User Guide

AWS Artifact



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Artifact: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is AWS Artifact? 1
Pricing 1
Getting started 2
Sign up for an AWS account 2
Features 2
Downloading reports 3
Downloading a report 3
Viewing attachments in PDF documents 4
Securing your documents 5
Troubleshooting 5
Managing agreements 6
Accepting account agreements 6
Terminating account agreements 8
Accepting organization agreements 8
Terminating organization agreements 10
Offline agreements 11
Assurance Assistant 12
Setting up 13
Prerequisites 13
Navigating to Assurance Assistant 13
Submitting questions 14
Single-question mode 14
Uploading a questionnaire (bulk) 14
Reviewing and exporting responses 15
Understanding your responses 15
Response statuses 15
Exporting responses 16
Important information about AI-generated responses 16
Best practices for effective questions 16
Frame questions with the shared responsibility model in mind 16
Make each question self-contained 17
Tips for high-quality responses 17
Additional resources 18
Glossary 18

Configuring notifications 20
Prerequisite 20
Creating a configuration 21
Editing a configuration 22
Deleting a configuration 23
Identity and access management 24
Granting user access 24
Step 1: Create an IAM policy 25
Step 2: Create an IAM group and attach the policy 25
Step 3: Create IAM users and add them to the group 26
Example IAM policies in commercial AWS Regions 26
Example IAM policies in AWS GovCloud (US) Regions 46
Using AWS managed policies 57
AWSArtifactReportsReadOnlyAccess 58
AWSArtifactAgreementsReadOnlyAccess 58
AWSArtifactAgreementsFullAccess 59
AWSArtifactComplianceInquiriesReadOnlyAccess 59
AWSArtifactComplianceInquiriesFullAccess 59
Policy updates 60
Using service-linked roles 62
Service-linked role permissions for AWS Artifact 63
Creating a service-linked role for AWS Artifact 63
Editing a service-linked role for AWS Artifact 64
Deleting a service-linked role for AWS Artifact 64
Supported Regions for AWS Artifact service-linked roles 64
Using IAM condition keys 66
CloudTrail logging 69
AWS Artifact information in CloudTrail 69
Understanding AWS Artifact log file entries 70
Document history 73

What is AWS Artifact?

AWS Artifact provides on-demand downloads of AWS security and compliance documents. For example, reports on compliance with International Organization for Standardization (ISO) standards and Payment Card Industry (PCI) Security Standards, and System and Organization Controls (SOC) reports. AWS Artifact also provides downloads of certifications from accreditation bodies that validate the implementation and operating effectiveness of AWS security controls.

With AWS Artifact, you can also download security and compliance documents for independent software vendors (ISVs) who sell their products on AWS Marketplace. For more information, see AWS Marketplace Vendor Insights.

Additionally, you can use AWS Artifact to review, accept, and track the status of your agreements with AWS for your AWS account and for multiple AWS accounts in your organization. For more information about agreements in AWS Artifact, see Managing agreements in AWS Artifact.

You can also use Assurance Assistant in AWS Artifact to generate AI-powered responses to your compliance and due diligence questions. For more information, see Using Assurance Assistant in AWS Artifact.

To demonstrate the security and compliance of the AWS infrastructure and services that you use, you can submit AWS Artifact documents to your auditors or regulators as *audit artifacts*. You can also use these audit artifacts as guidelines to evaluate your own cloud architecture and to assess the effectiveness of your company's internal controls. For more information about audit artifacts, see AWS Artifact FAQs.

> **Note**
>
> AWS customers are responsible for developing or obtaining documents that demonstrate the security and compliance of their companies. For more information, see Shared Responsibility Model.

Pricing

AWS provides AWS Artifact documents and agreements to you free of charge.

Getting started with AWS Artifact

To get started using AWS Artifact, try out its key features in the AWS Artifact console. In the console, you can download AWS security and compliance reports, download and accept legal agreements, and subscribe to notifications about AWS Artifact documents.

Sign up for an AWS account

To get started with AWS, you need an AWS account. There are two ways to sign up for AWS. If you want complete control over account configuration and where your content is stored, or if you have regulated workloads such as HIPAA or FedRAMP, use Sign up for AWS (advanced). If you are a new user and want to use a login you already own to sign in to AWS and create an AWS environment with preconfigured defaults in select AWS Regions, use Sign up for AWS.

Features

For instructions on using the features of AWS Artifact, see the following topics:

- Downloading reports
- Managing agreements
- Assurance Assistant
- Configuring notifications

Downloading reports in AWS Artifact

You can download reports from the AWS Artifact console. When you download a report from AWS Artifact, the report is generated specifically for you, and every report has a unique watermark. For this reason, you should share the reports only with those you trust. Don't email the reports as attachments, and don't share them online. To share a report, use a secure sharing service. Some reports require you to accept the **Terms and conditions** before you can download them.

Contents

- Downloading a report
- Viewing attachments in PDF documents
- Securing your documents
- Troubleshooting

Downloading a report

To download a report, you must have the required permissions. For more information, see Identity and access management in AWS Artifact.

When you sign up for AWS Artifact, your account is automatically granted permissions to download some reports. If you are having trouble accessing AWS Artifact, follow the guidance on AWS Artifact Service Authorization Reference page.

To download a report

1. Open the AWS Artifact console at https://console.aws.amazon.com/artifact/.
2. On the AWS Artifact home page, choose **View reports**.

   On the **Reports** page, on the **AWS reports** tab, you can access AWS reports (for example, SOC 1/2/3, PCI, C5, and so on). On the **Third-party reports** tab, you can access reports from independent software vendors (ISVs) who sell their products on AWS Marketplace.
3. (Optional) To find a report, enter a keyword in the search field. You can also perform targeted searches for reports based on individual columns, including report title, category, series, and description. For example, to find the Cloud Computing Compliance Controls Catalogue (C5) report, you can search the **Title** column using "Title", the "contains" operator (:), and the term "C5" (**`Title : C5`**).

4. (Optional) For more information about a report, choose the title of the report to open its details page.
5. (Optional) If you want to **download a previous version of a report**, you can open the details page of the report by choosing the report title. On the details page, look for the **Previous versions** section, and in the desired version row, choose **Download** to download that specific version of the report.
6. Select a report, and then choose **Download report**.
7. You might be prompted to accept terms and conditions (**Accept terms to download report**) for the specific report that you're downloading. We recommend that you read the terms and conditions closely. When you're finished reading, select **I have read and agree to the terms**, and then choose **Accept terms and download report**.
8. Open the downloaded file via a PDF viewer. Review the terms and conditions for acceptance and scroll down to find the audit report. Reports could have additional information embedded as attachments within the PDF document, so make sure to check for attachments within the PDF file for supporting documentation. For instructions on how to view attachments, see Viewing attachments in PDF documents.

