Malware Protection in Amazon Macie

**Contents**

[Scope 2](#_Toc115190395)

[Problem Statement 2](#_Toc115190396)

[Introduction 2](#_Toc115190397)

[Features of Amazon Macie 3](#_Toc115190408)

Getting started with amazon Macie [3](#_Toc115190413)

[Implementation 6](#_Toc115190402)

Step1:[Enable Amazon Macie 6](#_Toc115190403)

Step2:[Configure Repository 7](#_Toc115190405)

Step3:[Explore Sample Findings 8](#_Toc115190412)

Step4:[Create a job to discover sensitive data](#_Toc115190412) 10

Step5:[Review your Findings 12](#_Toc115190412)

Services Protected by Amazon Macie18

[How Amazon Macie Protects S3? 18](file:///C:\Users\User\Desktop\AWS\To%20GitHub\Amazon%20Inspector.docx#_Toc115190412)

Advantages19

[Limitations 20](#_Toc115190402)

**Malware Protection in** **Amazon Macie**

Document Name: Malware Protection in Amazon Macie

Owner: Hema Paul

**Scope**

Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial data, to provide you with a better understanding of the data that your organization stores in Amazon Simple Storage Service (Amazon S3). Macie also provides you with an inventory of your S3 buckets, and it automatically evaluates and monitors those buckets for security and access control. Within minutes, Macie can identify and report overly permissive or unencrypted buckets for your organization.

**Problem Statement**

If Macie detects sensitive data or potential issues with the security or privacy of your data, it creates detailed findings for you to review and remediate as necessary.

**Introduction**

Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to help you discover, monitor, and protect sensitive data in your AWS environment.

**Features of Amazon Macie**

Here are some of the key ways that Amazon Macie can help you discover, monitor, and protect your sensitive data in Amazon S3.

**Automate the discovery of sensitive data**

With Macie, you can automate discovery and reporting of sensitive data by [creating and running sensitive data discovery jobs](https://docs.aws.amazon.com/macie/latest/user/discovery-jobs.html). A sensitive data discovery job analyzes objects in S3 buckets to determine whether they contain sensitive data. If Macie detects sensitive data in an object, it creates a sensitive data finding for you. The finding provides a detailed report of the sensitive data that Macie found.

You can configure a job to run only once, for on-demand analysis and assessment, or on a recurring basis for periodic analysis, assessment, and monitoring. You can also choose various options to control the breadth and depth of a job's analysis—the S3 buckets to analyze, the sampling depth, and custom include and exclude criteria that derive from properties of S3 objects. With these scheduling and scope options, you can build and maintain a comprehensive view of the data that your organization stores in Amazon S3 and any security or compliance risks for that data.

**Discover a variety of sensitive data types**

When you create a sensitive data discovery job, you can configure the job to use built-in criteria and techniques, such as machine learning and pattern matching, to analyze objects in S3 buckets. These criteria and techniques, referred to as [managed data identifiers](https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html), can detect a large and growing list of sensitive data types for many countries and regions, including multiple types of personally identifiable information (PII), financial data, and credentials data.

You can also configure the job to use [custom data identifiers](https://docs.aws.amazon.com/macie/latest/user/custom-data-identifiers.html). A custom data identifier is a set of criteria that you define to detect sensitive data—a regular expression (*regex*) that defines a text pattern to match and, optionally, character sequences and a proximity rule that refine the results. With this type of identifier, you can detect sensitive data that reflects your particular scenarios, intellectual property, or proprietary data, and supplement the managed data identifiers that Macie provides.

To fine tune the analysis, a job can also use [allow lists](https://docs.aws.amazon.com/macie/latest/user/allow-lists.html). Allow lists define specific text and text patterns that you want Macie to ignore in S3 objects—for example, the names of public representatives for your organization, public phone numbers for your organization, or sample data that your organization uses for testing.

**Evaluate and monitor data for security and access control**

When you enable Macie, Macie immediately generates and begins maintaining a complete inventory of your S3 buckets, and it begins evaluating and monitoring the buckets for security and access control. If Macie detects a potential issue with the security or privacy of a bucket, it creates a [policy finding](https://docs.aws.amazon.com/macie/latest/user/findings-types.html#findings-policy-types) for you.

In addition to specific findings, a [dashboard](https://docs.aws.amazon.com/macie/latest/user/monitoring-s3-dashboard.html) gives you a snapshot of aggregated statistics for your buckets. This includes statistics that indicate how many of your buckets are publicly accessible, are shared with other AWS accounts, or don’t encrypt objects by default. You can drill down on each statistic to review the supporting data.

Macie also provides detailed information and statistics for individual buckets in your inventory. This data includes breakdowns of a bucket’s public access and encryption settings, and the size and number of objects that Macie can analyze to detect sensitive data in the bucket. You can [browse the inventory](https://docs.aws.amazon.com/macie/latest/user/monitoring-s3-inventory.html), or sort and filter the inventory by certain fields. When you choose a bucket, a panel displays the bucket’s details.

**Review and analyze findings**

In Macie, a finding is a detailed report of sensitive data in an S3 object or a potential policy-related issue with the security or privacy of an S3 bucket. Each finding provides a severity rating, information about the affected resource, and additional details, such as when and how Macie found the issue.

To [review, analyze, and manage findings](https://docs.aws.amazon.com/macie/latest/user/findings.html), you can use the **Findings** pages on the Amazon Macie console. These pages list your findings and provide the details of individual findings. They also provide multiple options for grouping, filtering, sorting, and suppressing findings. You can also use the Amazon Macie API to query, retrieve, and suppress findings. If you use the API, you can pass the data to another application, service, or system for deeper analysis, long-term storage, or reporting.

**Monitor and process findings with other services and systems**

To support integration with other services and systems, Macie [publishes findings to Amazon EventBridge](https://docs.aws.amazon.com/macie/latest/user/findings-monitor-events-eventbridge.html) as finding events. EventBridge is a serverless event bus service that can route findings data to targets such as AWS Lambda functions and Amazon Simple Notification Service (Amazon SNS) topics. With EventBridge, you can monitor and process findings in near-real time as part of your existing security and compliance workflows.

