud Volumes ONTAP are in the same Availability Zone and region, then there are no data transfer costs. But if Cloud Volumes ONTAP is in a *different* Availability Zone or region, then you'll be charged by your cloud provider for data transfer costs. See these links for more details:

- [AWS: Amazon EC2 Pricing](#)
- [Microsoft Azure: Bandwidth Pricing Details](#)

## Amazon S3

You need to pay to scan your Amazon S3 buckets. [Learn about pricing](#).

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends. [Learn how to subscribe](#).

## How Cloud Compliance works

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

1. You enable Cloud Compliance on one or more working environments.
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.

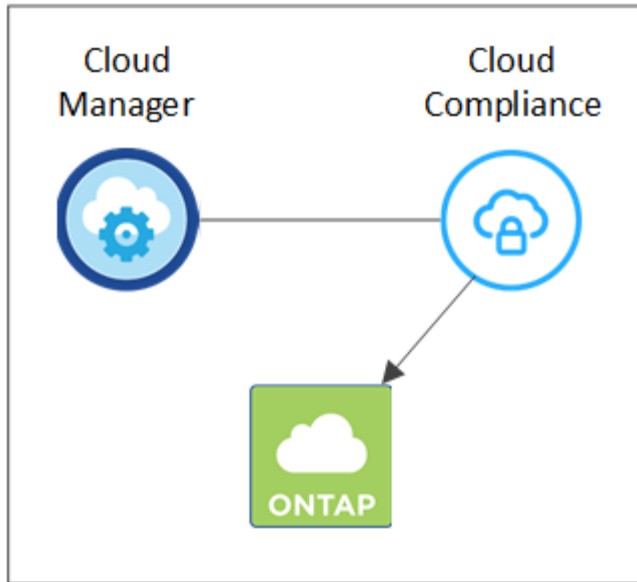
## The Cloud Compliance instance

When you enable Cloud Compliance, Cloud Manager deploys a Cloud Compliance instance in the same subnet as Cloud Manager.



If Cloud Manager is installed on-prem, it deploys the Cloud Compliance instance in same VPC or VNet as the first Cloud Volumes ONTAP system in the request.

## VPC or VNet



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 GP2 disk.

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



Changing or resizing the instance/VM type isn't supported. You need to use the default size that's provided.

- 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 volumes.

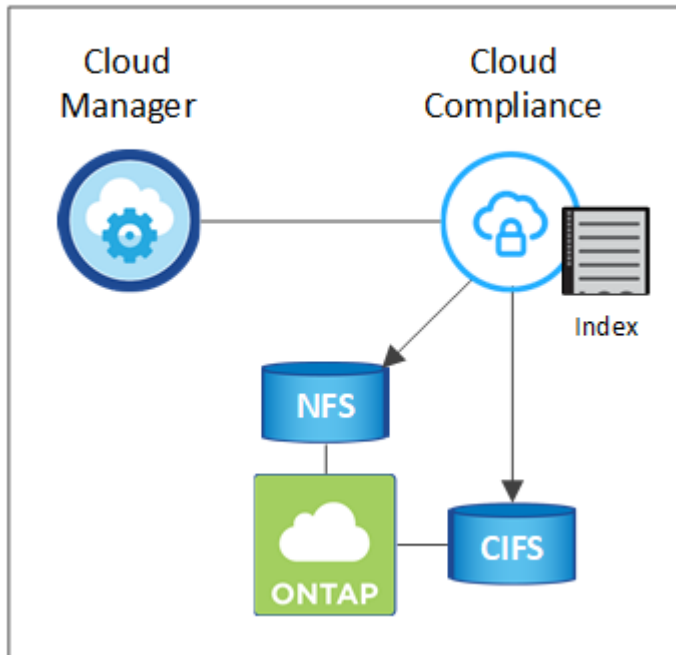
## How scans work

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

Cloud Compliance connects to the data 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.

### VPC or VNet



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 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.](#)

# Get started

## Getting started with Cloud Compliance

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

### Quick start

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

## 1

### Review prerequisites

Ensure that your cloud environment can meet the prerequisites, which includes 16 vCPUs for the Cloud Compliance instance, outbound internet access for the instance, connectivity between Cloud Manager and Cloud Compliance over port 80, and more. [See the complete list.](#)

## 2

### Enable Cloud Compliance

- 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**.

## 3

### 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 or Azure NetApp Files 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 > Scan Configuration > 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.

### 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 to volumes 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. Note that Cloud Manager deploys the Cloud Compliance instance in the same subnet as Cloud Manager.



Endpoints	Purpose
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srnrn.cloudfront.net/">https://dseasb33srnrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Provides access to software images, manifests, and templates.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

### Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Compliance instance. You can find the latest Cloud Manager permissions in [the policies provided by NetApp](#).

### Check your vCPU limits

Ensure that your cloud provider's vCPU limit allows for the deployment of an instance with 16 cores. You'll need to verify the vCPU limit for the relevant instance family in the region where Cloud Manager is running.

In AWS, the instance family is *On-Demand Standard instances*. In Azure, the instance family is *Standard D5v3 Family*.

For more details on vCPU limits, see the following:

- [AWS documentation: Amazon EC2 Service Limits](#)
- [Azure documentation: Virtual machine vCPU quotas](#)

### Ensure that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and the Cloud Compliance instance:

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

This connection enables deployment of the Cloud Compliance instance and enables you to view information in the Compliance tab.

- 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.

### Set up discovery of Azure NetApp Files

Before you can scan volumes for Azure NetApp Files, [Cloud Manager must be set up to discover the configuration](#).

### Ensure that you can keep Cloud Compliance running

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

### Ensure web browser connectivity to Cloud Compliance

After Cloud Compliance is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Cloud Compliance instance.

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.

### Enabling Cloud Compliance on a new working environment

Cloud Compliance is enabled by default in the Cloud Volumes ONTAP 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**.

 Cloud Compliance  

---

Easily demonstrate data compliance and address privacy regulations across all Cloud Volumes ONTAP implementations

#### ADVANTAGES

- ✓ Automatically scan this Working Environment, no configuration required.
- ✓ Control your sensitive data.

#### CLARIFICATIONS

- > Activation is free but requires deploying a cloud instance, which will incur charges by your cloud provider.
- > Cloud Compliance scan can be disabled at any time.

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 is 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, Cloud Compliance starts scanning the data in the working environment. Results will be available in the Compliance dashboard as soon as Cloud Compliance finishes the initial scans.

### **Enabling Cloud Compliance on existing working environments**

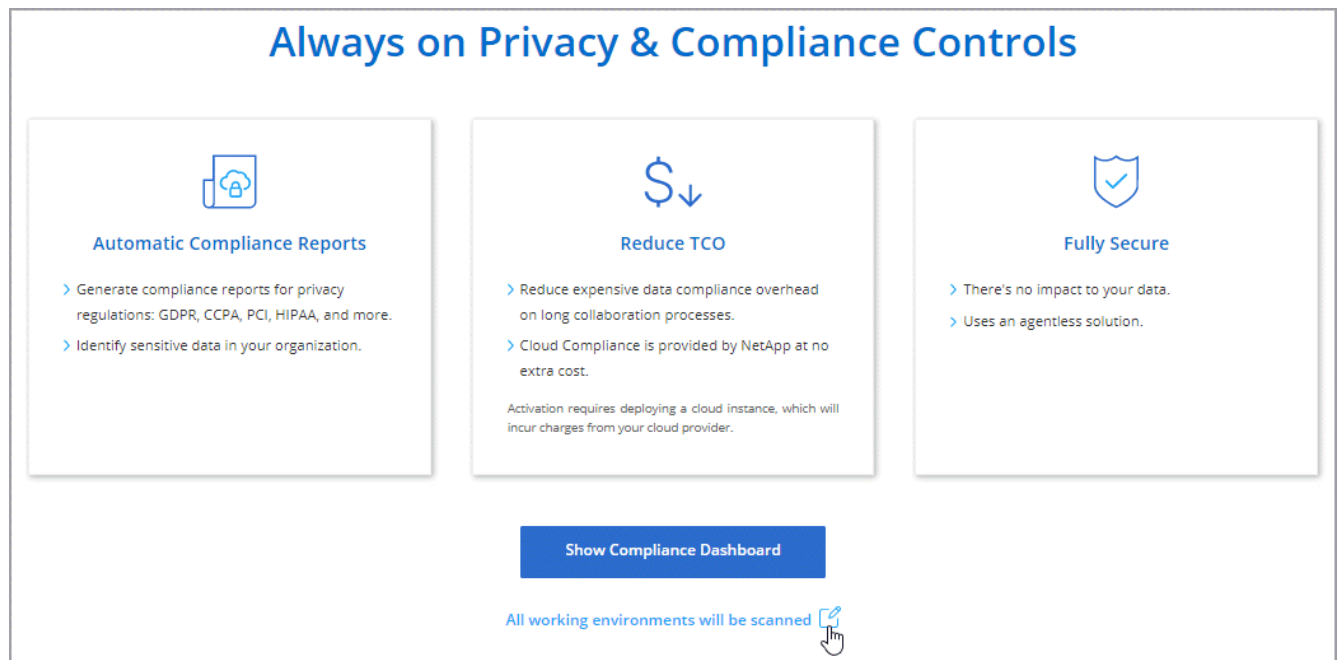
If you haven't enabled Cloud Compliance yet, enable it on existing Cloud Volumes ONTAP or Azure NetApp Files working environments from the **Compliance** tab in Cloud Manager.

Another option is to enable Cloud Compliance from the **Working Environments** tab by selecting each working environment individually.

#### *Steps for multiple working environments (first time only)*

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.

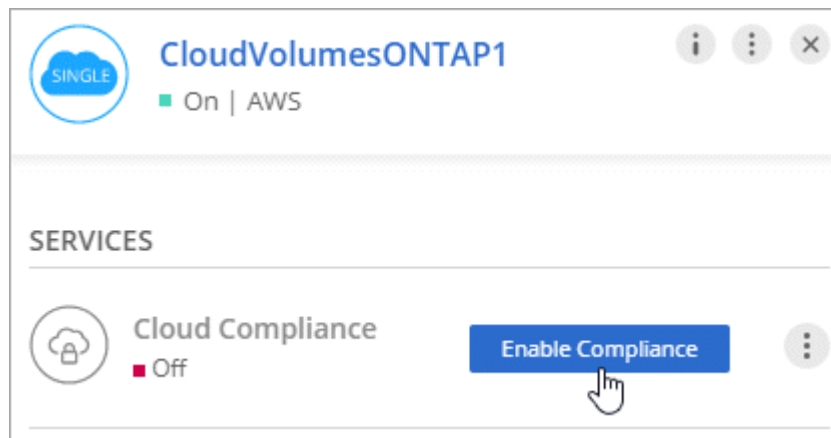
Otherwise, Cloud Manager is set to enable Cloud Compliance on all working environments to which you have access.