Viewing attachments in PDF documents

We recommend the following applications that currently support viewing PDF attachments:

Adobe Acrobat Reader

Download the latest version of Adobe Acrobat Reader from the Adobe website at https://get.adobe.com/reader/.

For instructions on how to view PDF attachments in Acrobat Reader, see Links and attachments in PDFs on the Adobe Support website.

Firefox Browser

1. Download the latest Firefox web browser from the Mozilla website at https://www.mozilla.org/en-US/firefox/new/.
2. Open the PDF file in Firefox's built-in PDF viewer. For instructions, see View PDF files in Firefox or choose another viewer on the Mozilla Support website.
3. To view PDF attachments in Firefox's built-in PDF viewer, choose **Toggle Sidebar**, **Show Attachments**.

Securing your documents

AWS Artifact documents are confidential and should be kept secure at all times. AWS Artifact uses the AWS shared responsibility model for its documents. This means that AWS is responsible for keeping documents secure while they are in the AWS Cloud, but you are responsible for keeping them secure after you download them. AWS Artifact might require you to accept the **Terms and conditions** before you can download documents. Each document download has a unique, traceable watermark.

You are only permitted to share documents marked as confidential within your company, with your regulators, and with your auditors. You aren't permitted to share these documents with your customers or on your website. We strongly recommend that you use a secure document sharing service to share documents with others. Do not send the documents through email or upload them to a site that is not secure.

Troubleshooting

If you cannot download a document or receive an error message, see Troubleshooting in the AWS Artifact FAQ.

Managing agreements in AWS Artifact

You can use AWS Artifact to review and manage agreements for your AWS account or organization. For example, companies that are subject to the Health Insurance Portability and Accountability Act (HIPAA) typically require a Business Associate Addendum (BAA) agreement with AWS to ensure that protected health information (PHI) is appropriately safeguarded. In the AWS Artifact console, you can review and accept such agreements, and you can designate an AWS account that can legally process PHI.

If you use AWS Organizations, you can accept agreements, such as a BAA with AWS, on behalf of all AWS accounts in your organization. All existing and subsequent member accounts are automatically covered by the agreement and can legally process PHI.

You can also use AWS Artifact to confirm that your AWS account or organization has accepted an agreement, and to review the terms of an accepted agreement to understand your obligations. If your account or organization no longer needs to use an accepted agreement, then you can use AWS Artifact to terminate the agreement. If you terminate the agreement but later realize that you need it, then you can activate the agreement again.

Contents

- Accepting agreements for your AWS account in AWS Artifact
- Terminating agreements for your AWS account in AWS Artifact
- Accepting agreements for your organization in AWS Artifact
- Terminating agreements for your organization in AWS Artifact
- Offline agreements in AWS Artifact

Accepting agreements for your AWS account in AWS Artifact

You can use the AWS Artifact console to review and accept agreements with AWS for your AWS account.

> **Important**
>
> Before you accept an agreement, we recommend that you consult with your legal, privacy, and compliance team.

Required permissions

If you're an administrator of an account, then you can grant IAM users and federated users with the permissions to access and manage one or more of your agreements. By default, only users with administrative privileges can accept an agreement. To accept an agreement, IAM and federated users must have the required permissions.

For more information, see Identity and access management in AWS Artifact.

To accept an agreement with AWS

1. Open the AWS Artifact console at https://console.aws.amazon.com/artifact/.
2. On the AWS Artifact navigation pane, choose **Agreements**.
3. On the **Agreements** page, do either of the following:
   - To accept an agreement only for your account, choose the **Account agreements** tab.
   - To accept an agreement on behalf of your organization, choose the **Organization agreements** tab.
4. Select an agreement, and then choose **Download agreement**.

   The **Accept NDA to download report** dialog box appears.
5. Before you can download the agreement that you selected, you must first accept the terms of the AWS Artifact Nondisclosure Agreement (AWS Artifact NDA).

   a. In the **Accept NDA to download report** dialog box, review the AWS Artifact NDA.

   b. (Optional) To print a copy of the AWS Artifact NDA (or to save it as a PDF), choose **Print NDA**.

   c. Select **I have read and agree to all the terms of the NDA.**

   d. To accept the AWS Artifact NDA and to download a PDF of the agreement that you selected, choose **Accept NDA and download**.
6. In a PDF viewer, review the agreement PDF that you downloaded.
7. In the AWS Artifact console, with the agreement selected, choose **Accept agreement**.
8. In the **Accept agreement** dialog box, do the following:

   a. Review the agreement.

   b. Select **I agree to all of these terms and conditions**.

   c. Choose **Accept agreement**.

9. Choose **Accept** to accept the agreement for your account.

Terminating agreements for your AWS account in AWS Artifact

If you used the AWS Artifact console to accept an agreement for a single AWS account, then you can use the console to terminate that agreement. Otherwise, see Offline agreements in AWS Artifact.

Required permissions

To terminate an agreement, IAM and federated users must have the required permissions.

For more information, see Identity and access management in AWS Artifact.

To terminate your online agreement with AWS

1. Open the AWS Artifact console at https://console.aws.amazon.com/artifact/.
2. On the AWS Artifact navigation pane, choose **Agreements**.
3. Choose the **Account agreements** tab.
4. Select the agreement and choose **Terminate agreement**.
5. Select all checkboxes to indicate that you agree to terminate the agreement.
6. Choose **Terminate**. When prompted for confirmation, choose **Terminate**.

Accepting agreements for your organization in AWS Artifact

If you're the owner of the management account of an AWS Organizations organization, then you can accept an agreement with AWS on behalf of all AWS accounts in your organization.

> **Important**
>
> Before you accept an agreement, we recommend that you consult with your legal, privacy, and compliance team.

AWS Organizations has two available feature sets: *consolidated billing features* and *all features*. To use AWS Artifact for your organization, the organization that you belong to must be enabled for all

features. If your organization is configured only for consolidated billing, see Enabling all features in your organization in the *AWS Organizations User Guide*.

To accept or terminate organization agreements, you must be signed in to the management account with the correct AWS Artifact permissions. Users of member accounts that have `organizations:DescribeOrganization` permissions can view the organization agreements that are accepted on their behalf.

For more information, see Managing accounts in an organization with AWS Organizations in the *AWS Organizations User Guide*.

Required permissions

To accept an agreement, the owner of the management account must have the required permissions.

For more information, see Identity and access management in AWS Artifact.

To accept an agreement for an organization

1. Open the AWS Artifact console at https://console.aws.amazon.com/artifact/.
2. On the AWS Artifact dashboard, choose **Agreements**.
3. Choose the **Organization agreements** tab.
4. On the **Agreements** page, do either of the following:
   - To accept an agreement only for your account, choose the **Account agreements** tab.
   - To accept an agreement on behalf of your organization, choose the **Organization agreements** tab.
5. Select an agreement, and then choose **Download agreement**.