You can configure Macie to also [publish findings to AWS Security Hub](https://docs.aws.amazon.com/macie/latest/user/securityhub-integration.html). Security Hub is a service that provides a comprehensive view of your security posture across your AWS environment and helps you check your environment against security industry standards and best practices. With Security Hub, you can more easily monitor and process your findings as part of a broader analysis of your organization's security posture in AWS.

**Centrally manage multiple Macie accounts**

If your AWS environment has multiple accounts, you can [centrally manage Macie](https://docs.aws.amazon.com/macie/latest/user/macie-accounts.html) for accounts in your environment. You can do this in two ways, by integrating Macie with AWS Organizations or by sending membership invitations from Macie.

In a multiple-account configuration, a designated Macie administrator can perform certain tasks and access certain Macie settings, data, and resources for accounts that are members of the same organization. Tasks include reviewing information about S3 buckets that are owned by member accounts, reviewing policy findings for those buckets, and running sensitive data discovery jobs to detect sensitive data in the buckets. If the accounts are associated through AWS Organizations, the Macie administrator can also enable Macie for member accounts in the organization.

**Develop and manage resources programmatically**

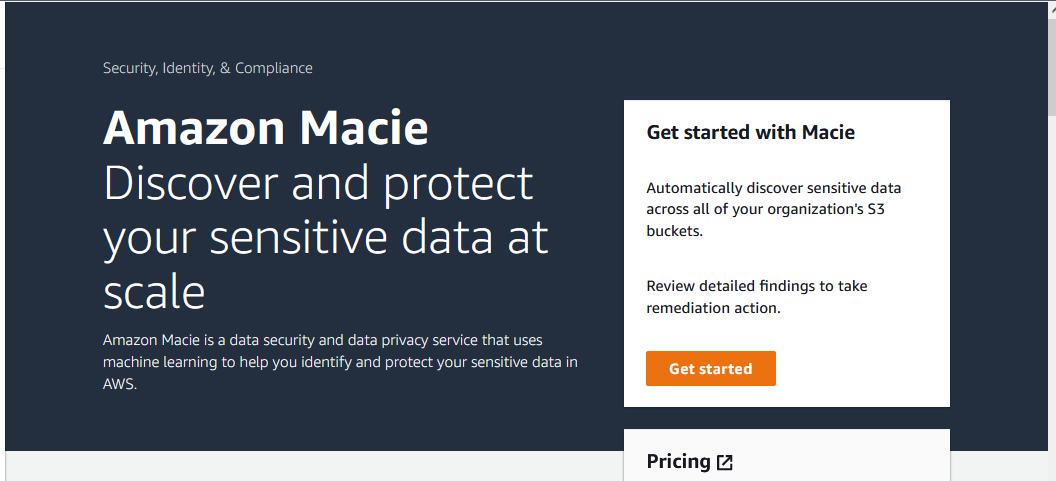
In addition to the Amazon Macie console, you can interact with Macie by using the [Amazon Macie API](https://docs.aws.amazon.com/macie/latest/APIReference/welcome.html). The Amazon Macie API gives you comprehensive, programmatic access to your Macie account and resources.

To develop and manage resources with the Amazon Macie API, you can send HTTPS requests directly to Macie or use a current version of an AWS command line tool or an AWS SDK. AWS provides tools and SDKs that consist of libraries and sample code for various languages and platforms, such as PowerShell, Java, Go, Python, C++, and .NET.

**Getting started with Amazon Macie**

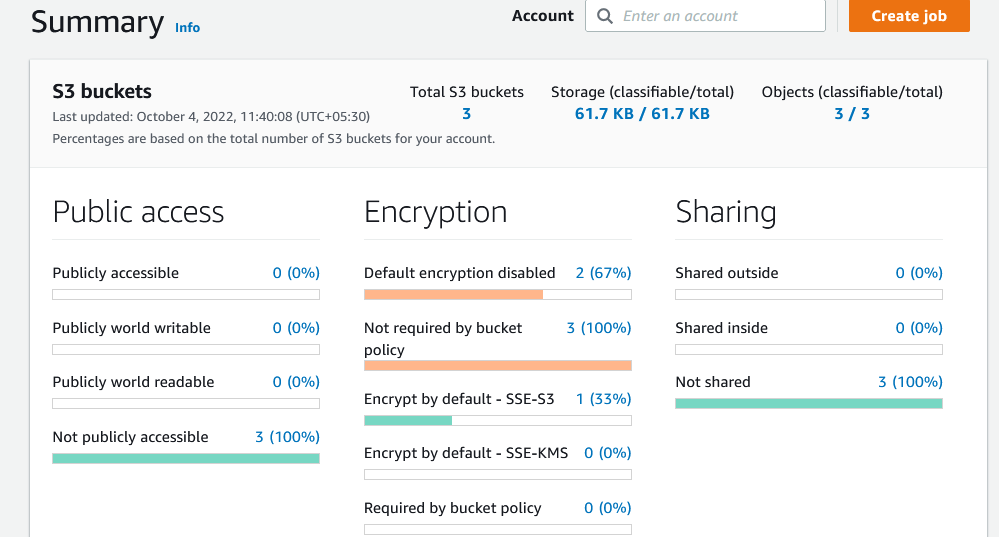
When you sign up for Amazon Web Services (AWS), your account is automatically signed up for all AWS services, including Amazon Macie. However, to enable and use Macie, you have to first set up permissions that allow you to access the Amazon Macie console and API operations. You can do this by using the AWS Identity and Access Management (IAM) console to attach the AmazonMacieFullAccess managed policy to your IAM identity. To learn more, see [AWS managed policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html) in the IAM User Guide.

**Implementation**



**Step 1: Enable Amazon Macie**

View summary



Within minutes, Macie generates an inventory of the Amazon Simple Storage Service (Amazon S3) buckets for your account in the current Region. Macie also begins monitoring the buckets for security and access control.

To review your bucket inventory, choose **S3 buckets** in the navigation pane on the console. To then display details about a bucket, choose the bucket's name in the table. The details panel displays statistics and other information that provides insight into the security and privacy of the bucket’s data.