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.

As soon as the instance is available, Cloud Compliance starts scanning the data on each working environment. Results 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 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 network that includes volumes for Cloud Volumes ONTAP or Azure NetApp Files.

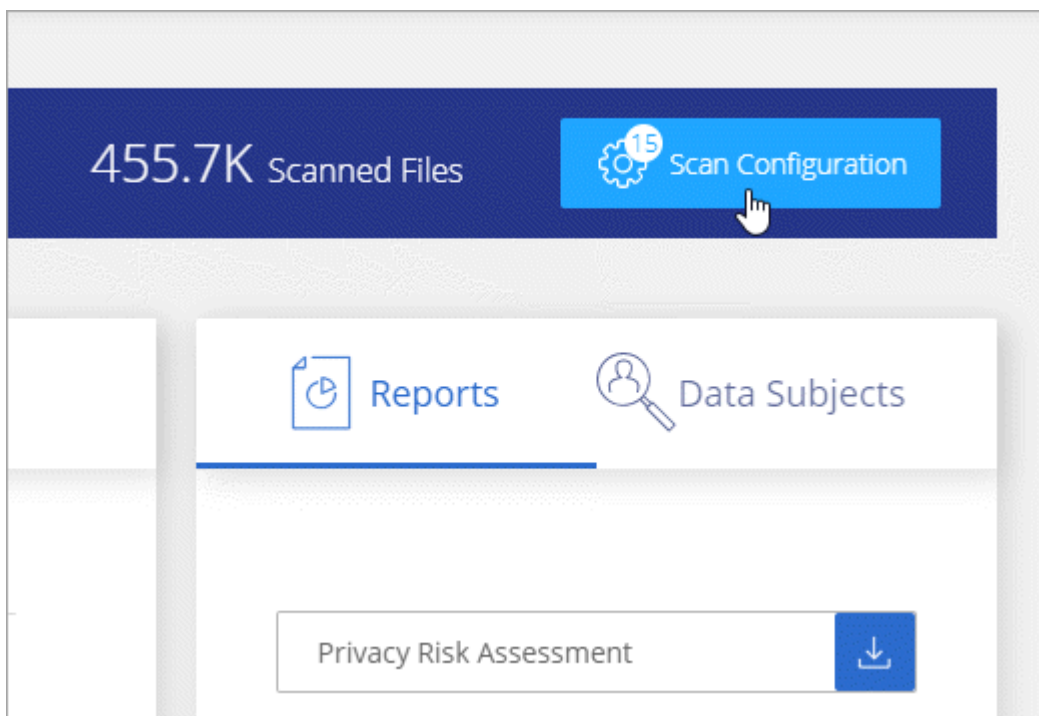


For Azure NetApp Files, Cloud Compliance can only scan volumes that are in the same region as Cloud Manager.

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 **Scan Configuration**.

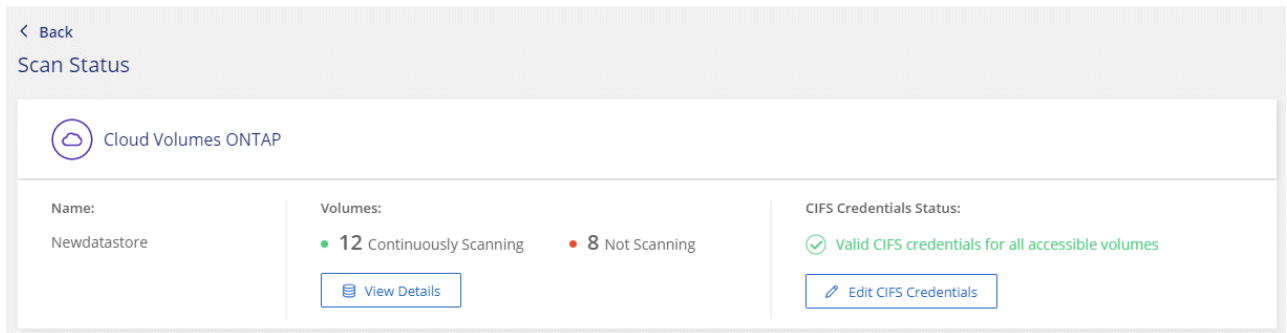


- c. For each working environment, click **Edit CIFS Credentials** and enter the user name and

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.



5. On the **Scan Configuration** page, click **View Details** to review the status for each CIFS and NFS volume and correct any errors.

For example, the following image shows three volumes; one of which Cloud Compliance can't scan due to network connectivity issues between the Cloud Compliance instance and the volume.

A screenshot of the 'Newdatastore Scan Configuration' page. It shows '23/23 Volumes selected for compliance scan'. A table lists three volumes. The first two are NFS volumes with status 'Continuously Scanning'. The third is a CIFS volume with status 'No Access' and a message: 'The CIFS credentials that you provided have expired. Edit the CIFS credential...'. There is a search icon and an 'Edit CIFS Credentials' button at the top right.

Name ↑↓	Protocol ↑↓	Status ↑↓	Required Action ↑↓
10.160.7.6:/yuval22	NFS	● Continuously Scanning	
10.160.7.6:/yuvalnewtarget	NFS	● Continuously Scanning	
\\10.160.7.6\Danny_share	CIFS	● No Access	The CIFS credentials that you provided have expired. Edit the CIFS credential...

## Getting started with Cloud Compliance for Amazon S3

Cloud Compliance can scan your Amazon S3 buckets to identify the personal and sensitive data that resides in S3 object storage. Cloud Compliance can scan any bucket in the account, regardless if it was created for a NetApp solution.

### Pricing

You need to pay to scan your Amazon S3 buckets. [Learn about pricing.](#)

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends. [Learn how to](#)

[subscribe](#).

## Quick start

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



### Deploy Cloud Manager in AWS

If you haven't already done so, log in to [Cloud Central](#) and deploy Cloud Manager in AWS.

Cloud Manager automatically discovers the S3 buckets in this AWS account and displays them in an Amazon S3 working environment.



### Set up your cloud environment

Ensure that your cloud environment can meet the requirements for Cloud Compliance, which includes preparing an IAM role, setting up connectivity from Cloud Compliance to S3, and more. [See the complete list](#).



### Subscribe from the AWS Marketplace

A subscription to the AWS Marketplace is required to scan Amazon S3 after the 30-day free trial ends.

Click **Settings > Credentials** and click **Add Subscription** for the Instance Profile.



### Enable Cloud Compliance

Select the Amazon S3 working environment, click **Enable Compliance**, and select an IAM role that includes the required permissions.



### Configure buckets

Select the buckets that you'd like to scan and Cloud Compliance will start scanning them.

## Reviewing prerequisites

Review the following prerequisites to make sure that you have a supported configuration before you enable Cloud Compliance.

### Requirements specific to S3

The first two requirements are specific to scanning S3 buckets.

## Set up an IAM role for the Cloud Compliance instance

Cloud Compliance needs permissions to connect to the S3 buckets in your account and to scan them. Set up an IAM role that includes the permissions listed below. Cloud Manager prompts you to select an IAM role when you enable Cloud Compliance on the Amazon S3 working environment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

## Provide connectivity from Cloud Compliance to Amazon S3

Cloud Compliance needs a connection to Amazon S3. The best way to provide that connection is through a VPC Endpoint to the S3 service. For instructions, see [AWS Documentation: Creating a Gateway Endpoint](#).

When you create the VPC Endpoint, be sure to select the region, VPC, and route table that corresponds to the Cloud Compliance instance. You must also modify the security group to add an outbound HTTPS rule that enables traffic to the S3 endpoint. Otherwise, Cloud Compliance can't connect to the S3 service.

If you experience any issues, see [AWS Support Knowledge Center: Why can't I connect to an S3 bucket using a gateway VPC endpoint?](#)

An alternative is to provide the connection by using a NAT Gateway.





You can't use a proxy to get to S3 over the internet.

## General requirements

The requirements in this section apply to Cloud Compliance in general, whether you're scanning Amazon S3, Cloud Volumes ONTAP, or Azure NetApp Files. If you've already enabled Cloud Compliance (for Cloud Volumes ONTAP or Azure NetApp Files), then you can skip these requirements and [Subscribe from the AWS Marketplace](#).

## 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. Note that Cloud Manager deploys the Cloud Compliance instance in the same subnet as Cloud Manager.

Endpoints	Purpose
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Communication with the Cloud Manager service, which includes Cloud Central accounts.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication with NetApp Cloud Central for centralized user authentication.
<a href="https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srnrn.cloudfront.net/">https://dseasb33srnrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Provides access to software images, manifests, and templates.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Enables NetApp to stream data from audit records.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a>	Enables Cloud Compliance to access and download manifests and templates, and to send logs and metrics.

## Ensure that Cloud Manager has the required permissions

Ensure that Cloud Manager has permissions to deploy resources and create security groups for the Cloud Compliance instance. You can find the latest Cloud Manager permissions in [the policies provided by NetApp](#).

## Check your vCPU limits

Ensure that your cloud provider's vCPU limit allows for the deployment of an instance with 16 cores. You'll need to verify the vCPU limit for the relevant instance family in the region where Cloud

Manager is running.

In AWS, the instance family is *On-Demand Standard instances*. In Azure, the instance family is *Standard D5v3 Family*.

For more details on vCPU limits, see the following:

- [AWS documentation: Amazon EC2 Service Limits](#)
- [Azure documentation: Virtual machine vCPU quotas](#)

## Ensure that Cloud Manager can access Cloud Compliance

Ensure connectivity between Cloud Manager and the Cloud Compliance instance:

- The security group for Cloud Manager must allow inbound and outbound traffic over port 80 to and from the Cloud Compliance instance.

This connection enables deployment of the Cloud Compliance instance and enables you to view information in the Compliance tab.

- 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.

## Ensure that you can keep Cloud Compliance running

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

## Ensure web browser connectivity to Cloud Compliance

After Cloud Compliance is enabled, ensure that users access the Cloud Manager interface from a host that has a connection to the Cloud Compliance instance.