   The **Accept NDA to download report** dialog box appears.
6. Before you can download the agreement that you selected, you must first accept the terms of the AWS Artifact Nondisclosure Agreement (AWS Artifact NDA).

   a. In the **Accept NDA to download report** dialog box, review the AWS Artifact NDA.

   b. (Optional) To print a copy of the AWS Artifact NDA (or to save it as a PDF), choose **Print NDA**.

   c. Select **I have read and agree to all the terms of the NDA.**

d. To accept the AWS Artifact NDA and to download a PDF of the agreement that you selected, choose **Accept NDA and download**.

7. In a PDF viewer, review the agreement PDF that you downloaded.
8. In the AWS Artifact console, with the agreement selected, choose **Accept agreement**.
9. In the **Accept agreement** dialog box, do the following:

   a. Review the agreement.

   b. Select **I agree to all of these terms and conditions**.

   c. Choose **Accept agreement**.

10. Choose **Accept** to accept the agreement for all existing and future accounts in your organization.

Terminating agreements for your organization in AWS Artifact

If you used the AWS Artifact console to accept an agreement on behalf of all member accounts in an organization in AWS Organizations, then you can use the console to terminate that agreement. Otherwise, see Offline agreements in AWS Artifact.

If a member account is removed from an organization, then that member account is longer covered by organization agreements. Before removing member accounts from an organization, a management account administrator should communicate this to member accounts so that they can put new agreements in place if necessary. You can view a list of active organization agreements in the AWS Artifact console on the **Agreements** page, under Organization agreements.

For more information about AWS Organizations, see Managing accounts in an organization with AWS Organizations in the *AWS Organizations User Guide*.

Required permissions

To terminate an agreement, the owner of the management account must have the required permissions.

For more information, see Identity and access management in AWS Artifact.

To terminate your online organization agreement with AWS

1. Open the AWS Artifact console at https://console.aws.amazon.com/artifact/.

2. On the AWS Artifact dashboard, choose **Agreements**.
3. Choose the **Organization agreements** tab.
4. Select the agreement and choose **Terminate agreement**.
5. Select all checkboxes to indicate that you agree to terminate the agreement.
6. Choose **Terminate**. When prompted for confirmation, choose **Terminate**.

Offline agreements in AWS Artifact

If you have an existing offline agreement, AWS Artifact displays the agreements that you accepted offline. For example, the console might display the **Offline Business Associate Addendum (BAA)** with an **Active** status. The active status indicates that the agreement was accepted. To terminate an offline agreement, see the termination guidelines and instructions that are included in your agreement.

For more information, see Identity and access management in AWS Artifact.

Using Assurance Assistant in AWS Artifact

What Is Assurance Assistant?

Assurance Assistant is an AI-powered capability within AWS Artifact that generates citation-backed responses to compliance and due diligence questions about AWS services and security controls. It helps you accelerate vendor assessments, security reviews, and compliance questionnaire completion by providing substantive, sourced answers in minutes rather than weeks.

Assurance Assistant works by mapping your question to AWS security controls, searching across verified AWS compliance documentation, and returning a response with citations from the source documents. Citations let you independently review the source materials and build confidence in the information provided.

Who Can Benefit

Assurance Assistant is designed for anyone involved in compliance assessments or security reviews related to AWS, including:

- Third-party risk managers and compliance officers
- Security engineers and IT consultants
- Auditors and legal teams conducting vendor due diligence
- Teams responding to customer questionnaires about AWS security posture

Supported Questionnaire Formats

Assurance Assistant is optimized for industry-standard due diligence formats, including:

- Consensus Assessments Initiative Questionnaire (CAIQ)
- Standardized Information Gathering questionnaire (SIG)
- Custom due diligence questionnaires (DDQs) in CSV (comma-separated values), XLSX, Word (.docx), and PDF format

Assurance Assistant addresses questions about AWS's security controls, compliance posture, and operational practices. Assurance Assistant might not respond to questions that are incomplete, not compliance-related, or contain inappropriate content. Questions about customer-side implementation are outside its scope.

> **Note**
>
> Assurance Assistant is available at no additional charge through the AWS Artifact console.

Contents

- Setting up
- Submitting questions
- Reviewing and exporting responses
- Best practices for effective questions
- Glossary

Setting up

Prerequisites

To use Assurance Assistant, attach one of the following AWS IAM managed policies to your AWS account:

IAM managed policies for Assurance Assistant

IAM policy	What it allows
`AWSArtifactComplianceInquiriesReadOnlyAccess`	View responses and export results
`AWSArtifactComplianceInquiriesFullAccess`	Submit questions, review responses, and export results

For instructions on attaching managed policies, see Granting user access to AWS Artifact.

Navigating to Assurance Assistant

In the AWS Artifact console homepage, choose **Assurance Assistant** in the left navigation panel.

Submitting questions

Assurance Assistant offers two modes for submitting questions: single-question mode for immediate, on-the-spot answers, and questionnaire upload mode for processing multiple questions in bulk.

Single-question mode

Use single-question mode to get an instant, cited answer to one compliance question at a time.

To submit a single question using Assurance Assistant

1. In the AWS Artifact console, choose **Assurance Assistant** in the navigation pane.
2. If this is your first time using Assurance Assistant, enter your question directly in the text field. Otherwise choose **Ask question**, then enter your question in the text field. Questions can be up to 2,048 characters in English.
3. Choose **Submit**. Your response appears with citations referencing the source documents used.
4. Choose the copy button to copy the response to your clipboard.

Uploading a questionnaire (bulk)

Use questionnaire upload mode to submit an entire questionnaire at once. This mode is well-suited for CAIQ, SIG, and custom DDQ files.

To upload a questionnaire using Assurance Assistant

1. Navigate to **Assurance Assistant**.
2. If this is your first time using Assurance Assistant, the upload option is available directly. Otherwise, choose **Ask question** to access the submission interface.
3. Choose **Choose file** and select your questionnaire. Supported formats: CSV (comma-separated values), Excel spreadsheet (XLSX), Word (.docx), PDF, maximum 5 MB, up to 1,000 questions.
4. (Optional) Add tags as key-value pairs to help organize questionnaires and manage access.
5. Choose **Submit**.
6. For Excel file upload, Assurance Assistant takes you to the **Configure responses** page. Select the tabs that you want to process, then choose **Configure**. For CSV, Word (.docx), and PDF files, this step is skipped and processing begins directly.

7. Processing begins immediately. Assurance Assistant takes you to the details page where you can monitor the status of your questionnaire.
8. To receive a notification when processing is complete, configure a notification under **Compliance Inquiries** by selecting the **Compliance inquiry updates** checkbox. For instructions, see Configuring email notifications in AWS Artifact.
9. You can also monitor the status of your questionnaire from the Assurance Assistant landing page.