## Step 2: Configure a repository for sensitive data discovery results

With Macie, you detect sensitive data by creating and running sensitive data discovery jobs. A sensitive data discovery job analyzes objects in S3 buckets to determine whether the objects contain sensitive data. If Macie discovers sensitive data in an object, Macie creates a sensitive data finding. A sensitive data finding is a detailed report of sensitive data that Macie found in an object.

Macie also creates a sensitive data discovery result for each object that you configure a job to analyze. A sensitive data discovery result is a record that logs details about the analysis of an object. This includes objects that don't contain sensitive data, and therefore don't produce sensitive data findings, and objects that Macie can't analyze due to issues such as permissions settings. If an object does contain sensitive data, the sensitive data discovery result includes data from the corresponding sensitive data finding. It provides additional information too.

Macie stores your sensitive data discovery results for 90 days. To access the results and enable long-term storage and retention of them, configure Macie to store the results in an S3 bucket. You must do this within 30 days of enabling Macie. After you do this, the S3 bucket can serve as a definitive, long-term repository for all of your discovery results.

## Step 3: Explore sample findings

Macie provides two categories of findings, policy findings and sensitive data findings. A finding is a detailed report of a potential policy violation for an S3 bucket or sensitive data in an S3 object. Macie generates a policy finding when the policies or settings for an S3 bucket are changed in a way that reduces the security or privacy of the bucket and the bucket's objects. Macie generates a sensitive data finding when it discovers sensitive data in an S3 object that you configure a sensitive data discovery job to analyze. Within each category, there are multiple types of findings.

To explore and learn about the different categories and types of findings that Macie can generate, optionally create and review sample findings. Sample findings use example data and placeholder values to demonstrate the kinds of information that Macie might include in each type of finding. Follow these steps to create and review sample findings.

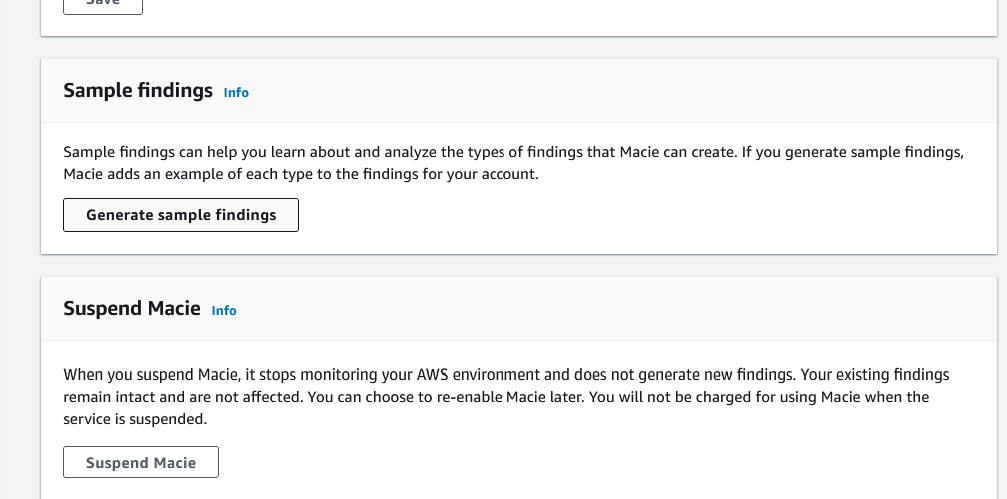
**To create and review sample findings**

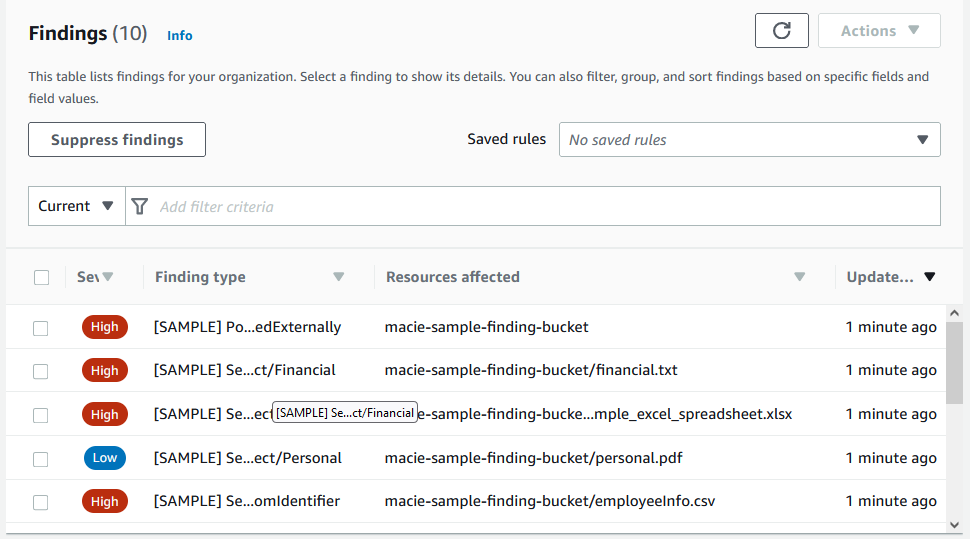
* Open the Amazon Macie console.
* In the navigation pane, choose **Settings**.
* Under **Sample findings**, choose **Generate sample findings**.
* Macie generates one sample finding for each type of finding that Macie supports.
* In the navigation pane, choose **Findings**.