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.

## Subscribing from the AWS Marketplace

A 30-day free trial is available to scan Amazon S3 data with Cloud Compliance. A subscription to the AWS Marketplace is required to continue scanning Amazon S3 after the free trial ends.

These steps must be completed by a user who has the *Account Admin* role.

### Steps

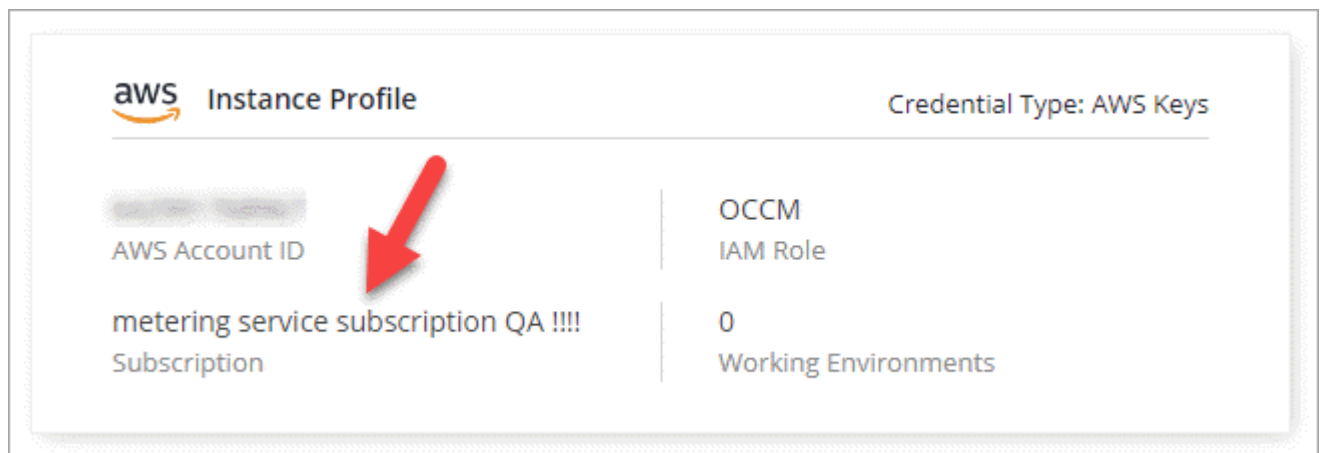
1. In the upper right of the Cloud Manager console, click the Settings icon, and select **Credentials**.



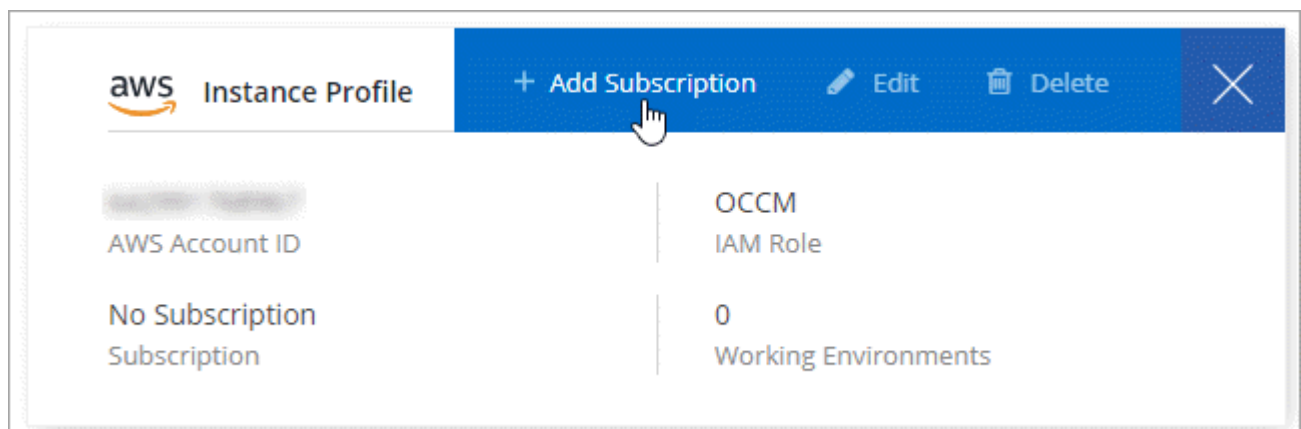
2. Find the credentials for the AWS Instance Profile.

The subscription must be added to the Instance Profile. Charging won't work otherwise.

If you already have a subscription, then you're all set—there's nothing else that you need to do.



3. If you don't have a subscription yet, hover over the credentials and click the action menu.
4. Click **Add Subscription**.



5. Click **Add Subscription**, click **Continue**, and follow the steps.

► [https://docs.netapp.com/us-en/occm/media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/us-en/occm/media/video_subscribing_aws.mp4) (video)

## Enabling Cloud Compliance

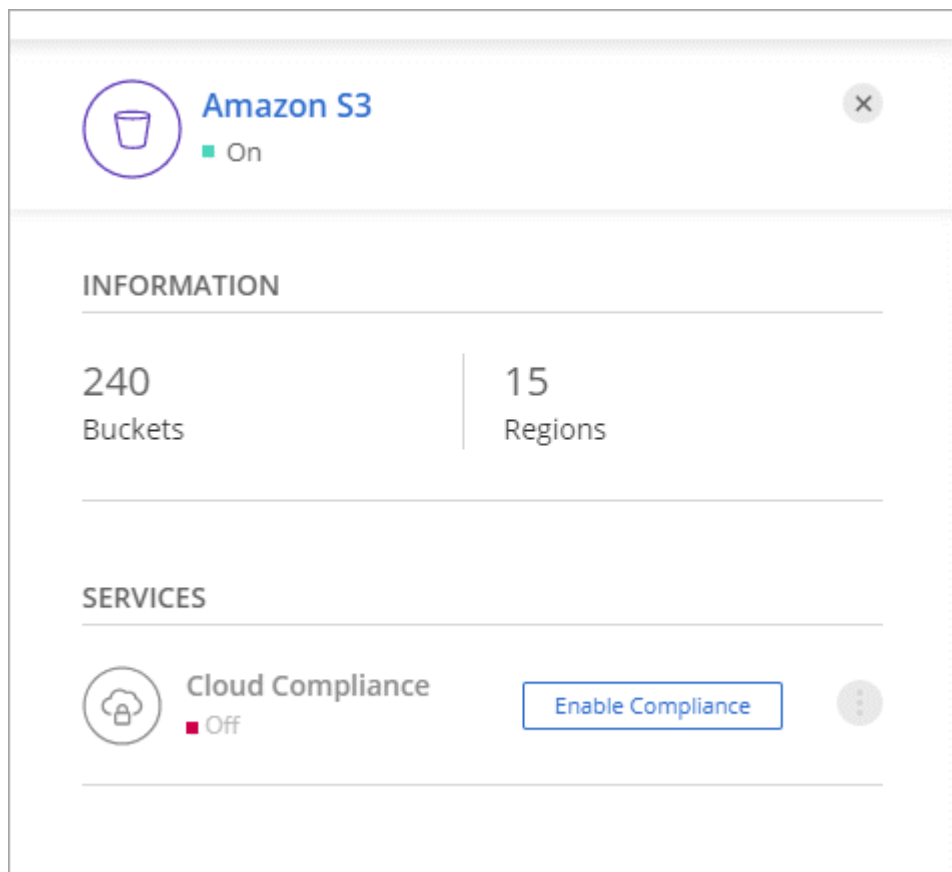
Enable Cloud Compliance on Amazon S3 after you verify the prerequisites.

### Steps

1. At the top of Cloud Manager, click **Working Environments**.
2. Select the Amazon S3 working environment.



3. In the pane on the right, click **Enable Compliance**.



- When prompted, assign an IAM role to the Cloud Compliance instance that has [the required permissions](#).

### Assign an AWS IAM Role for Cloud Compliance

To enable Cloud Compliance on Amazon S3 buckets, select an existing IAM role. Make sure that your AWS IAM role has the permission defined in the [Policy Requirements](#).

#### Select IAM Role

NetAppCloudCompliance ▼


#### VPC Endpoint for Amazon S3 Required

A VPC endpoint to the Amazon S3 service is required so Cloud Compliance can securely scan the data. Alternatively, ensure that the Cloud Compliance instance has direct access to the internet via a NAT Gateway or Internet Gateway.

Enable ComplianceCancel

- Click **Enable Compliance**.



You can also enable compliance scans for a working environment from the Scan Configuration page by clicking the  icon and selecting **Activate Compliance**.

#### Result

If the Cloud Compliance instance hasn't been deployed yet, Cloud Manager deploys it. If it has been deployed, Cloud Manager assigns the IAM role to the instance.