> **Note**
>
> You can submit questions in either mode at any time. For compliance questionnaires with many related questions, bulk upload is the recommended approach.

Reviewing and exporting responses

Understanding your responses

On the Assurance Assistant landing page, you can see all submitted questionnaires. Select a questionnaire to review individual responses. Each response includes an AI-generated answer grounded in verified AWS compliance documentation, along with citations from the source documents used.

Response statuses

Each question in your questionnaire has one of the following statuses:

Status	What it means	Recommended action
Generating a response	Assurance Assistant is generating a response.	N/A
Auto-generated	Assurance Assistant generated a response, and it's available for review.	Review the response and citations. Use the export options to include in your questionnaire file.

Exporting responses

After responses are ready, you have two export options:

- **Export selected** – Choose specific questions and download only those responses as a spreadsheet.
- **Export all** – Download all responses for the questionnaire as a spreadsheet.

For either option, you can choose to include source citations in the export.

> **Note**
>
> If you need additional information beyond what Assurance Assistant provides, AWS compliance documentation is available through the AWS Artifact console and at aws.amazon.com/compliance.

Important information about AI-generated responses

Assurance Assistant responses are generated using AI and grounded in verified, publicly available AWS compliance documentation, including AWS SOC reports, ISO certifications, and other published materials.

Responses include citations so you can independently review and verify information against the original source documents. As with any AI-generated content, review responses in the context of your specific requirements before relying on them for official purposes.

Responses reflect AWS compliance documentation available at the time of generation.

Best practices for effective questions

Well-formed questions produce the most relevant and complete responses. The guidance below helps you get the most value from Assurance Assistant.

Frame questions with the shared responsibility model in mind

AWS operates under a Shared Responsibility Model: AWS is responsible for security *of* the cloud; customers are responsible for security *in* the cloud.

Frame your questions to clearly distinguish what you are asking about AWS's responsibilities versus your own responsibilities as a customer. Assurance Assistant addresses what AWS does – its security controls, compliance posture, and operational practices. Questions about customer-side implementation are outside its scope.

Interpret responses with the same lens: a response describes what AWS does and is responsible for. Your organization remains responsible for the controls you implement on top of AWS services.

Make each question self-contained

Assurance Assistant treats each question independently. To ensure you receive the most complete and accurate response:

- Make each question **atomic and complete** – include all context needed for a full, standalone answer within the question itself.
- Do not rely on context from previous or subsequent questions. There is no carry-over of information between questions.
- Include the relevant AWS service name, compliance framework, or specific control area directly in the question.

Tips for high-quality responses

- **Be specific and include relevant context** – Name the AWS service, security control, or compliance standard. For example: "How does Amazon S3 encrypt data at rest?" rather than "How is data encrypted?"
- **Ask one clear question at a time** – Avoid compound or multi-part questions within a single submission.
- **Use industry-standard terminology** – Where possible, align your phrasing with common compliance vocabulary to improve matching.
- **For bulk uploads** – Ensure each question is complete and clearly articulated. In CSV and XLSX files, use one question per row; in Word or PDF files, present each question as a distinct, clearly delineated item.

Additional resources

The following resources provide additional context and support for using AWS Artifact and related compliance tools:

- AWS Artifact console – Access Assurance Assistant and all AWS Artifact features.
- What is AWS Artifact? – Overview of the AWS Artifact service.
- AWS Shared Responsibility Model – Understand the division of responsibilities between AWS and customers.
- AWS Compliance Programs – Browse the full list of AWS compliance certifications and attestations.
- AWS Services in Scope by Compliance Program – Check which AWS services are in scope for specific compliance programs.
- AWS Support – Contact AWS for additional support through your existing support plan.

Glossary

Term	Definition
DDQ	Due Diligence Questionnaire – a structured set of questions used in vendor assessments and security reviews to evaluate an organization's security and compliance posture.
CAIQ	Consensus Assessments Initiative Questionnaire – a standardized due diligence questionnaire published by the Cloud Security Alliance (CSA).
SIG	Standardized Information Gathering questionnaire – a widely used due diligence questionnaire format for assessing third-party vendors.
SOC	System and Organization Controls – a set of audit report types (SOC 1, SOC 2, SOC 3) that evaluate service organizations' controls.
ISO	International Organization for Standardization – a globally recognize d body that publishes standards, including ISO 27001 for information security management.

Term	Definition
Citation	A reference to a specific statement in a verified AWS compliance document that supports an AI-generated response, allowing independent verification.
IAM	AWS Identity and Access Management – the service used to manage permissions and access to AWS resources, including AWS Artifact features.
Compliance inquiry	A record in Assurance Assistant that contains a submitted question or questionnaire and the AI-generated responses.

Configuring email notifications in AWS Artifact

> **Note**
>
> The content of this page is only applicable to commercial AWS Regions, and does not currently apply to AWS GovCloud (US) Regions.

You can use the AWS Artifact console to configure email notifications for updates on agreements and reports in AWS Artifact. AWS Artifact sends these email notifications using AWS User Notifications. To receive AWS Artifact email notifications, you must first select AWS User Notifications notification hubs in the User Notifications console. Then, in the AWS Artifact console, you can create a configuration for notification settings, in which you specify your notification recipients and which notifications they receive.

To configure AWS Artifact email notifications, you must have the required permissions for AWS Artifact and AWS User Notifications. For more information, see Identity and access management in AWS Artifact.

Contents

- Prerequisite: Select notification hubs in User Notifications
- Creating a configuration for AWS Artifact notification settings
- Editing a configuration for AWS Artifact notification settings
- Deleting a configuration for AWS Artifact notification settings

Prerequisite: Select notification hubs in User Notifications

Before you can receive AWS Artifact email notifications, you must first open the User Notifications console and select the notification hubs in the AWS Regions where you want to store your User Notifications data. Selecting notification hubs is required for AWS User Notifications, which AWS Artifact uses to send notifications.

To select notification hubs

1. Open the Notification hubs page of the AWS User Notifications console.

2. Select the notification hubs in the AWS Regions where you want to store your AWS User Notifications resources. By default, your User Notifications data is stored in the US East (N. Virginia) Region. User Notifications replicates your notifications data across the other Regions that you select. For more information, see the notification hubs documentation in the *AWS User Notifications User Guide*.
3. Choose **Save and continue**.

Creating a configuration for AWS Artifact notification settings

> **Note**
>
> The content of this page is only applicable to commercial AWS Regions, and does not currently apply to AWS GovCloud (US) Regions.