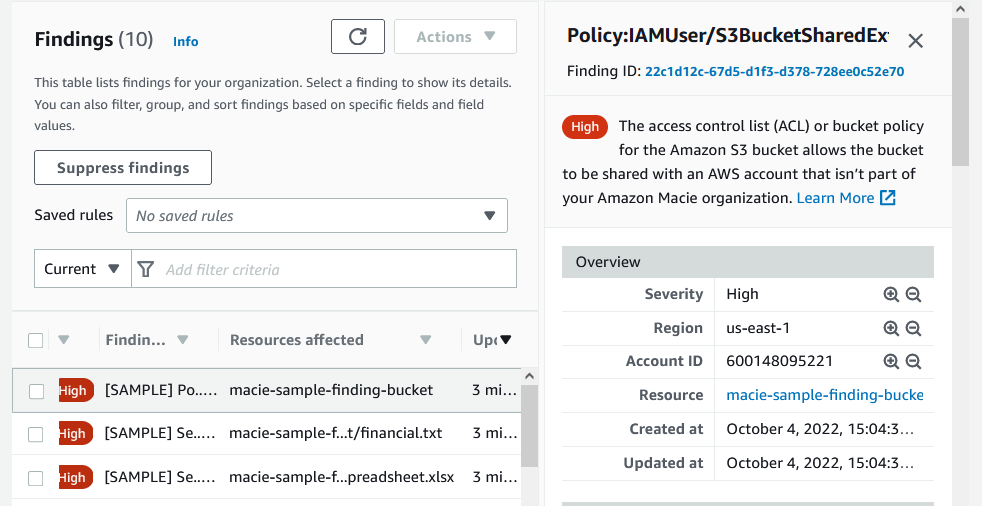
The **Findings** page displays current findings for your account in the current AWS Region. This includes the sample findings that you created in the preceding step.

* On the **Findings** page, locate findings whose type begins with **[SAMPLE]**.
* To review the details of a specific sample finding, choose any field other than the check box for the finding. The details panel displays information for the finding.

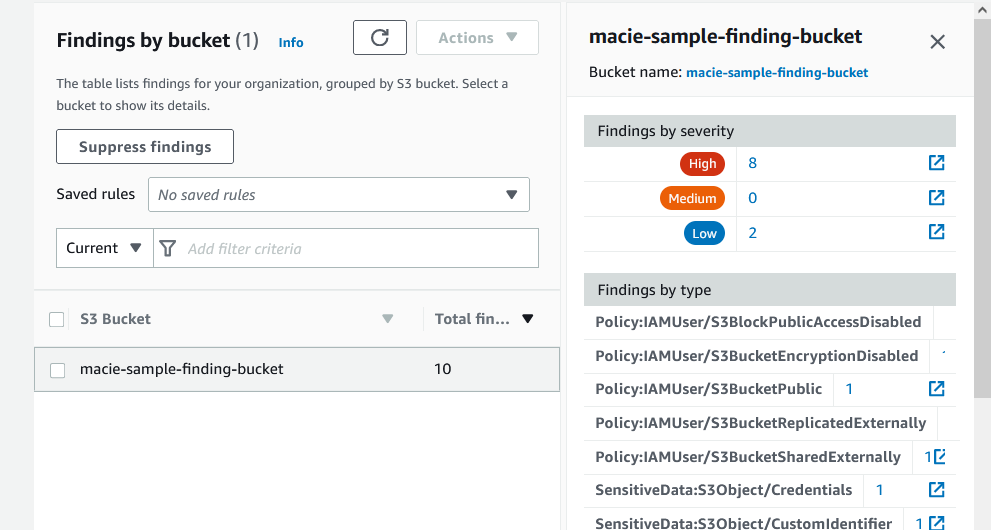
**Generate Sample findings**







Findings by bucket



**Step 4: Create a job to discover sensitive data**

In Macie, you create and run sensitive data discovery jobs to analyze S3 objects and report sensitive data in those objects. To analyze objects, a job can use built-in, managed data identifiers that Macie provides, custom data identifiers that you create, or a combination of the two. For information about the types of S3 objects that Macie can analyze, see [Discovering sensitive data](https://docs.aws.amazon.com/macie/latest/user/data-classification.html). For information about the types of sensitive data that Macie can detect, see [Using managed data identifiers](https://docs.aws.amazon.com/macie/latest/user/managed-data-identifiers.html).

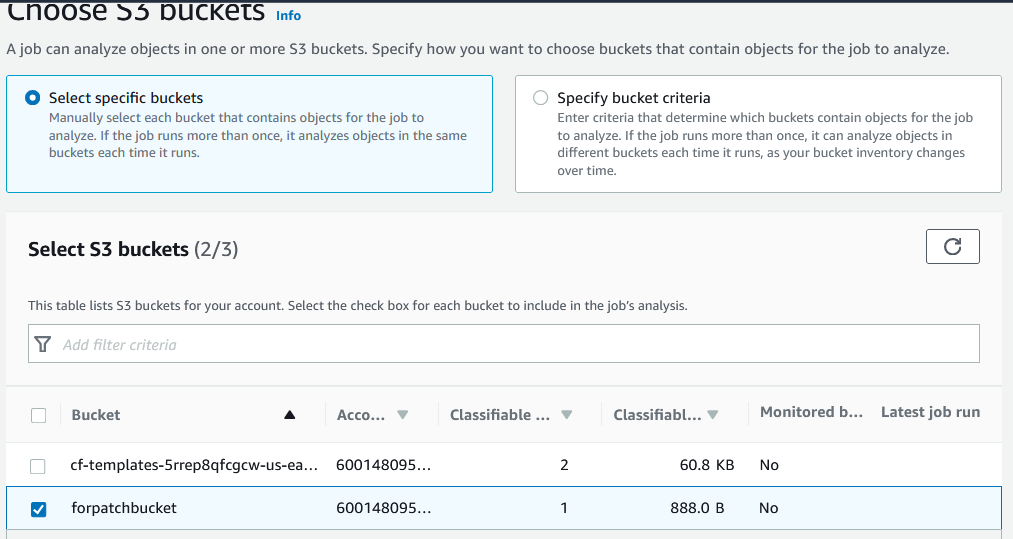
Follow these steps to create a job that runs once, immediately after you create it, and uses default settings. To learn how to create a job that runs periodically or uses custom settings, see [Creating a sensitive data discovery job](https://docs.aws.amazon.com/macie/latest/user/discovery-jobs-create.html).