#### Configuring buckets

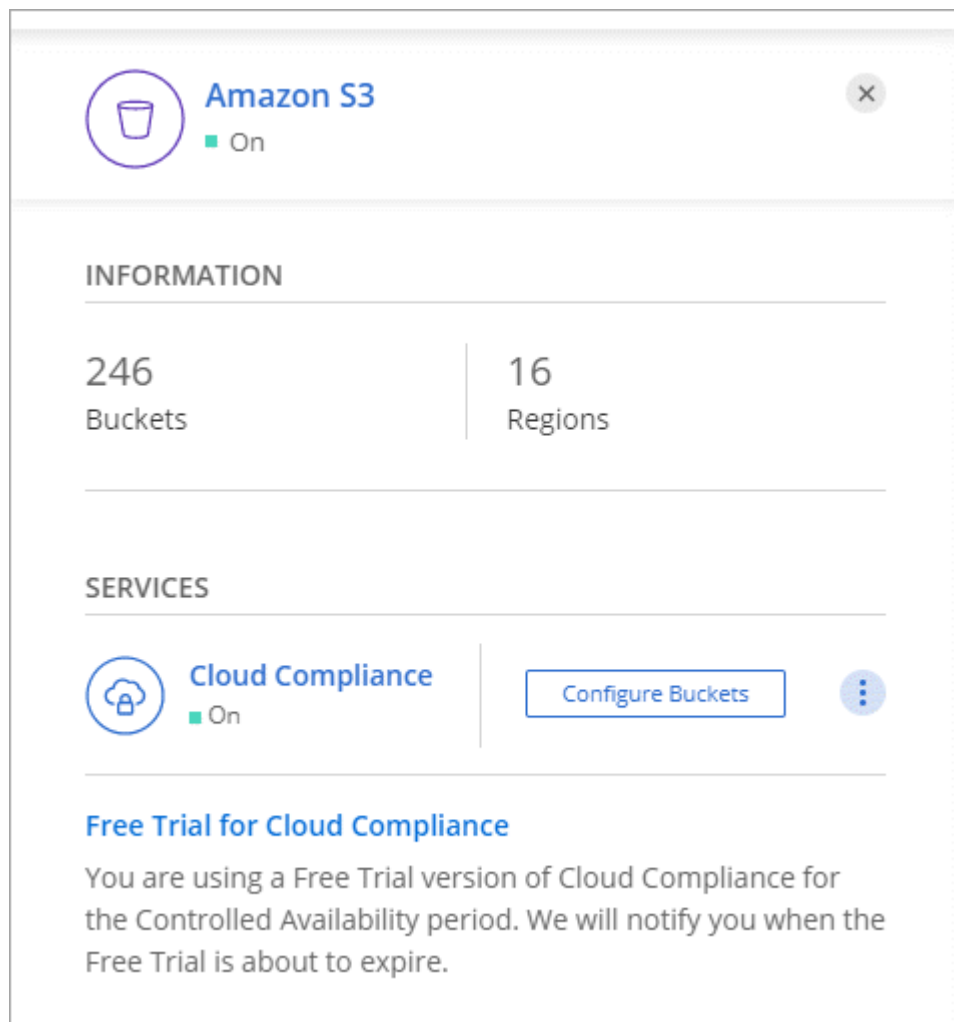
After Cloud Manager enables Cloud Compliance on Amazon S3, the next step is to configure the buckets that you want to scan.

When Cloud Manager is running in the AWS account that has the S3 buckets you want to scan, it discovers those buckets and displays them in an Amazon S3 working environment.

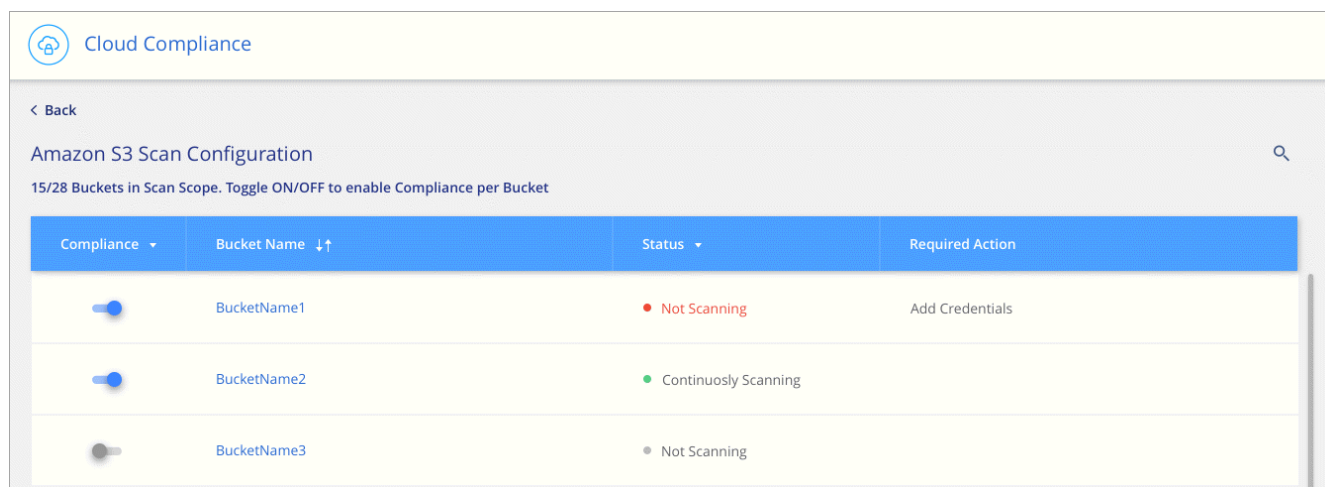
Cloud Compliance can also [scan S3 buckets that are in different AWS accounts](#).

## Steps

1. Select the Amazon S3 working environment.
2. In the pane on the right, click **Configure Buckets**.



3. Enable compliance on the buckets that you want to scan.



## Result

Cloud Compliance starts scanning the S3 buckets that you enabled. If there are any errors, they'll appear in the Status column, alongside the required action to fix the error.

## Scanning buckets from additional AWS accounts

You can scan S3 buckets that are under a different AWS account by assigning a role from that account to access the existing Cloud Compliance instance.





### Steps

1. Go to the target AWS account where you want to scan S3 buckets and create an IAM role by selecting **Another AWS account**.

### Create role




#### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

#### Specify accounts that can use this role

Account ID\*

- Options**
- ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA 

Be sure to do the following:

- Enter the ID of the account where the Cloud Compliance instance resides.
- Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
- Attach the Cloud Compliance IAM policy. Make sure it has the required permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:HeadBucket"
      ],
      "Resource": "*"
    }
  ]
}
```

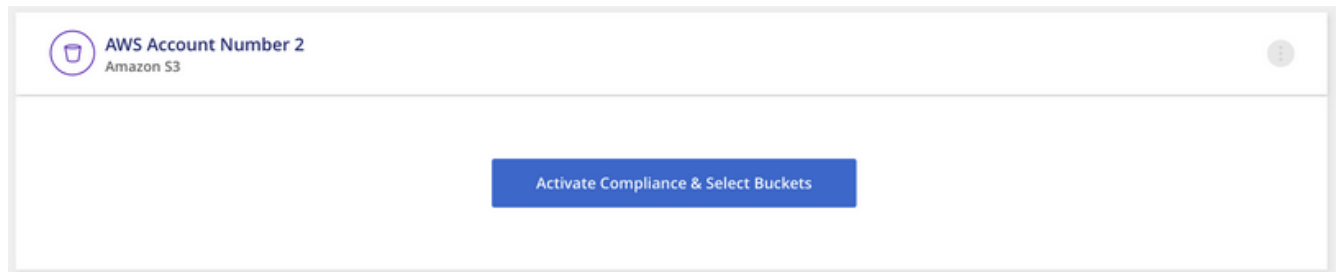
2. Go to the source AWS account where the Cloud Compliance instance resides and select the IAM role that is attached to the instance.
  - a. Change the **Maximum CLI/API session duration** from 1 hour to 12 hours and save that change.
  - b. Click **Attach policies** and then click **Create policy**.
  - c. Create a policy that includes the "sts:AssumeRole" action and the ARN of the role that you created in the target account.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

The Cloud Compliance instance profile account now has access to the additional AWS account.

3. Go to the **Amazon S3 Scan Configuration** page and the new AWS account is displayed. Note that it can take a few minutes for Cloud Compliance to sync the new account's working environment and show this information.



4. Click **Activate Compliance & Select Buckets** and select the buckets you want to scan.

#### Result

Cloud Compliance starts scanning the new S3 buckets that you enabled.

## Scanning on-premises ONTAP data with Cloud Compliance by using SnapMirror

You can scan your on-premises ONTAP data with Cloud Compliance by replicating the on-prem NFS or CIFS data to a Cloud Volumes ONTAP working environment and then enabling compliance. Scanning the data directly from an on-premises ONTAP working environment isn't supported.

### Steps

1. From Cloud Manager, create a SnapMirror relationship between the on-premises ONTAP cluster and Cloud Volumes ONTAP.
  - a. [Discover the on-premises cluster in Cloud Manager.](#)
  - b. [Create a SnapMirror replication between the on-premises ONTAP cluster and Cloud Volumes ONTAP from Cloud Manager.](#)
2. From the ONTAP CLI, configure the destination volume for data access.
  - a. [Mount destination volumes to the NAS namespace.](#)
  - b. If you're using CIFS:
    - [Create a CIFS share on the destination volume.](#)
    - [Apply the appropriate ACLs to the CIFS share at the destination volume.](#)
  - c. If you're using NFS:
    - [Assign NFS export policies to the destination volume.](#)
3. From Cloud Manager, activate Cloud Compliance on the Cloud Volumes ONTAP working environment that contains the SnapMirror data.
  - a. Click **Working Environments**.
  - b. Select the working environment that contains the SnapMirror data.
  - c. In the pane on the right, click **Enable Compliance**.

[Click here if you need help with enabling Cloud Compliance on a Cloud Volumes ONTAP system.](#)

## 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.

By default, the Cloud Compliance dashboard displays compliance data for all working environments. If you want to see data for only some of the working environments, [select those working environments](#).

## Personal data

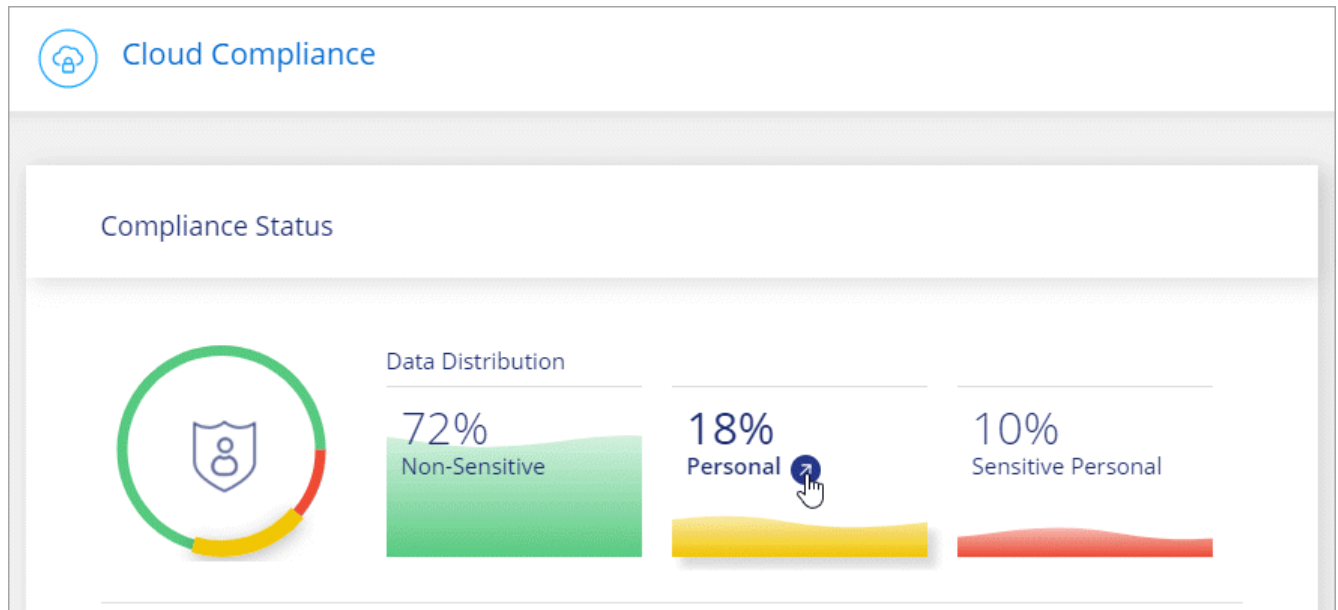
Cloud Compliance automatically identifies specific words, strings, and patterns (Regex) inside the data. For example, Personal Identification Information (PII), credit card numbers, social security numbers, bank account numbers, and more. [See the full list](#).

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.

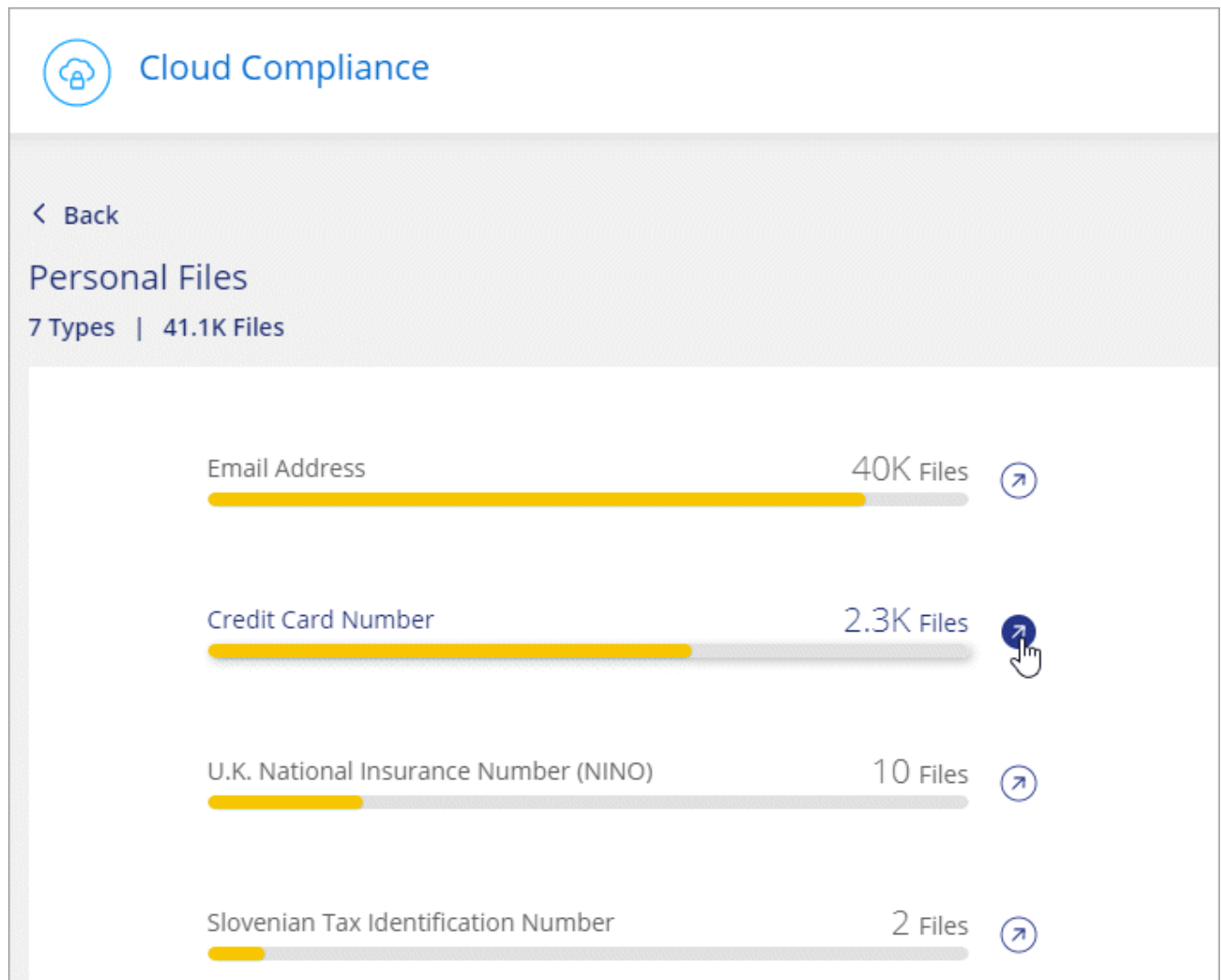