After you select your User Notifications notification hubs, you can create a configuration for notification settings in the AWS Artifact console. In the configuration that you create, you specify the recipient email addresses that you want to receive AWS Artifact notifications. You also specify which updates those recipients should receive notifications about, such as updates for AWS Artifact agreements, and updates for all (or a subset of) AWS Artifact reports.

To create a configuration

1. Open the Notification settings page of the AWS Artifact console.
2. Choose **Create configuration**.
3. On the **Create configuration** page, do the following:
   - To receive notifications for agreements, under **Agreements**, keep **Updates on AWS Agreements** selected.
   - To receive notifications for reports, under **Reports**, keep **Updates on AWS Reports** selected.
     a. To receive notifications for all reports, choose **All reports**.
     b. To receive notifications only for reports under specific categories and series, choose **A subset of reports**. Then, select the categories and series that you're interested in.
   - Under **Configuration name**, enter a **Name** for your configuration.

- Under **Email**, for **Recipients**, enter a comma-separated list of email addresses that you want to receive AWS Artifact notification emails.
- (Optional) To add tags to the notification configuration, expand **Tags**, choose **Add new tag**, and then enter tags as key-value pairs. For more information about tagging User Notifications resources, see Tagging your AWS User Notifications resources in the *AWS User Notifications User Guide*.
- Choose **Create configuration**.

  User Notifications sends a verification email to each of the recipient email addresses that you provided. To verify the email address, in the verification email, the recipient must choose **Verify email**. Only verified email addresses will receive AWS Artifact notifications.

Editing a configuration for AWS Artifact notification settings

> **Note**
>
> The content of this page is only applicable to commercial AWS Regions, and does not currently apply to AWS GovCloud (US) Regions.

After you create a configuration for AWS Artifact notification settings, you can edit the configuration at any time to change your notification settings. For example, to add or remove recipients, change what types of notifications they receive, and add or remove tags.

To edit a configuration

1. Open the Notification settings page of the AWS Artifact console.
2. Select the configuration that you want to edit.
3. Choose **Edit**.
4. Edit any of the configuration selections and fields. When you're done, choose **Save changes**.

   If you've added new email addresses as notification recipients, then AWS User Notifications sends a verification email those email addresses. To verify the email address, in the verification email, the recipient must choose **Verify email**. Only verified email addresses will receive AWS Artifact notifications.

Deleting a configuration for AWS Artifact notification settings

> **Note**
>
> The content of this page is only applicable to commercial AWS Regions, and does not currently apply to AWS GovCloud (US) Regions.

If you no longer need a configuration that you created for AWS Artifact notification settings, then you can delete the configuration in the AWS Artifact console.

To delete a configuration

1. Open the Notification settings page of the AWS Artifact console.
2. Select the configuration that you want to delete.
3. Choose **Delete**.
4. In the **Delete configuration** dialog box, choose **Delete**.

Identity and access management in AWS Artifact

When you sign up for AWS, you provide an email address and password that are associated with your AWS account. These are your *root credentials*, and they provide complete access to all of your AWS resources, including resources for AWS Artifact. However, we strongly recommend that you don't use the root account for everyday access. We also recommend that you don't share account credentials with others to give them complete access to your account.

Instead of signing in to your AWS account with root credentials or sharing your credentials with others, you should create a special user identity called an *IAM user* for yourself and for anyone who might need access to a document or agreement in AWS Artifact. With this approach, you can provide individual sign-in information for each user, and you can grant each user only the permissions that they need to work with specific documents. You can also grant multiple IAM users the same permissions by granting the permissions to an IAM group and adding the IAM users to the group.

If you already manage user identities outside AWS, you can use IAM *identity providers* instead of creating IAM users. For more information, see Identity providers and federation in the *IAM User Guide*.

Contents

- Granting user access to AWS Artifact
- Example IAM policies for AWS Artifact in commercial AWS Regions
- Example IAM policies for AWS Artifact in AWS GovCloud (US) Regions
- Using AWS managed policies for AWS Artifact
- Using service-linked roles for AWS Artifact
- Using IAM condition keys for AWS Artifact reports

Granting user access to AWS Artifact

Complete the following steps to grant users permissions to AWS Artifact based on the level of access they need.

Tasks

- Step 1: Create an IAM policy

- Step 2: Create an IAM group and attach the policy
- Step 3: Create IAM users and add them to the group

Step 1: Create an IAM policy

As an IAM administrator, you can create a policy that grants permissions to AWS Artifact actions and resources.

To create an IAM policy

Use the following procedure to create an IAM policy that you can use to grant permissions to your IAM users and groups.

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Policies**.
3. Choose **Create policy**.
4. Choose the **JSON** tab.
5. Enter a policy document. You can create you own policy, or you can use one of the policies from Example IAM policies for AWS Artifact in commercial AWS Regions.
6. Choose **Review Policy**. The policy validator reports any syntax errors.
7. On the **Review policy** page, enter a unique name that helps you remember the purpose of the policy. You can also provide a description.
8. Choose **Create policy**.

Step 2: Create an IAM group and attach the policy

As an IAM administrator, you can create a group and attach the policy that you created to the group. You can add IAM users to the group at any time.

To create an IAM group and attach your policy

1. In the navigation pane, choose **Groups** and then choose **Create New Group**.
2. For **Group Name**, enter a name for your group and then choose **Next Step**.
3. In the search field, enter the name of the policy that you created. Select the check box for your policy and then choose **Next Step**.
4. Review the group name and policies. When you are ready, choose **Create Group**.

Step 3: Create IAM users and add them to the group

As an IAM administrator, you can add users to a group at any time. This grants the users the permissions granted to the group.

To create an IAM user and add the user to a group

1. In the navigation pane, choose **Users** and then choose **Add user**.
2. For **User name**, enter the names for one or more users.
3. Select the check box next to **AWS Management Console access**. Configure an auto-generated or custom password. You can optionally select **User must create a new password at next sign-in** to require a password reset when the user first signs in.
4. Choose **Next: Permissions**.
5. Choose **Add user to group** and then select the group that you created.
6. Choose **Next: Tags**. You can optionally add tags to your users.
7. Choose **Next: Review**. When you are ready, choose **Create user**.

Example IAM policies for AWS Artifact in commercial AWS Regions

You can create permissions policies that grant permissions to IAM users. You can grant users access to AWS Artifact reports and the ability to accept and download agreements on behalf of either a single account or an organization.

The following example policies show permissions that you can assign to IAM users based on the level of access that they need.

These policies are applicable in commercial AWS Regions. For policies applicable to AWS GovCloud (US) Regions, see Example IAM policies for AWS Artifact in AWS GovCloud (US) Regions

- Example policies to manage AWS reports with fine-grained permissions
- Example policies to manage third-party reports
- Example policies to manage agreements
- Example policies to integrate with AWS Organizations
- Example policies to manage agreements for the management account

- Example policies to manage organizational agreements
- Example policies to manage compliance inquiries
- Example policies to manage notifications

Example policies to manage AWS reports through fine-grained permissions

> **Tip**
>
> You should consider using the AWSArtifactReportsReadOnlyAccess managed policy instead of defining your own policy.