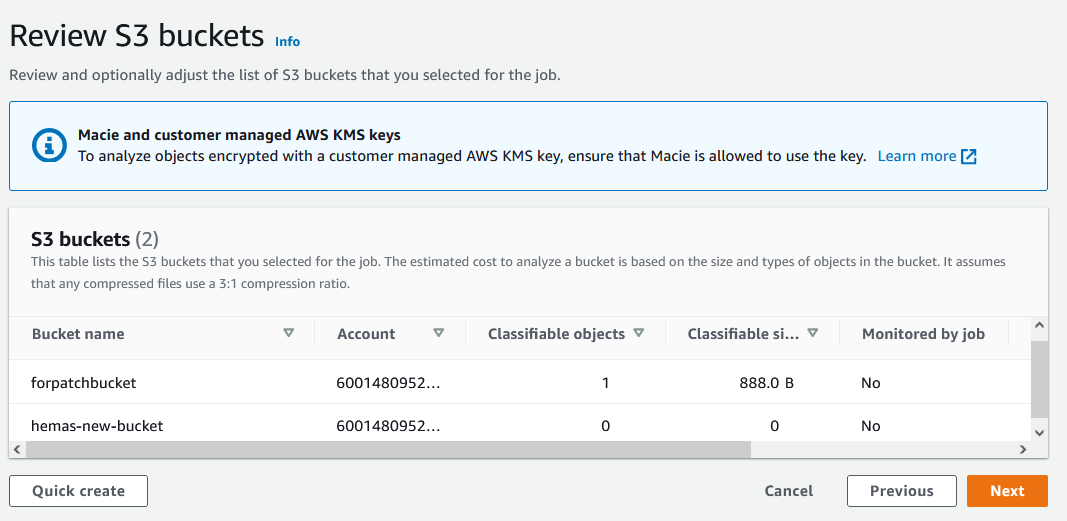
**To create a sensitive data discovery job**

1. Open the Amazon Macie console
2. In the navigation pane, choose **Jobs**.
3. Choose **Create job**.
4. For the **Choose S3 buckets** step, choose **Select specific buckets**.
5. Macie displays a complete inventory of the S3 buckets for your account in the current AWS Region.
6. Select the check box for each bucket that you want the job to analyse.
   1. To find specific buckets more easily, enter filter criteria in the filter bar above the table. You can also sort the inventory by choosing a column heading in the table.
7. When you finish selecting buckets, choose **Next**.
8. For the **Review S3 buckets** step, review and verify your bucket selections. Then choose **Next**.
9. For the **Refine the scope** step, choose **One-time job**, and then choose **Next**.
10. For the **Select managed data identifiers** step, choose **All**, and then choose **Next**.
11. For the **Select custom data identifiers** step, choose **Next**.
12. For the **Select allow lists** step, choose **Next**.
13. For the **Enter general settings** step, enter a name and, optionally, a description of the job. Then choose **Next**.
14. For the **Review and create** step, review the job's configuration settings and verify that they're correct.

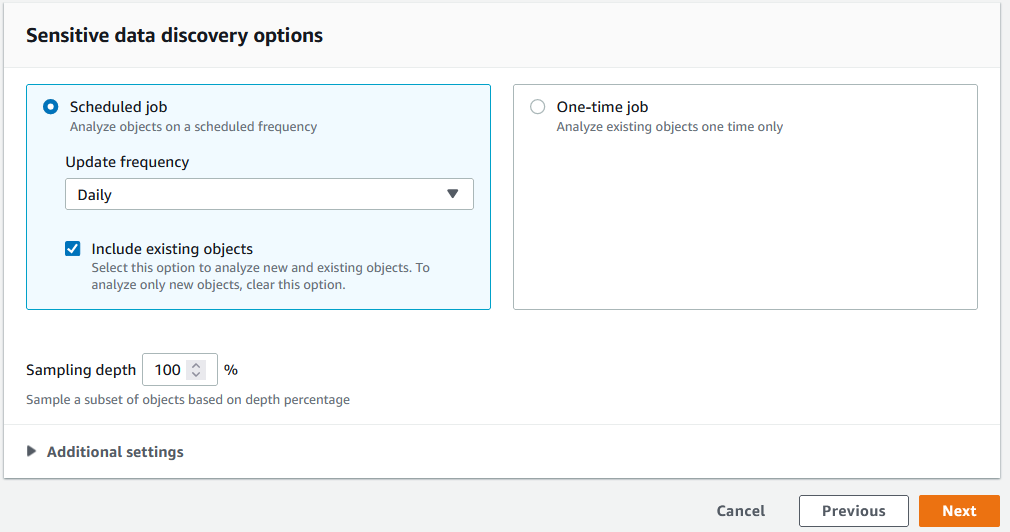
You can also review the total estimated cost (in US Dollars) of running the job. To learn more about this estimate, When you finish reviewing and verifying the job's settings, choose **Submit**.

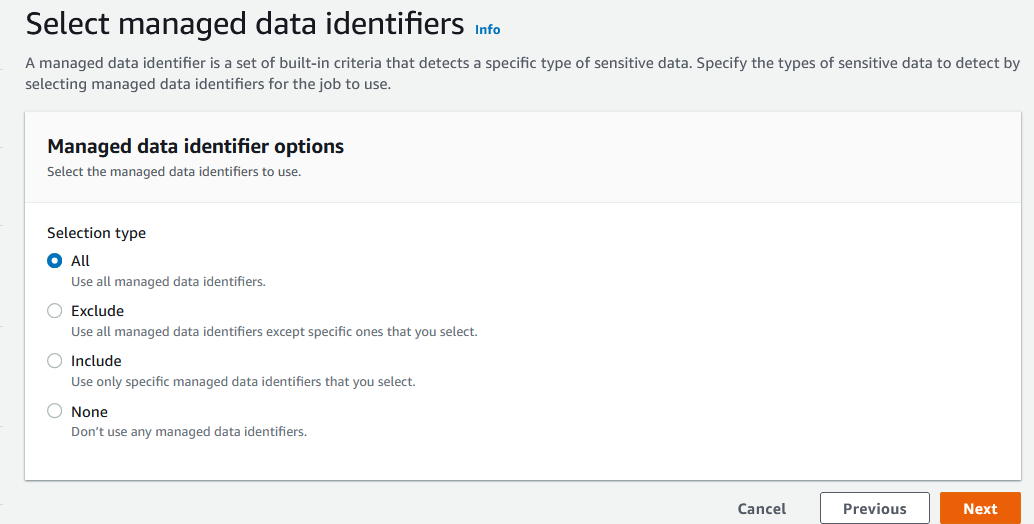
Macie immediately starts running the job. You can then [monitor and check the status of the job](https://docs.aws.amazon.com/macie/latest/user/discovery-jobs-manage.html#discovery-jobs-status-check).