### Viewing files that contain personal data

#### Steps

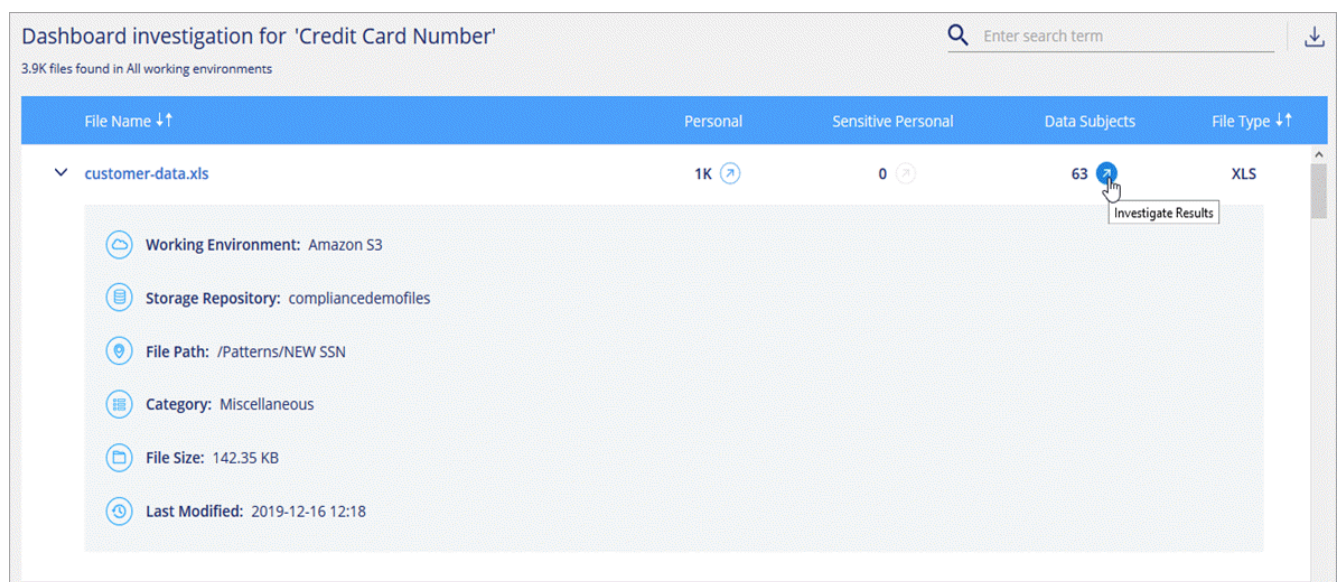
1. At the top of Cloud Manager, click **Compliance**.
2. To investigate the details for all personal data, click the icon next to the personal data percentage.



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



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



5. You can also filter the contents of the investigation page to display only the results you want to see.

Filters include working environment, category, private data, file type, last modified date, and whether the S3 object's permissions are open to public access.

Dashboard Investigation		3011 Results Found				Q	↓
FILTERS: Clear All		File Name ↓↑	Personal ↓↑	Sensitive Personal ↓↑	Data Subjects ↓↑	File Type ↓↑	
Working Environment	+	> Expense Report EXP-TPO-1060388	6	3	16	PDF	
Storage Repository	+	> Expense Report EXP-TPO-1060388	9	2	11	PDF	
Category	+	> Expense Report EXP-TPO-1060388	4	1	7	PDF	
Private Data 6	+	> Expense Report EXP-TPO-1060388	9	1	6	PDF	
File Type	+	> Expense Report EXP-TPO-1060388	8	6	4	PDF	

## 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

Type	Identifier	Proximity validation?
National Identifiers	Belgian ID (Numero National)	Yes
	Brazilian ID (CPF)	Yes
	Bulgarian ID (Unified Civil Number)	Yes
	California Driver's License	Yes
	Cyprus Tax Identification Number (TIC)	Yes
	Danish ID (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 ID	Yes
	Lithuanian ID (Asmens kodas)	Yes
	Luxembourg ID	Yes
	Maltese ID Card Number	Yes
	Netherlands ID (BSN)	Yes
	Polish Tax Identification Number	Yes
	Portuguese ID (NIF)	Yes
	Romanian ID (CNP)	Yes
	Slovak Tax Identification Number	Yes
	Slovenian Tax Identification Number	Yes
	South African ID	Yes
	Spanish ID (DNI)	Yes
	Swedish ID (personnummer)	Yes
	U.K. ID (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."

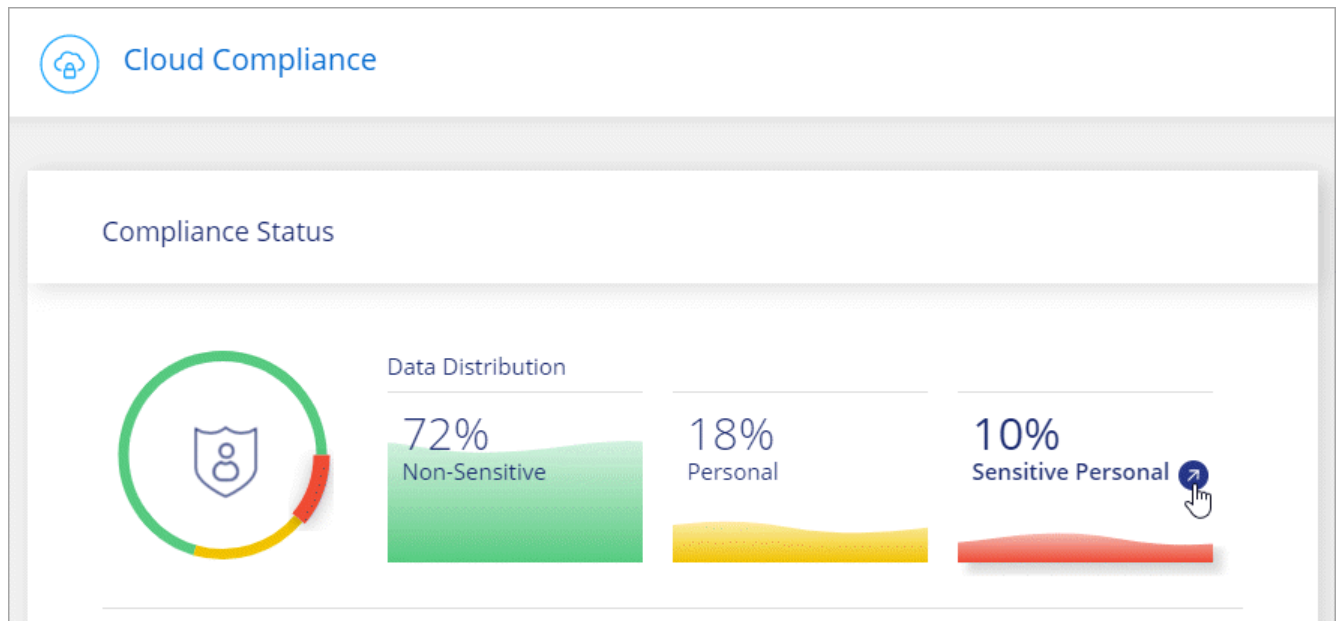


Only English is supported when scanning for sensitive personal data. Support for more languages will be added later.

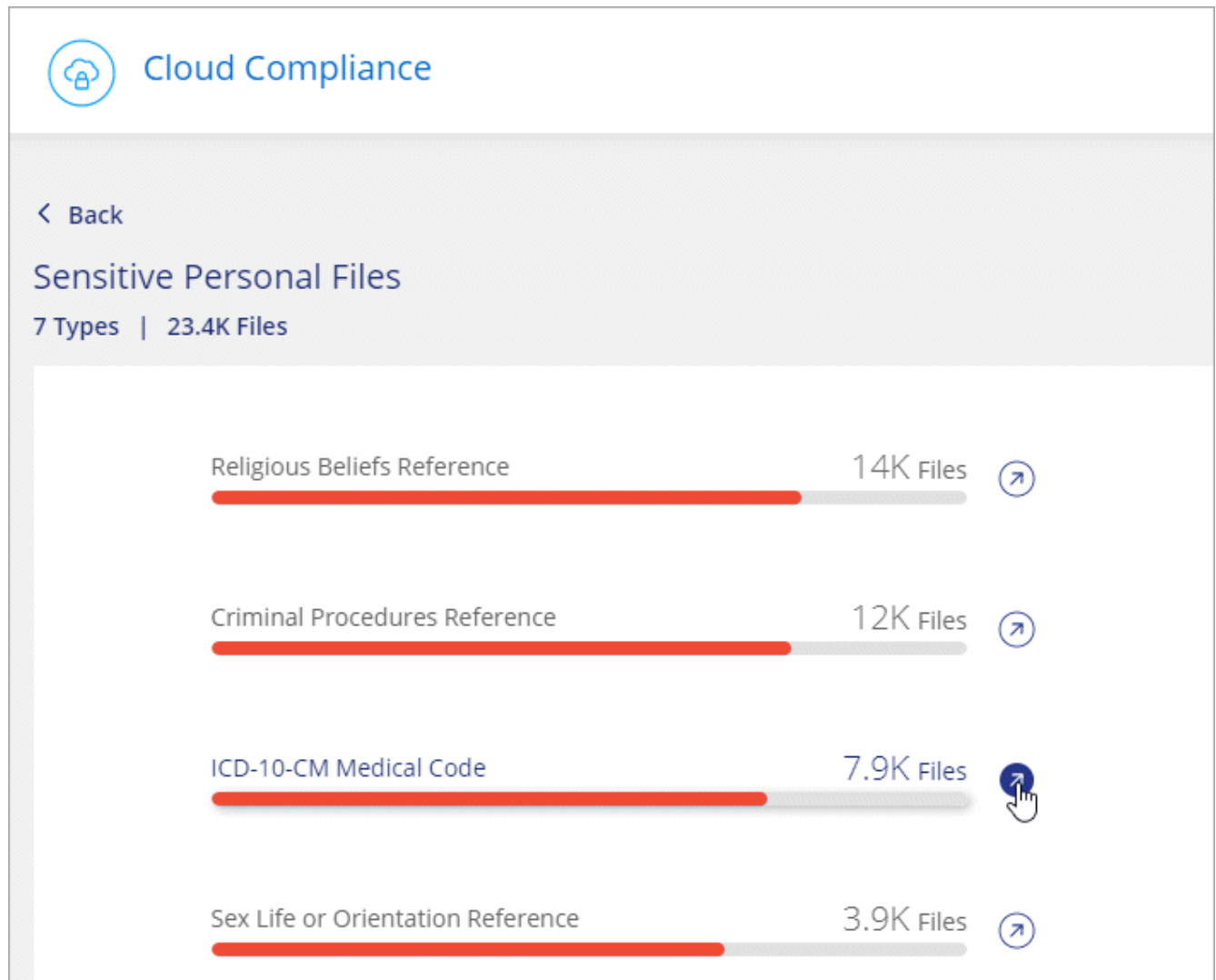
### Viewing files that contain sensitive personal data

#### Steps

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



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



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.

### 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.

#### ICD-10-CM Medical Codes

Codes used in the medical and health industry.



## 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 types of information that you have. For example, a category like resumes or employee contracts can include sensitive data. When you investigate the results, you might find that employee contracts are stored in an insecure location. You can then correct that issue.



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

## Viewing files by categories

### *Steps*

1. At the top of Cloud Manager, click **Compliance**.
2. Click the **Investigate Results** icon for one of the top 4 categories directly from the main screen, or click **View All** and then click the icon for any of the categories.

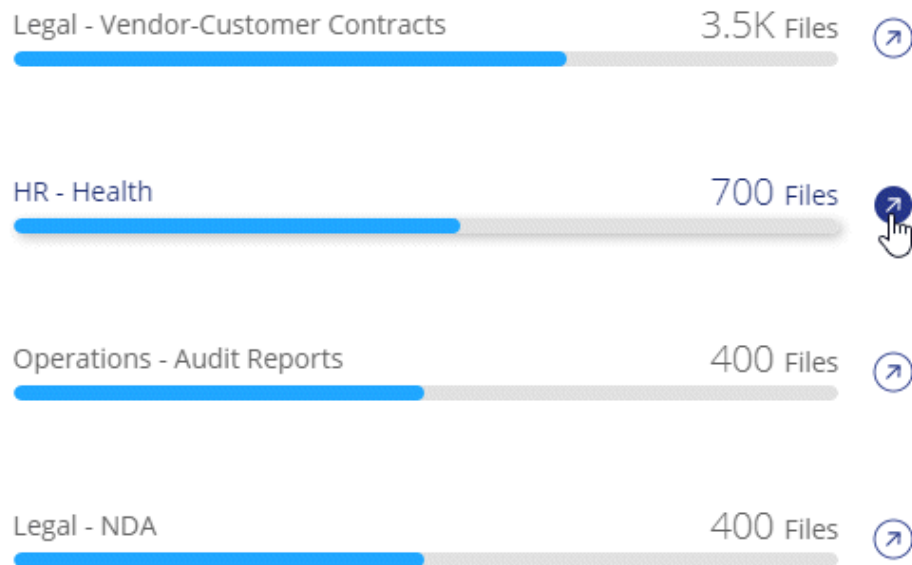


## Cloud Compliance

< Back

### Categories

27 Categories | 219.9K Files



3. 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.

### Types of categories

Cloud Compliance categorizes your data as follows:

#### 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

## **Metadata categories**

- Application Data
- Archive Files
- Audio
- Business Application Data
- CAD Files
- Code
- Database and index files
- Design Files