The following policy grants permission to download all AWS reports through fine-grained permissions.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permission to download only the AWS SOC, PCI, and ISO reports through fine-grained permissions.

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example policies to manage third-party reports

> **Tip**
>
> You should consider using the AWSArtifactReportsReadOnlyAccess managed policy instead of defining your own policy.

Third-party reports are denoted by the IAM resource `report`.

The following policy grants permission to all third-party report functionality.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permission to download third-party reports.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permission to list third-party reports.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permission to view a third-party report's details for all versions.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

The following policy grants permission to view a third-party report's details for a specific version.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

Tip

You should consider using the AWSArtifactAgreementsReadOnlyAccess or AWSArtifactAgreementsFullAccess managed policy instead of defining your own policy.

Example policies to manage agreements

The following policy grants permission to download all agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
```

```
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

The following policy grants permission to accept all agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

The following policy grants permission to terminate all agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

The following policy grants permissions to view and execute account level agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example policies to integrate with AWS Organizations

The following policy grants permission to create the IAM role that AWS Artifact uses to integrate with AWS Organizations. Your organization's management account must have these permissions to get started with organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
```

```
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

The following policy grants permission to grant AWS Artifact the permissions to use AWS Organizations. Your organization's management account must have these permissions to get started with organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   },
   {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
```

```
      }
    }
 ]
}
```

Example policies to manage agreements for the management account

The following policy grants permissions to manage agreements for the management account.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
```

```
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
  ]
}
```

Example policies to manage organizational agreements

The following policy grants permissions to manage organizational agreements. Another user with the required permissions must set up the organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

The following policy grants permissions to view organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

Example policies to manage compliance inquiries

> **Tip**
>
> We recommend using the AWSArtifactComplianceInquiriesReadOnlyAccess or AWSArtifactComplianceInquiriesFullAccess managed policy instead of defining your own policy.

The following policy grants read-only permission to list, view, export compliance inquiries, and list tags for compliance inquiry resources.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListComplianceInquiries",
      "Effect": "Allow",
      "Action": [
        "artifact:ListComplianceInquiries"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAndExportComplianceInquiries",
      "Effect": "Allow",
      "Action": [
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ListComplianceInquiryQueries",
        "artifact:ExportComplianceInquiry",
        "artifact:ListTagsForResource"
      ],
      "Resource": "arn:aws:artifact:*:*:compliance-inquiry/*"
    }
```

```
  ]
}
```

The following policy grants full permission to create, list, view, export compliance inquiries, and manage tags for compliance inquiry resources. It also grants permission to list the existing AWS User Notifications notification configurations that you can select when you create an inquiry. In addition, it grants permission to read each configuration's delivery channels, event rules, and email contacts.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAndCreateComplianceInquiries",
      "Effect": "Allow",
      "Action": [
        "artifact:ListComplianceInquiries",
        "artifact:CreateComplianceInquiry"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewExportAndTagComplianceInquiries",
      "Effect": "Allow",
      "Action": [
        "artifact:GetComplianceInquiryMetadata",
        "artifact:ListComplianceInquiryQueries",
        "artifact:ExportComplianceInquiry",
        "artifact:TagResource",
        "artifact:UntagResource",
        "artifact:ListTagsForResource"
      ],
      "Resource": "arn:aws:artifact:*:*:compliance-inquiry/*"
    },
    {
      "Sid": "NotificationConfigurationListActions",
      "Effect": "Allow",
      "Action": [
        "notifications:ListNotificationConfigurations",
        "notifications:ListChannels",
        "notifications:ListEventRules"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "NotificationConfigurationContactReadActions",
      "Effect": "Allow",
      "Action": [
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": "*"
    }
  ]
}
```

Example policies to manage notifications

The following policy grants complete permissions to use AWS Artifact notifications.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
```

```
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to list all configurations.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to create a configuration.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to edit a configuration.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
```

```
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to delete a configuration.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to view details of a configuration.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to register or deregister notification hubs.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example IAM policies for AWS Artifact in AWS GovCloud (US) Regions

These policies are ONLY applicable in AWS GovCloud (US) Regions. For policies applicable to commercial AWS Regions, see Example IAM policies for AWS Artifact in commercial AWS Regions

You can create permissions policies that grant permissions to IAM users. You can grant users access to AWS Artifact reports and the ability to accept and download agreements on behalf of either a single account or an organization.

The following example policies show permissions that you can assign to IAM users based on the level of access that they need.

- Example policies to manage AWS reports
- Example policies to manage agreements
- Example policies to integrate with AWS Organizations
- Example policies to manage agreements for the management account
- Example policies to manage organizational agreements

Example policies to manage reports

The following policy grants permission to download all reports.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permission to download only the SOC, PCI, and ISO reports.

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport",
        "artifact:ListReportVersions"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example policies to manage agreements

The following policy grants permission to download all agreements. IAM users must also have this permission to accept agreements.

```
{
  "Version":"2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

The following policy grants permission to accept all agreement.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
```

```
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    }
  ]
}
```

The following policy grants permission to terminate all agreement.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
```

```
}
```

The following policy grants permissions to view and execute account level agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example policies to integrate with AWS Organizations

The following policy grants permission to create the IAM role that AWS Artifact uses to integrate with AWS Organizations. Your organization's management account must have these permissions to get started with organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

The following policy grants permission to grant AWS Artifact the permissions to use AWS Organizations. Your organization's management account must have these permissions to get started with organizational agreements.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
```

```
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EnableServiceTrustForArtifact",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "aws-artifact-account-sync.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

Example policies to manage agreements for the management account

The following policy grants permissions to manage agreements for the management account.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "EnableServiceTrustForArtifact",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "organizations:ServicePrincipal": [
                "aws-artifact-account-sync.amazonaws.com"
            ]
        }
      }
    }
  ]
}
```

Example policies to manage organizational agreements

The following policy grants permissions to manage organizational agreements. Another user with the required permissions must set up the organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
```

```
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permissions to view organizational agreements.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
```

```
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Using AWS managed policies for AWS Artifact

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

AWS managed policy: AWSArtifactReportsReadOnlyAccess

You can attach the `AWSArtifactReportsReadOnlyAccess` policy to your IAM identities.

This policy grants *read-only* permissions that allow listing, viewing, and downloading reports.

Permissions details

This policy includes the following permissions.

- `artifact` – Allows principals to list, view, and download reports from AWS Artifact.