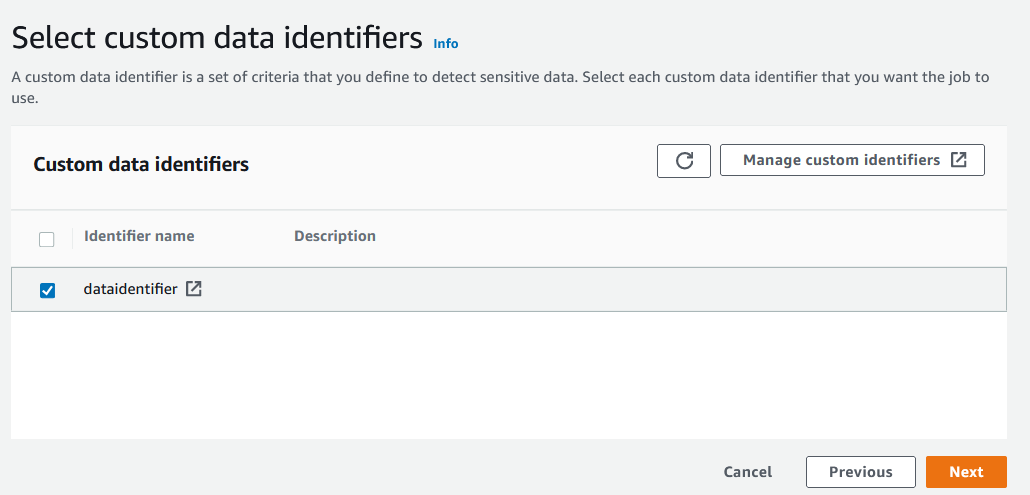


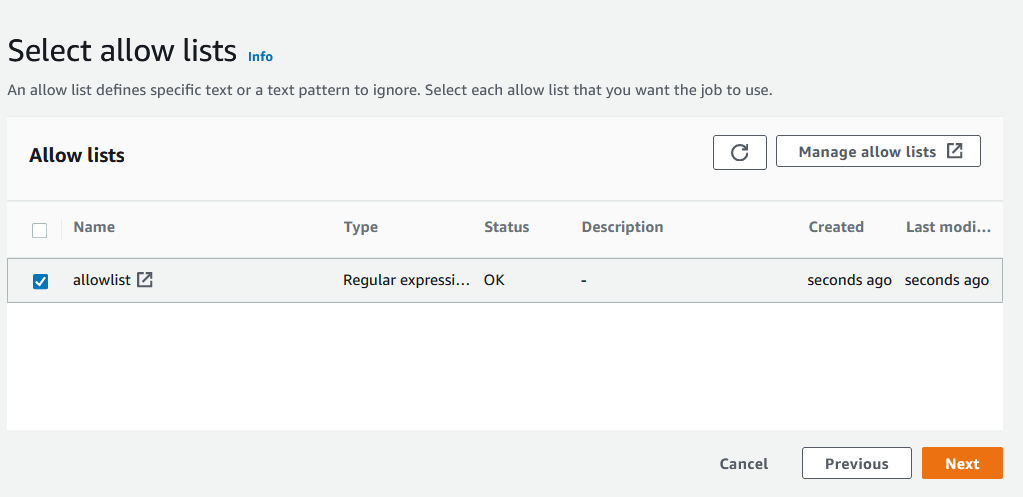


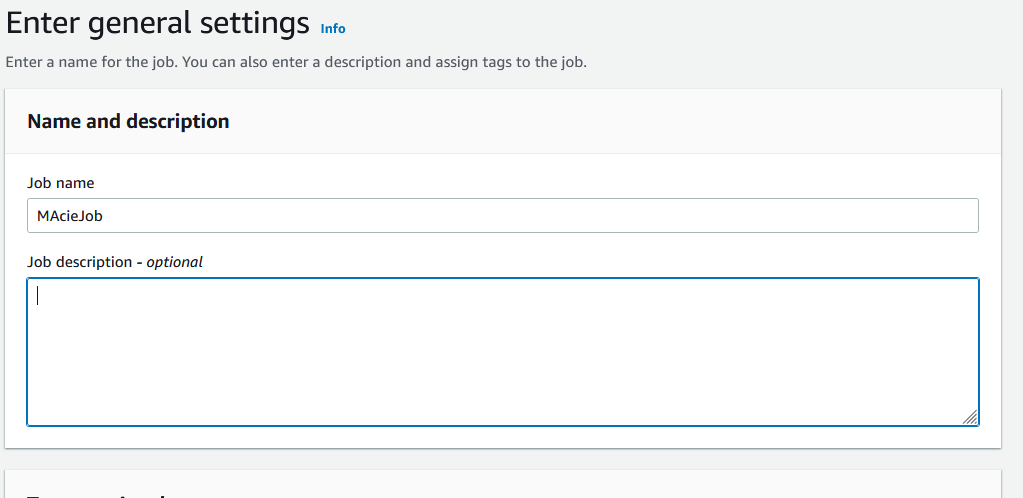
Refine the scope

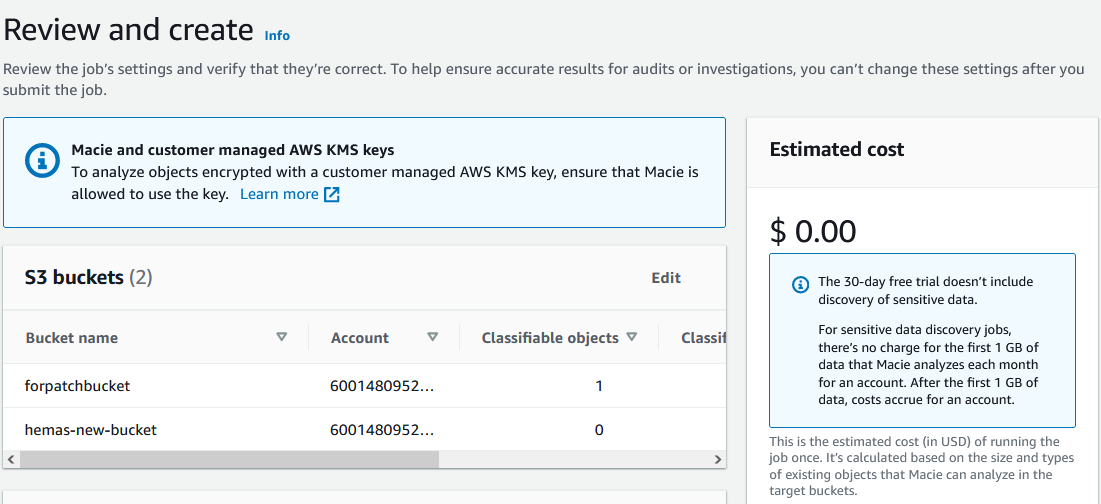


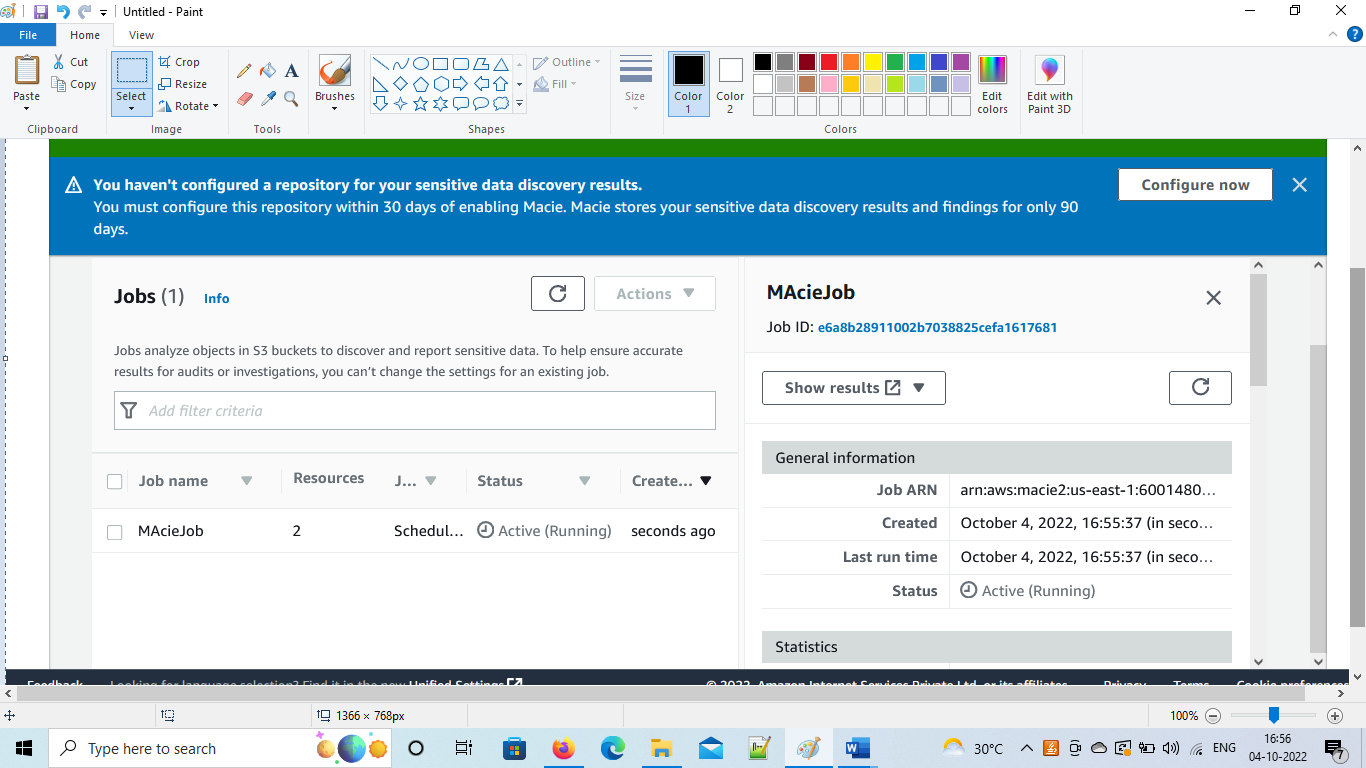


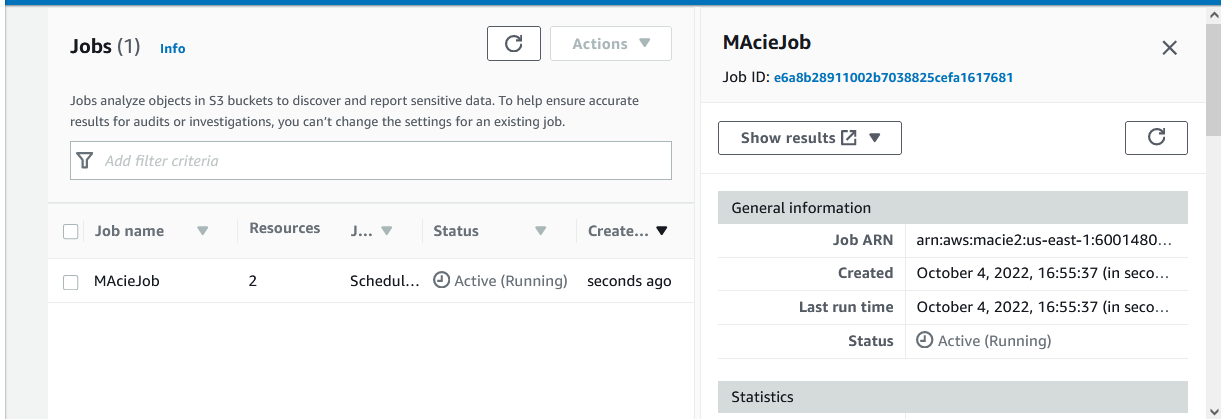












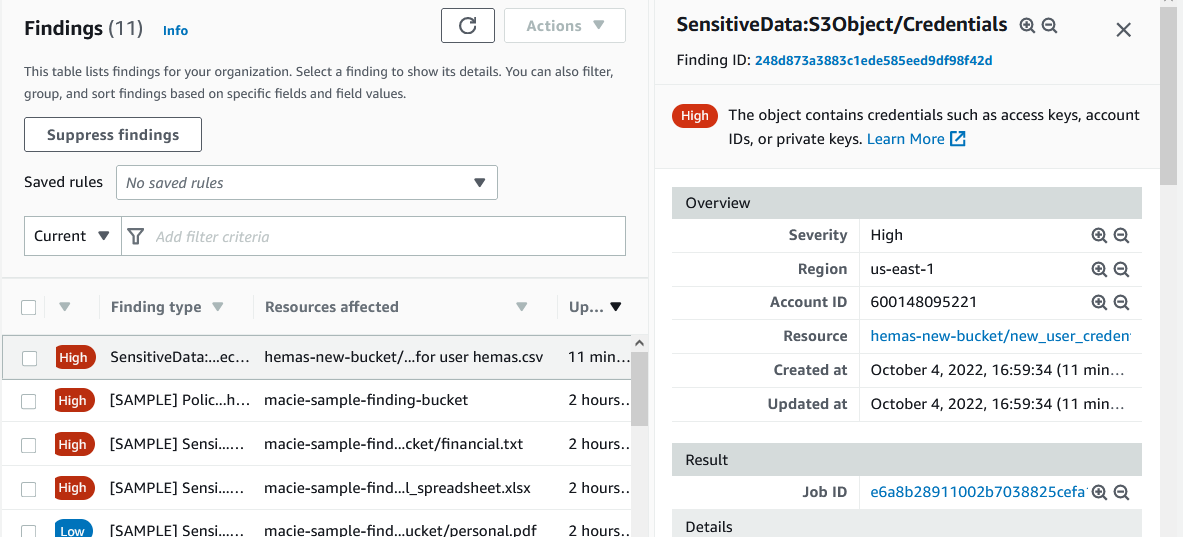
## Step 5: Review your findings

Macie automatically monitors your S3 buckets for security and access control, and it creates policy findings to report potential issues with the security or privacy of your buckets. If you create and run a sensitive data discovery job, Macie also creates sensitive data findings to report sensitive data that it discovers in S3 objects.

Follow these steps to review your findings.

**To review your findings**

* Open the Amazon Macie console
* In the navigation pane, choose **Findings**. The **Findings** page displays current findings for your account in the current AWS Region.
* (Optional) To filter the findings by specific criteria, enter the criteria in the filter bar above the table.
* To review the details of a specific finding, choose any field other than the check box for the finding. The details panel displays information for the finding.



You can disable or suspend Macie in order to avoid getting charged.

**Services Protected by Amazon Macie**

Amazon Simple Storage Service (S3) is the one service protected by Macie.

**How Macie Protects?**

When you enable Amazon Macie for your AWS account, Macie automatically generates and begins maintaining a complete inventory of your Amazon Simple Storage Service (Amazon S3) buckets in the current AWS Region. Macie also begins monitoring and evaluating the buckets for