- Email Application Data

- Executables
- Financial Application Data
- Health Application Data
- Images
- Logs
- Miscellaneous Documents
- Miscellaneous Presentations
- Miscellaneous Spreadsheets
- Videos

## File types

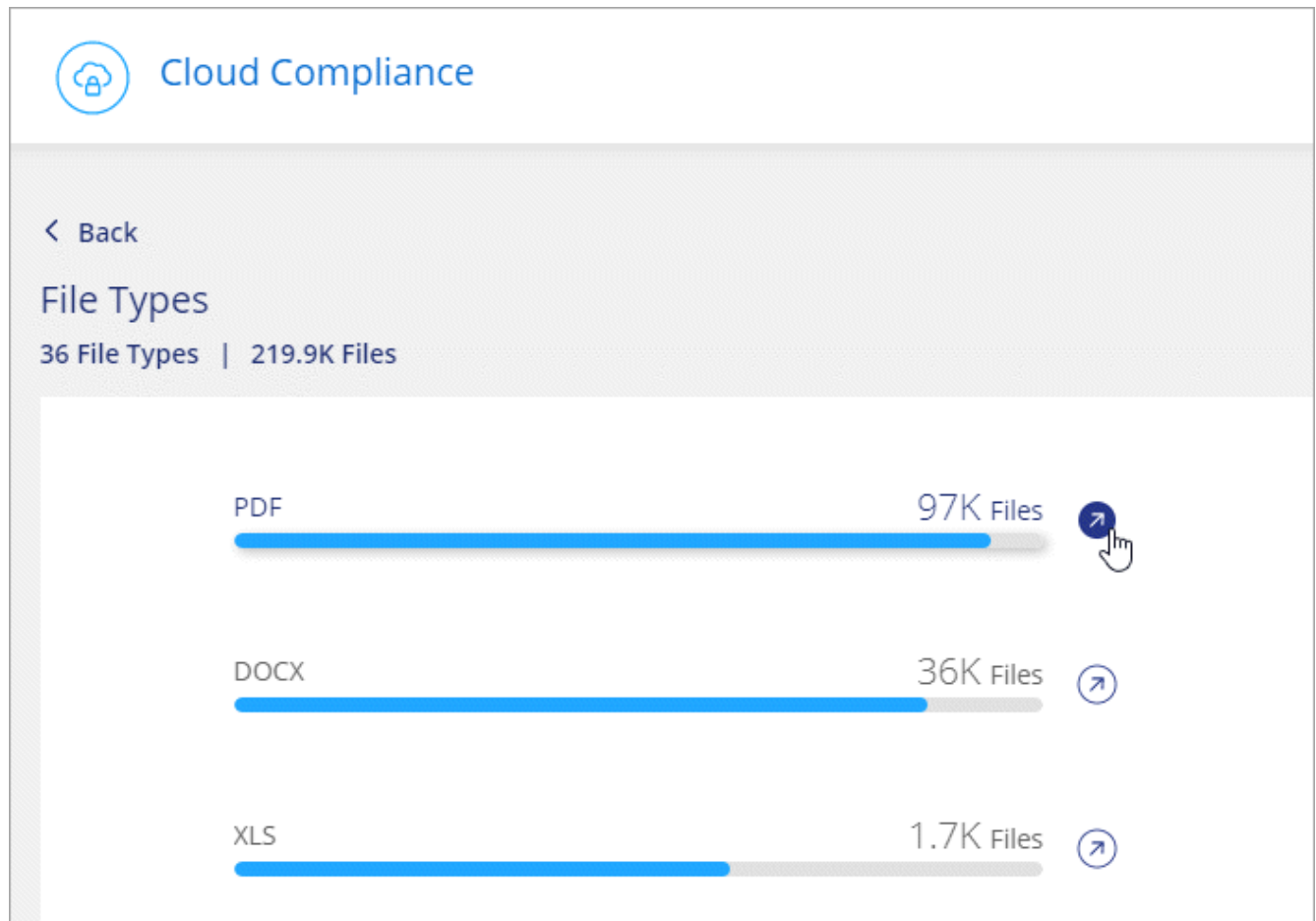
Cloud Compliance takes the data that it scanned and breaks it down by file type. Reviewing your file types can help you control your sensitive data because you might find that certain file types are not stored correctly. [See the list of file types](#).

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

### Viewing file types

#### *Steps*

1. At the top of Cloud Manager, click **Compliance**.
2. Click the **Investigate Results** icon for one of the top 4 file types directly from the main screen, or click **View All** and then click the icon for any of the file types.



3. 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.

### Types of files

Cloud Compliance scans all files for category and metadata insights and displays all file types in the file types section of the dashboard.

But when Cloud Compliance detects Personal Identifiable Information (PII), or when it performs a DSAR search, only the following file formats are supported:

.PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF, and .JSON.

### Viewing data from specific working environments

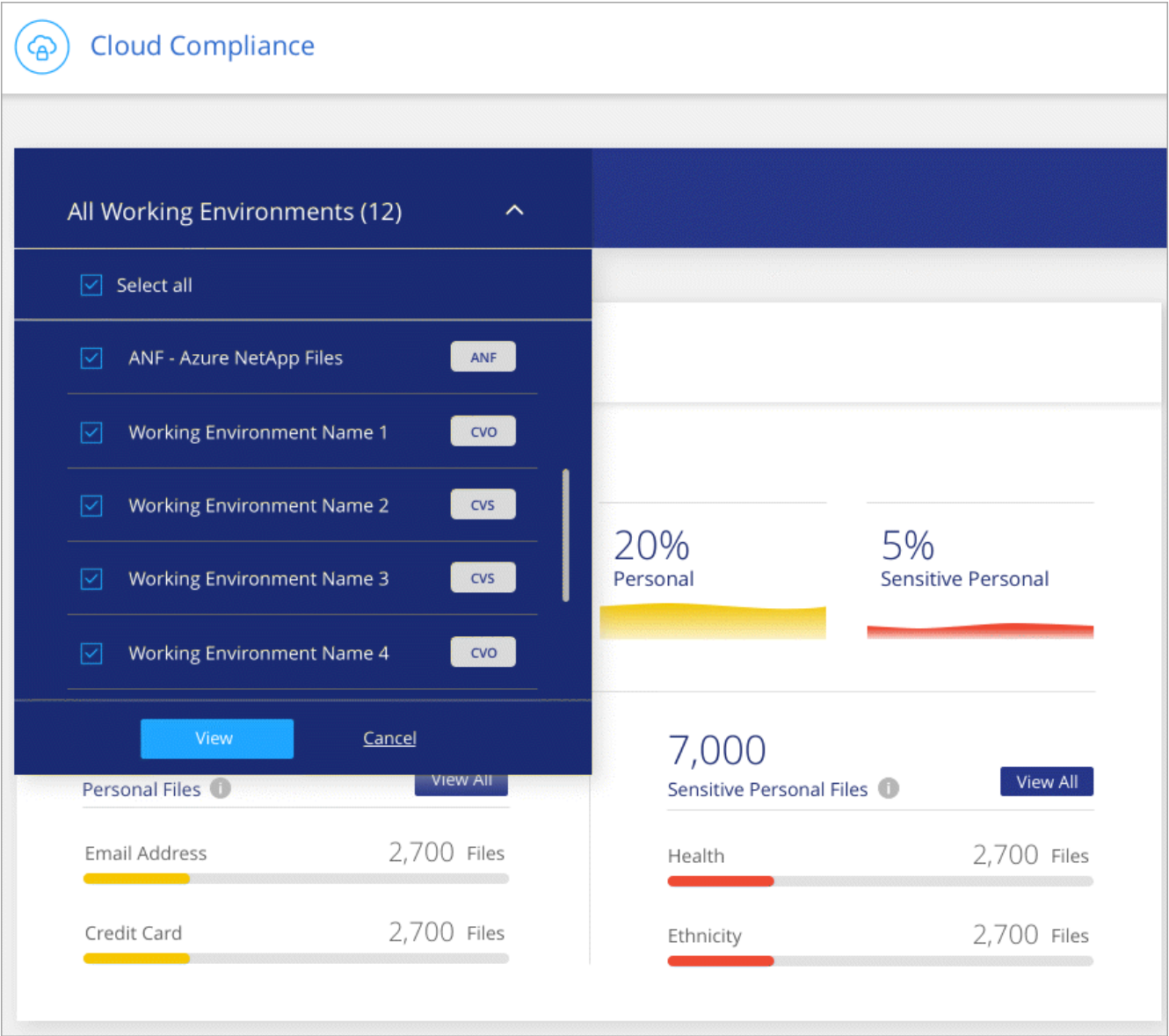
You can filter the contents of the Cloud Compliance dashboard to see compliance data for specific working environments.

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

#### Steps

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

click **View**.



**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)

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

Each file list includes the following information:

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

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

# Viewing compliance reports

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

By default, the Cloud Compliance dashboard displays compliance data for all working environments. If you want to view reports that contain data for only some of the working environments, [select those working environments](#).



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.

## 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.

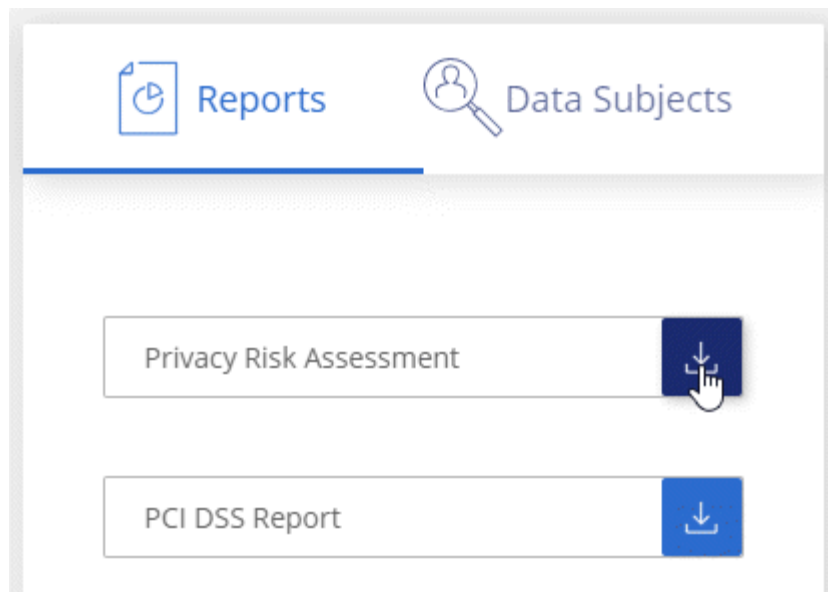
## Generating the Privacy Risk Assessment Report

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%
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%

Severity score	Logic
9	Two of the variables are larger than 15%
10	Three of the variables are larger than 15%

## 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 working environments.

### Encryption

The percentage of files containing credit card information that are on encrypted or unencrypted working environments. This information is specific to Cloud Volumes ONTAP.

### Ransomware Protection

The percentage of files containing credit card information that are on working environments 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

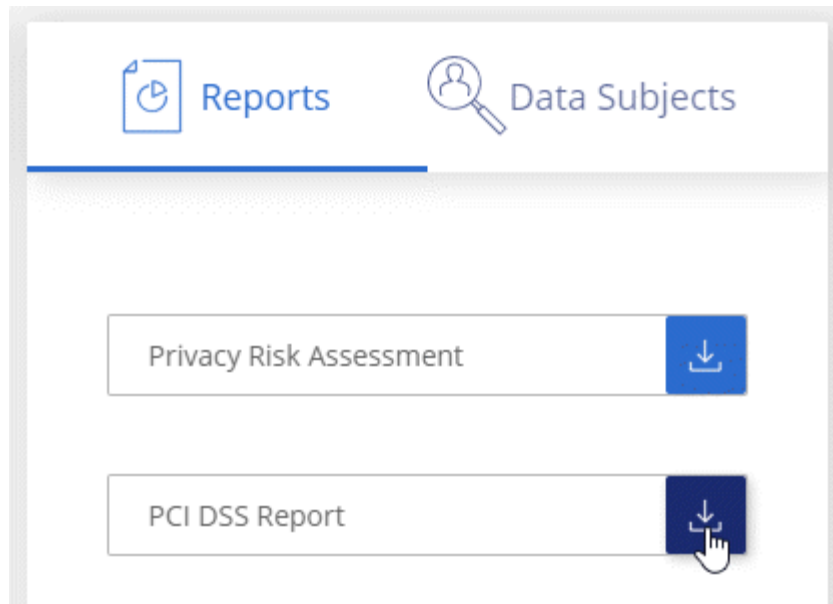
The working environments where the credit card information was found and whether encryption and ransomware protection are enabled.

## Generating the PCI DSS 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 **PCI DSS Report**.



### *Result*

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

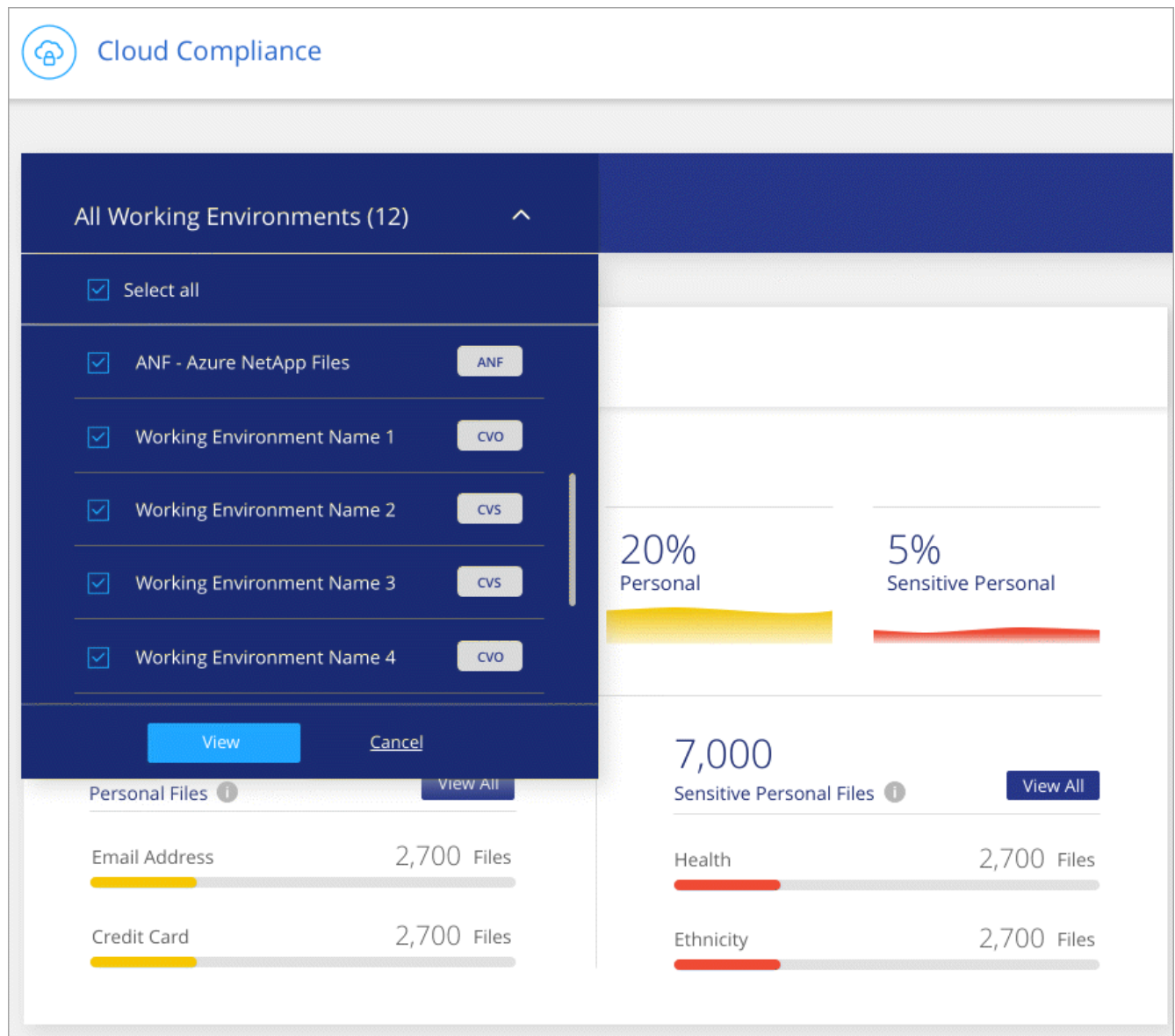