AWS managed policy: AWSArtifactAgreementsReadOnlyAccess

You can attach the `AWSArtifactAgreementsReadOnlyAccess` policy to your IAM identities.

This policy grants *read-only* access to list the AWS Artifact service agreements and to download the accepted agreements. It also includes permissions to list as well as describe the organization details. Additionally, the policy provides the ability to check if the required service-linked role exists.

Permissions details

This policy includes the following permissions.

- `artifact` – Allows principals to list all the agreements and to view accepted agreements from AWS Artifact.
- `iam` – Allows principals to check if the required service linked role exists.
- `organizations` – Allows principals to describe the current organization and to list service access for that organization.

AWS managed policy: AWSArtifactAgreementsFullAccess

You can attach the `AWSArtifactAgreementsFullAccess` policy to your IAM identities.

This policy grants *`full`* permissions to list, download, accept, and terminate AWS Artifact agreements. It also includes permissions to list and enable AWS service access in the AWS Organizations service, as well as describe the organization details. Additionally, the policy provides the ability to check if the required service-linked role exists and creates one if it doesn't.

Permissions details

This policy includes the following permissions.

- `artifact` – Allows principals to list, download, accept, and terminate the agreements from AWS Artifact.
- `iam` – Allows principals to check if the required service linked role exists, and create one if it doesn't.
- `organizations` – Allows principals to describe the current organization and to list/enable service access for that organization.

AWS managed policy: AWSArtifactComplianceInquiriesReadOnlyAccess

You can attach the `AWSArtifactComplianceInquiriesReadOnlyAccess` policy to your IAM identities.

With this policy attached, you can list, view, and export AWS Artifact compliance inquiries for Assurance Assistant.

Permissions details

This policy includes the following permissions.

- `artifact` – Allows principals to list, view, and export compliance inquiries in AWS Artifact.

AWS managed policy: AWSArtifactComplianceInquiriesFullAccess

You can attach the `AWSArtifactComplianceInquiriesFullAccess` policy to your IAM identities.

With this policy attached, you can create, list, view, export, and submit feedback on AWS Artifact compliance inquiries for Assurance Assistant.

You can also select an existing notification configuration when you create an inquiry.

> **Note**
>
> This policy lets you select an existing notification configuration, but you can't use it to create a new one. Before a configuration is available to select, you must set up AWS User Notifications separately. First, select notification hubs. Then, create a notification configuration with a verified email recipient. Until you do, no configurations appear in the list when you create an inquiry. For more information, see Configuring email notifications in AWS Artifact.

Permissions details

This policy includes the following permissions.

- `artifact` – Allows principals to create, list, view, export, and submit feedback on compliance inquiries in AWS Artifact.
- `notifications` – Allows principals to list the existing notification configurations that they can select when they create an inquiry, and to read each configuration's delivery channels and event rules so that AWS Artifact can show which notifications the configuration sends.
- `notifications-contacts` – Allows principals to view the email contact for each delivery channel on those notification configurations.

AWS Artifact updates to AWS managed policies

View details about updates to AWS managed policies for AWS Artifact since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Artifact Document history page.

Change	Description	Date
AWSArtifactComplianceInquiriesFullAccess – Update to an existing policy	Added AWS User Notifications and AWS User Notifications Contacts (`notifications` and `notifications-contacts`) permissions. With these permissions, you can select an existing notification configuration when you create a compliance inquiry. AWSArtifactComplianceInquiriesReadOnlyAccess is unchanged.	2026-09-30
AWSArtifactComplianceInquiriesFullAccess – Update to an existing policy	Added the `artifact:PutComplianceInquiryFeedback` permission. With this permission, you can submit feedback on compliance inquiry responses.	2026-07-23
Introduced AWS Compliance Inquiries managed policies	Introduced AWSArtifactComplianceInquiriesReadOnlyAccess and AWSArtifactComplianceInquiriesFullAccess managed policies for Assurance Assistant.	2026-06-30
AWSArtifactReportsReadOnlyAccess – Update to an existing policy	AWS Artifact added the `artifact:ListReportVersions` permission to allow listing report versions.	2025-12-15
Updated AWS Agreements managed policies	Updated AWSArtifactAgreementsFullAccess managed policy to scope	2025-10-16

Change	Description	Date
	`organizations:EnableAWSServiceAccess` permissions down to AWS Artifact's service principal. This does not impact the managed policy's functionality.	
Updated AWS Reports managed policies	Updated AWSArtifactReportsReadOnlyAccess managed policy to remove the artifact:get permission.	2025-03-21
Introduced AWS Agreements managed policies	Introduced AWSArtifactAgreementsReadOnlyAccess and AWSArtifactAgreementsFullAccess managed policies.	2024-11-21
AWS Artifact started tracking changes	AWS Artifact started tracking changes for its AWS managed policies and introduced AWSArtifactReportsReadOnlyAccess.	2023-12-15

Using service-linked roles for AWS Artifact

AWS Artifact uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to AWS Artifact. Service-linked roles are predefined by AWS Artifact and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Artifact easier because you don't have to manually add the necessary permissions. AWS Artifact defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Artifact can assume its roles. The defined permissions include

the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting its related resources. This protects your AWS Artifact resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have **Yes** in the **Service-linked roles** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Artifact

AWS Artifact uses the service-linked role named **AWSServiceRoleForArtifact** – Allows AWS Artifact to gather information about an organization via AWS Organizations.

The AWSServiceRoleForArtifact service-linked role trusts the following services to assume the role:

- `artifact.amazonaws.com`

The role permissions policy named AWSArtifactServiceRolePolicy allows AWS Artifact to complete the following actions on the `organizations` resource.

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

Creating a service-linked role for AWS Artifact

You don't need to manually create a service-linked role. When you go to the **Organization agreements** tab in an organization management account and choose the **Get started** link in the AWS Management Console, AWS Artifact creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you go to the **Organization agreements** tab in an organization management account and choose the **Get started** link, AWS Artifact creates the service-linked role for you again.

Editing a service-linked role for AWS Artifact

AWS Artifact does not allow you to edit the AWSServiceRoleForArtifact service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for AWS Artifact

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

> **Note**
>
> If the AWS Artifact service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete AWS Artifact resources used by the AWSServiceRoleForArtifact

1. Visit the 'Organization Agreements' table in the AWS Artifact console
2. Terminate any active Organization agreements

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForArtifact service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for AWS Artifact service-linked roles

AWS Artifact does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForArtifact role in the following Regions.

