User Guide

AWS Artifact

AWS Artifact: User Guide

Table of Contents

What is AWS Artifact?

AWS Artifact provides on-demand downloads of AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI) reports, and Service Organization Control (SOC) reports. You can submit the security and compliance documents (also known as *audit artifacts*) to your auditors or regulators to demonstrate the security and compliance of the AWS infrastructure and services that you use. You can also use these documents as guidelines to evaluate your own cloud architecture and assess the effectiveness of your company's internal controls.

Additionally, AWS Artifact provides on-demand downloads of the security and compliance documents such as ISO certifications, and Service Organization Control (SOC) reports of the Independent Software Vendors (ISVs) who sell their products on AWS Marketplace. For more information, see AWS Marketplace Vendor Insights.

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.

You can also use AWS Artifact to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA). A BAA typically is required for companies that are subject to the Health Insurance Portability and Accountability Act (HIPAA) to ensure that protected health information (PHI) is appropriately safeguarded. With AWS Artifact, you can accept agreements with AWS and designate AWS accounts that can legally process restricted information. You can accept an agreement on behalf of multiple accounts. To accept agreements for multiple accounts, use AWS Organizations to create an organization.

For more information, see AWS Artifact.

Pricing

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

Getting started with AWS Artifact

AWS Artifact provides a central resource for AWS security and compliance reports. The artifacts available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies that validate the implementation and operating effectiveness of AWS security controls. Additionally, AWS Artifact provides on-demand access to the security and compliance documents such as ISO certifications, and Service Organization Control (SOC) reports of the Independent Software Vendors (ISVs) who sell their products on AWS Marketplace. For more information, see AWS Marketplace Vendor Insights.

AWS Artifact enables you to accept and manage legal agreements such as the Business Associate Addendum (BAA). If you use AWS Organizations, you can accept agreements on behalf of all accounts within your organization. When accepted, all existing and subsequent member accounts are automatically covered by the agreement.

Tasks

- Step 1: Sign up for AWS
- Step 2: Download a report
- Step 3: Manage agreements
- Step 4: Manage notifications

Step 1: Sign up for AWS

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign

administrative access to a user, and use only the root user to perform tasks that require root user access.

Step 2: Download a report

You can download reports using Adobe Acrobat Reader. Other PDF readers are not supported. For more information, see Downloading reports.

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**.
3. On the **Reports** page, use the **AWS reports** tab to access an AWS reports and navigate to the **Third-party reports** tab to access the reports of the Independent Software Vendors (ISVs) who sell their products on AWS Marketplace.
4. (Optional) Enter a keyword in the search field to locate a report.
5. Select a report, and then choose **Download report**.
6. (Optional) On the **Third-party reports** tab, you can access the details page of an ISV report by clicking on the **Report** title to learn more about the report.
7. You might be asked to accept **Terms and conditions** that apply to the specific report you are downloading. We recommend that you read them closely. When you are finished, 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 please make sure to check for attachments within the PDF file for supporting documentation. Check here for instructions on how to view attachments.

Third-party reports are accessible only for AWS customers who have onboarded to AWS Marketplace Vendor Insights. To learn more, see AWS Marketplace Vendor Insights.

Step 3: Manage agreements

Before you enter into an agreement, you must download and agree to the terms of the AWS Artifact nondisclosure agreement (NDA). Each agreement is confidential and cannot be shared with others outside of your company.

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. Choose **Account agreements** to manage agreements for your account or **Organization agreements** to manage agreements on behalf of your organization.
4. Expand the section of the agreement.
5. Choose **Download and review**.
6. Read the **Terms and conditions**. When you are finished, choose **Accept and download**.
7. Review the agreement and then select the check boxes to indicate that you agree.
8. Choose **Accept** to accept the agreement.

For more information, see Managing agreements.

Step 4: Manage notifications

You can subscribe to notifications for the availability of new reports and agreements or updates to existing reports and agreements. AWS Artifact uses the AWS User Notification service to send notifications. Notifications are sent to email addresses that the user provides during the notification configuration setup.

To create a configuration

1. Open the notification hubs page in AWS User Notifications service
2. Select the region(s) where you want to store your AWS User Notifications resources. By default, your User Notifications data will be stored in US East (N. Virginia), and replicated across other regions you select. See notification hubs documentation for more details.
3. Click on **Create configuration**.
4. To receive notifications for agreements, click the checkbox for **Updates on AWS Agreements**.