## Selecting the working environments for reports

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

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

### *Steps*

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



## 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 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.

## 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](#).

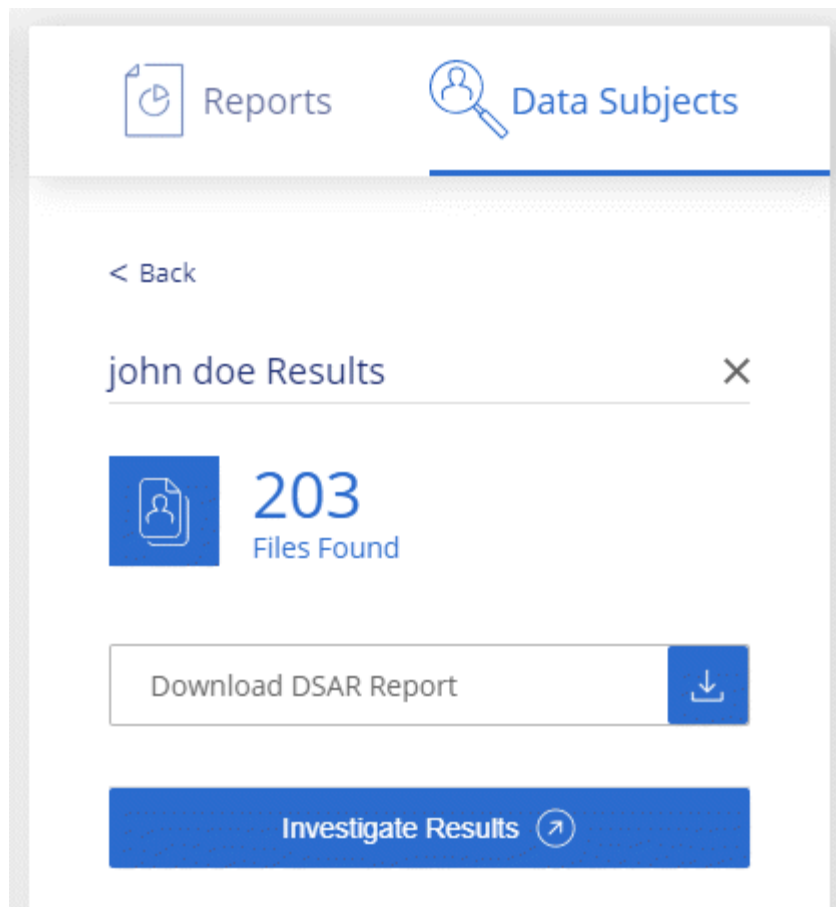


Only English is supported when searching for the names of data subjects. Support for more languages will be added later.

### 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 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.
- **Investigate Results:** A page that enables you to investigate the data by searching, sorting, expanding details for a specific file, and by downloading the file list.



If there are more than 10,000 results, only the top 10,000 appear in the file list.

## 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 working environments.

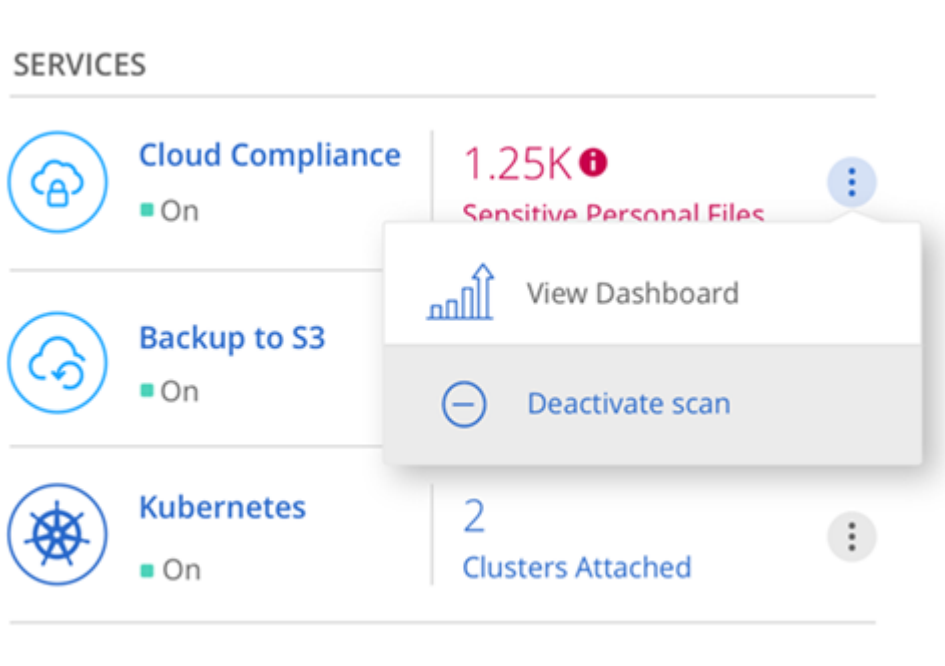
### Deactivating compliance scans for a working environment


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**.



You can also disable compliance scans for a working environment from the Scan Configuration page by clicking the  icon and selecting **Deactivate Compliance**.

## Deleting the Cloud Compliance instance

You can delete the Cloud Compliance instance if you no longer want to use Cloud Compliance. 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 Azure NetApp Files configurations, Cloud Volumes ONTAP systems hosted in AWS or Azure, and Amazon S3 buckets.

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 that are managed by Cloud Volumes ONTAP and Azure NetApp Files.

Cloud Compliance can also scan data stored on Amazon S3 buckets.

[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 volumes and indexes the data insights found.

[Learn more about how Cloud Compliance works.](#)

## How much does Cloud Compliance cost?

The cost depends on the type of working environment that you're scanning.

- Cloud Compliance is offered as part of Cloud Volumes ONTAP and Azure NetApp Files. There are no additional charges from NetApp, but you will incur costs from your cloud provider. [Learn more.](#)
- You need to pay to scan your Amazon S3 buckets. [Learn about pricing.](#)

## 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.](#)

### PCI DSS report

Helps you identify the distribution of credit card information across your files.

## 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.



Changing or resizing the instance/VM type isn't supported. You need to use the default size that's provided.

[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.

## Which file types are supported?

Cloud Compliance scans all files for category and metadata insights and displays all file types in the file types section of the dashboard.

But when Cloud Compliance detects Personal Identifiable Information (PII), or when it performs a DSAR search, only the following file formats are supported:

.PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF, and .JSON.

## 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 and Azure NetApp Files. We're planning to support Cloud Compliance with additional cloud offerings such as Cloud Volumes Service.

[Learn more.](#)

## 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.](#)

## Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

## Trademark Information

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