Region name	Region identity	Support in AWS Artifact
US East (N. Virginia)	us-east-1	Yes

Region name	Region identity	Support in AWS Artifact
US East (Ohio)	us-east-2	No
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Yes
Africa (Cape Town)	af-south-1	No
Asia Pacific (Hong Kong)	ap-east-1	No
Asia Pacific (Jakarta)	ap-southeast-3	No
Asia Pacific (Mumbai)	ap-south-1	No
Asia Pacific (Osaka)	ap-northeast-3	No
Asia Pacific (Seoul)	ap-northeast-2	No
Asia Pacific (Singapore)	ap-southeast-1	No
Asia Pacific (Sydney)	ap-southeast-2	No
Asia Pacific (Tokyo)	ap-northeast-1	No
Canada (Central)	ca-central-1	No
Europe (Frankfurt)	eu-central-1	No
Europe (Ireland)	eu-west-1	No
Europe (London)	eu-west-2	No
Europe (Milan)	eu-south-1	No
Europe (Paris)	eu-west-3	No
Europe (Stockholm)	eu-north-1	No
Middle East (Bahrain)	me-south-1	No

Region name	Region identity	Support in AWS Artifact
Middle East (UAE)	me-central-1	No
South America (São Paulo)	sa-east-1	No
AWS GovCloud (US-East)	us-gov-east-1	No
AWS GovCloud (US-West)	us-gov-west-1	Yes

Using IAM condition keys for AWS Artifact reports

You can use IAM condition keys to provide fine-grained access to reports on AWS Artifact, based on specific report categories and series.

The following example policies show permissions that you can assign to IAM users based on specific report categories and series.

Example policies to manage AWS reports read access

AWS Artifact reports are denoted by the IAM resource, `report`.

The following policy grants permission to read all AWS Artifact reports under the `Certifications and Attestations` category.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

The following policy lets you grant permission to read all AWS Artifact reports under the SOC series.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC"
                }
            }
        }
    ]
}
```

The following policy lets you grant permission to read all AWS Artifact reports under the `Certifications and Attestations` category, and SOC series.

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

Logging AWS Artifact API calls with AWS CloudTrail

AWS Artifact is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Artifact. CloudTrail captures API calls for AWS Artifact as events. The calls captured include calls from the AWS Artifact console and code calls to the AWS Artifact API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Artifact. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Artifact, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

AWS Artifact information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in AWS Artifact, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history.

For an ongoing record of events in your AWS account, including events for AWS Artifact, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

AWS Artifact supports logging the following actions as events in CloudTrail log files:

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding AWS Artifact log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the GetReportMetadata action.


```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
```

```
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    }
  ]
}
```

Document history for AWS Artifact

The following table provides a history of AWS Artifact releases and related changes to the AWS Artifact User Guide.

Change	Description	Date
Updated AWSArtifactComplianceInquiriesFullAccess managed policy	Updated the AWSArtifactComplianceInquiriesFullAccess managed policy to include AWS User Notifications and AWS User Notifications Contacts (`notifications` and `notifications-contacts`) permissions. With these permissions, you can select an existing notification configuration when you create a compliance inquiry.	September 30, 2026
Updated AWSArtifactComplianceInquiriesFullAccess managed policy	Updated the AWSArtifactComplianceInquiriesFullAccess managed policy to include the `artifact:PutComplianceInquiryFeedback` permission. With this permission, you can submit feedback on compliance inquiry responses.	July 23, 2026
Assurance Assistant	Added Assurance Assistant documentation for generating AI-powered responses to compliance and due diligence questions. Launched AWSArtifactComplianceInquir	June 30, 2026

	iesReadOnlyAccess and AWSArtifactComplianceInquiriesFullAccess AWS managed policies and added example IAM policies for compliance inquiry access.	
Updated permissions for ListReportVersions API	Updated example IAM policies, example GovCloud IAM policies, AWSArtifactReportsReadOnlyAccess managed policy, and downloading a report instructions to include the `artifact:ListReportVersions` permission and support for downloading report versions to accommodate the new ListReportVersions API.	December 15, 2025
Updated AWSArtifactAgreementsFullAccess managed policy	Updated AWSArtifactReportsReadOnlyAccess managed policy to scope `organizations:EnableAWSServiceAccess` permissions down to AWS Artifact's service principal. This does not impact the managed policy's functionality.	October 16, 2025
IAM Action Deprecation Notice Update	Updated the IAM action deprecation notice for `artifact:DownloadAgreement` and `artifact:Get` in the AWS GovCloud (US) partition.	July 1, 2025

Fine-grained permissions for AWS Artifact in AWS GovCloud (US) Regions	Updated and expanded policies for using AWS Artifact in AWS GovCloud (US) Regions, while removing notes about limitations as AWS Artifact functionality is now more broadly applicable across all regions.	March 31, 2025
Updated AWSArtifactReportsReadOnlyAccess managed policy	Updated AWSArtifactReportsReadOnlyAccess managed policy to remove the artifact:get permission.	March 21, 2025
Example policies for AWS Artifact in AWS GovCloud (US) Regions	Added example policies for using AWS Artifact in AWS GovCloud (US) Regions, and noted which pages do not apply to using AWS Artifact in AWS GovCloud (US) Regions.	December 6, 2024
Fine-grained permissions for agreement execution, AWSArtifactAgreementsFullAccess and AWSArtifactAgreementsReadOnlyAccess managed policies	Enabled fine-grained access for AWS Artifact agreement execution and launched AWSArtifactAgreementsFullAccess and AWSArtifactAgreementsReadOnlyAccess AWS managed policies.	November 21, 2024
Fine-grained report access and AWSArtifactReportReadOnlyAccess managed policy	Enabled fine-grained access to AWS Artifact reports, enabled report condition keys, and launched AWSArtifactReportsReadOnlyAccess managed policy.	December 15, 2023

AWS Artifact service-linked role	Added service-linked role documentation and updated example policies for AWS Artifact and AWS Organizations integration.	September 26, 2023
Notifications	Published the documentation for managing notifications, and made relevant updates to the AWS Artifact API Reference, CloudTrail logging documentation, and the **Identity and access management** page.	August 1, 2023
Third-party reports - Generally available	Added API reference documentation and CloudTrail logging documentation, and made third-party reports generally available.	January 27, 2023
Third-party reports (Preview)	Launched compliance reports of the independent software vendors (ISVs) who sell their products on AWS Marketplace. Added example policies to **Identity and access management** page for third-party reports.	November 30, 2022
Security	Added section to **Identity and access management** page for confused deputy prevention.	December 20, 2021

Reports	Removed nondisclosure agreement and introduced terms and conditions for report downloads.	December 17, 2020
Home page and search	Added service home page and search bar on the reports and agreements page.	May 15, 2020
AWS GovCloud (US) launch	Launched AWS Artifact in AWS GovCloud (US) Regions.	November 7, 2019
AWS Organizations agreements	Added support for managing agreements for an organization.	June 20, 2018
Agreements	Added support for managing AWS Artifact agreements.	June 17, 2017
Initial release	This release introduces AWS Artifact.	November 30, 2016