5. To receive notifications for reports, click the checkbox for **Updates on AWS Reports**. To only receive notifications for reports under specific categories and series, click the checkbox for **A subset of reports** and click the checkbox for the categories and series you are interested in.
6. Enter a name for your configuration.
7. Enter a comma separated list of emails where notifications should be sent.
8. (Optional) To assign a tag to the notification configuration, enter the key-value pairs by expanding the Tags section. Note: A tag is a label that you can assign to an AWS resource and each tag consists of a key and an optional value that you can define. Tags help you manage, search for, and filter resources.
9. Click **Submit**.
10. A verification email will be sent to the provided email addresses and the email recipients will need to click **Verify email** link within the verification email sent to them. Please note that only verified email addresses will start receiving notifications.

For more information, see Managing 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 such as Amazon WorkDocs. Some reports require you to accept the **Terms and conditions** before you can download them.

Contents

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**.
3. On the **Reports** page, use the **AWS reports** tab to access an AWS reports and navigate to the **Third-party reports** tab to access the reports of the Independent Software Vendors (ISVs) who sell their products on AWS Marketplace.
4. (Optional) Enter a keyword in the search field to locate a report.
5. Select a report, and then choose **Download report**.
6. (Optional) On the **Third-party reports** tab, you can access the details page of an ISV report by clicking on the **Report** title to learn more about the report.

7. You might be asked to accept **Terms and conditions** that apply to the specific report you are downloading. We recommend that you read them closely. When you are finished, 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 please make sure to check for attachments within the PDF file for supporting documentation. Check here for instructions on how to view attachments.

Viewing attachments in PDF documents

The following applications that currently support viewing PDF attachments are recommended:

Adobe Acrobat Viewer

1. Download the latest version of Adobe Acrobat from here.
2. Open the file in Adobe Acrobat viewer.
3. To open the Attachments panel, click the paperclip icon in the left of the PDF document or choose View > Show/Hide > Navigation Panes > Attachments.
4. In the Attachments panel, double-click the attachment to view the document.

Firefox Browser

1. Download Firefox browser from here
2. Open the PDF file in Firefox browser by using the open file option from File menu.
3. To open the attachments, click the Toggle sidebar icon on the top left of the screen.

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, such as Amazon WorkDocs, 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

AWS Artifact Agreements enable you to use the AWS Management Console to review, accept, and manage agreements for your account or organization. For example, a Business Associate Addendum (BAA) agreement typically is required for companies that are subject to the Health Insurance Portability and Accountability Act (HIPAA) to ensure that protected health information (PHI) is appropriately safeguarded. You can use AWS Artifact to accept an agreement such as the BAA with AWS, and designate an AWS account that can legally process PHI. If you use AWS Organizations, you can accept agreements such as the AWS BAA on behalf of all 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 accepted an agreement and to review the terms of the accepted agreement to understand your obligations. If your account or organization no longer needs to use the accepted agreement, you can use AWS Artifact to terminate the agreement. If you terminate the agreement but later realize that you need it, you can activate it again.

Contents

Managing an agreement for a single account in AWS Artifact

You can accept agreements for just your account, even if your account is a member account in an organization in AWS Organizations. For more information about AWS Organizations, see the AWS Organizations User Guide.

Accepting an agreement with AWS

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, you can grant IAM users and federated users with roles 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 following permissions:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

For more information, see Identity and access management.

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. Choose the **Account agreements** tab.
4. Expand the section of the agreement.
5. Choose **Download and review**.
6. Read the **Terms and conditions**. When you are finished, choose **Accept and download**.
7. Review the agreement and then select the check boxes to indicate that you agree.
8. Choose **Accept** to accept the agreement for your account.

Terminating an agreement with AWS

If you used the AWS Artifact console to accept an agreement, you can use the console to terminate that agreement. Otherwise, see Offline agreements.

Required permissions

To terminate an agreement, IAM and federated users must have the following permissions:

```
artifact:TerminateAgreement
```

For more information, see Identity and access management.