security and access control. If Macie detects an event that reduces the security or privacy of an S3 bucket, Macie creates a [*policy finding*](https://docs.aws.amazon.com/macie/latest/user/findings-types.html#findings-policy-types) for you to review and remediate as necessary.

To also monitor S3 buckets for the presence of sensitive data, you can create and run [*sensitive data discovery jobs*](https://docs.aws.amazon.com/macie/latest/user/discovery-jobs.html) that analyze bucket objects on a daily, weekly, or monthly basis. If you do this and Macie detects sensitive data in an object, Macie creates a[*sensitive data finding*](https://docs.aws.amazon.com/macie/latest/user/findings-types.html#findings-sensitive-data-types) to notify you of the sensitive data that Macie found.

In addition to findings, Macie provides constant visibility into the security and privacy of your Amazon S3 data. To assess the security posture of your data and determine where to take action, you can use the **Summary** dashboard on the console. This dashboard provides a snapshot of aggregated statistics for your Amazon S3 data. The statistics include data for key security metrics such as the number of buckets that are publicly accessible, don’t encrypt new objects by default, or are shared with other AWS accounts. The dashboard also displays groups of aggregated findings data for your account—for example, the names of 1–5 buckets that have the most findings for the preceding seven days. You can drill down on each statistic to view its supporting data. If you prefer to query the statistics programmatically, you can use the [Amazon S3 Data Source Statistics](https://docs.aws.amazon.com/macie/latest/APIReference/datasources-s3-statistics.html) resource of the Amazon Macie API.