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 check boxes to indicate that you agree to terminate the agreement.
6. Choose **Terminate**. When prompted for confirmation, choose **Terminate**.

Managing an agreement for multiple accounts in AWS Artifact

If you are the owner of the management account of an AWS Organizations organization, you can accept an agreement on behalf of all accounts in your organization. You must be signed in to the management account with the correct AWS Artifact permissions to accept or terminate organization agreements. Users of member accounts with `organizations:DescribeOrganization` permissions can view the organization agreements that are accepted on their behalf.

If your account is not part of an organization, you can create or join an organization by following the instructions in Creating and managing an organization in the *AWS Organizations User Guide*.

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*.

If a member account is removed from an organization, that member account will no longer be covered by organization agreements. Management account administrators should communicate this to member accounts before removing member accounts from the organization, so that member accounts can put new agreements in place if necessary. A list of active organization agreements can be viewed in AWS Artifact Organization agreements.

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

Accepting an agreement for your organization

You can accept an agreement on behalf of all member accounts in your organization in AWS Organizations. Before you accept an agreement, we recommend that you consult with your legal, privacy, and compliance team.

Required permissions

To accept an agreement, the owner of the management account must have the following permissions:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

For more information, see Identity and access management.

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. Expand the section of the agreement.
5. Choose **Download and review**.
6. Read the **Terms and conditions**. When you are finished, choose **Accept and download**.
7. Review the agreement and then select the check boxes to indicate that you agree.
8. Choose **Accept** to accept the agreement for all existing and future accounts in your organization..

Terminating an organization agreement

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

Required permissions

To terminate an agreement, the owner of the management account must have the following permissions:

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

For more information, see Identity and access management.

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 check boxes to indicate that you agree to terminate the agreement.
6. Choose **Terminate**. When prompted for confirmation, choose **Terminate**.

Managing an existing offline agreement 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.

If your account is the management account in an AWS Organizations organization, you can use AWS Artifact to apply the terms of your offline agreement to all accounts in your organization. To apply an agreement that you accepted offline to your organization and all accounts in your organization, you must have the following permissions:

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

If your account is a member account in an organization, you must have the following permissions to see your offline organization agreements:

```
organizations:DescribeOrganization
```

For more information, see Identity and access management.

Managing notifications in AWS Artifact

AWS Artifact notifications enables you to setup email notifications. On the notification settings page, you can subscribe to notifications and manage other notification settings as described below. AWS Artifact sends notifications using the AWS User Notifications service. To use AWS Artifact notifications you must have the required permissions for the AWS Artifact and AWS User Notification services. For more information, see Identity and access management.

Contents

Setting up your notifications

Before you can start receiving notifications, you will need to specify the region(s) where your User Notifications data will be stored. Follow the steps below to setup notification hubs.

To set up Notification hubs

1. Open the notification hubs page in AWS User Notifications service.
2. Select the region(s) that you would like to store your AWS User Notifications resources. By default, your User Notifications data will be stored in US East (N. Virginia), and will be replicated across the other regions you selected. Refer to notification hubs documentation for more details.
3. Click **Submit**.

To subscribe to notifications

1. Open AWS Artifact notification settings page.
2. Click the toggle **Subscribe to Artifact notifications** to subscribe to notifications on AWS Artifact.

To unsubscribe to notifications

1. Open AWS Artifact notification settings page.
2. Click the toggle **Subscribe to Artifact notifications** to unsubscribe to notifications on AWS Artitfact.

To create a configuration

1. Open AWS Artifact notification settings page.
2. Click **Create configuration**.
3. To receive notifications for agreements, keep the checkbox selected next to **Updates on AWS Agreements**.
4. To receive notifications for reports, keep the checkbox selected next to **Updates on AWS Reports**.
5. To receive notifications for all reports, keep the checkbox selected next to **All reports**.
6. To receive notifications only for reports under specific categories and series, click the checkbox for **A subset of reports**. Then, click the checkbox for the categories and series you are interested in.
7. Enter a name for your configuration.
8. Enter a comma-separated list of emails where notifications should be sent.
9. (Optional) To assign a tag to the notification configuration, enter the key-value pairs by expanding the Tags section. Note: A tag is a label that you can assign to an AWS resource and each tag consists of a key and an optional value that you can define. Tags help you manage, search for, and filter resources.
10. Click **Create configuration**.
11. A verification email will be sent to the provided email addresses and the email recipients will need to click **Verify email** link within the verification email sent to them. Please note that only verified email addresses will start receiving notifications.