For deeper analysis and evaluation, Macie also provides detailed information and statistics for individual buckets in your inventory. This includes breakdowns of each bucket’s public access and encryption settings, and the size and number of objects that Macie can analyze to detect sensitive data in the bucket. The inventory also indicates whether any sensitive data discovery jobs are configured to analyze objects in a bucket and, if so, when one of those jobs most recently ran. You can browse, sort, and filter the inventory by using the Amazon Macie console or the [Amazon S3 Data Source](https://docs.aws.amazon.com/macie/latest/APIReference/datasources-s3.html) resource of the Amazon Macie API.

If you're the Macie administrator for an organization, you can access statistical and other data for S3 buckets that are owned by member accounts in your organization. You can also access policy findings that Macie creates for the buckets, and create sensitive data discovery jobs to detect sensitive data in the buckets. This means that you can use Macie to evaluate and monitor your organization’s security posture across your Amazon S3 environment.

**Advantages**

* Automate sensitive data discovery at scale.
* Gain visibility of your data stored within Amazon Simple Storage Service (S3).
* Receive alerts about unencrypted buckets, publicly accessible buckets, and more.
* Discover proprietary or unique data types.

**Limitations**

* The list can't contain more than 100,000 entries and the storage size of the list can't exceed 35 MB.
* S3 buckets per sensitive data discovery job is 1,000.