To edit a configuration

1. Open AWS Artifact notification settings page.
2. Click on the row of the configuration you would like to edit.
3. Click **Edit** button on the top right of the page.

4. You can edit any of the fields. Once you are satisfied with your change, press **Save changes**.
5. If you have added new email addresses, a verification email will be sent to each those email addresses. Click the **Verify email** link within the verification email.

To delete a configuration

1. Open AWS Artifact notification settings page.
2. Click on the row of the configuration you would like to delete.
3. Click **Delete**.
4. Once you have read the warning message, click **Delete**.

Assigning tags to a configuration

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags help you manage, search for, and filter resources. You can optionally set tags when you create or edit a configuration. To read more, see Tagging resources

Troubleshooting

If you receive an error message while using AWS Artifact notifications, see Troubleshooting in the AWS Artifact FAQ.

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

Setup 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

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.
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**.

Migrating to fine-grained permissions

AWS Artifact now enables customers to use fine-grained permissions. Through these fine-grained permissions, customers will have granular control on providing access to features such as accepting terms and downloading reports.

To access reports through the fine-grained permissions, customers should utilize the AWSArtifactReportsReadOnlyAccess Managed Policy or update their permissions as per the below recommendation. Then customers should opt-in using the **try out the new AWS reports page** link available in the console.

Users will have the option to access the reports with old permissions through the **use the old reports page** link available in the console if there is an issue with updating to the new permissions.

Migrating to new permissions

Migrate non-resource specific permissions

Users need to replace the existing Policy containing legacy permissions with a Policy containing fine-grained permissions

Legacy Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/*"
      ]
    }
  ]
}
```

New Policy with fine-grained permissions:

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

Migrate resource-specific permissions

Users need to replace their existing Policy containing legacy permissions with a Policy containing fine-grained permissions. Report resource wildcard permissions have been replaced with condition keys.

Legacy Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get"
      ],
      "Resource": [
        "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
        "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
      ]
    }
  ]
}
```

New policy with fine-grained permissions and condition keys.

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

```
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example IAM policies

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 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 notifications

Example 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"
      ],
      "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",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
```

```
    }
  ]
}
```

Example 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:ListReport"
      ],
      "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"
      ]
    }
  ]
}
```

Example 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:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to accept an agreement.

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

```
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

The following policy grants permission to terminate an agreement.

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

The following policy grants permissions to manage single account agreements.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
```

```
      ]
    }
  ]
}
```

Example 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": [
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

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:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
```

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

Example 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": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
```

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

Example 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": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy grants permissions to view organizational agreements.

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 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": [
        "*"
      ]
    }
  ]
}
```

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.

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

Artifact updates to AWS managed policies

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

Change	Description	Date
Artifact started tracking changes	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 the AWS Organizations service.

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 visit the Organizations Agreements tab in an organization management account and select 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 visit the Organizations Agreements tab in an organization management account and select 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
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

Region name	Region identity	Support in AWS Artifact
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
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	No

Using IAM condition keys

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 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",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

The following policy lets you grant permission to read all AWS Artifact reports except for those 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: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

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 describes the releases for AWS Artifact.

Change	Description	Date
Fine-grained report access and AWSArtifactReportReadOnlyAccess managed policy	Enabled fine-grained access to 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 API reference guide, CloudTrail logging documentation, and the AWS Artifact Identity and Access Management page.	August 1, 2023
Third-party reports - Generally available	Added API reference documentation, 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	November 30, 2022

	products on AWS Marketpla ce. Additionally, added example policies to Identity and access management page for third-party reports.	
Security	Added section to Identity and access management page for confused deputy prevention.	December 20, 2021
Reports	Removed non-disclosure agreement and introduce d 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
GovCloud launch	Launched AWS Artifact in GovCloud regions.	November 7, 2019
AWS Organizations agreements	Added support for managing agreements for an organizat ion.	June 20, 2018
Agreements	Added support for managing AWS Artifact agreements.	June 17, 2017
Initial release	This release introduces AWS Artifact.	November 30, 2016