AWS Artifact

User Guide

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), 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. AWS Artifact provides documents about AWS only. 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 Managing Your Agreements in AWS Artifact (p. 8).

Topics

Are You a First-Time User of AWS Artifact?

If you're a first-time user of AWS Artifact, we recommend that you begin by reading the following sections:

- Securing Your Documents (p. 2)
- Setting Up AWS Artifact (p. 3)
- Getting Started with AWS Artifact (p. 5)
- Downloading Reports in AWS Artifact (p. 7)

Accessing AWS Artifact

AWS Artifact provides a web-based user interface, the AWS Artifact console. If you have signed up for an AWS account, you can access the AWS Artifact console by signing in to https://console.aws.amazon.com/artifact/ and choosing **Artifact** from the console home page. If you don't have an AWS account yet, see Sign Up for AWS (p. 3).

For information about creating permissions that control access to the console for you and other users, see Create an IAM Admin Group and User (p. 3).

Securing Your Documents

AWS Artifact documents are confidential and should be kept secure at all times. AWS Artifact uses the AWS shared compliance 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 sign a nondisclosure agreement (NDA) 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, or 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. Don't send the documents through email or upload them to an unsecure site.

AWS Artifact Regions

AWS Artifact is available in all public regions.

Pricing for AWS Artifact

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

Setting Up AWS Artifact

When you sign up for AWS, your AWS account is automatically signed up for all services in AWS, including AWS Artifact. If you haven't signed up for AWS, see Sign Up for AWS (p. 3).

To create and manage user permissions to provide highly secure, limited access to your AWS resources, both for yourself and for others who need to work with your AWS resources, see Create an IAM Admin Group and User (p. 3).

Topics

Sign Up for AWS

If you do not have an AWS account, use the following procedure to create one.

To sign up for AWS

1. Open https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   If you previously signed in to the AWS Management Console using AWS account root user credentials, choose **Sign in to a different account**. If you previously signed in to the console using IAM credentials, choose **Sign-in using root account credentials**. Then choose **Create a new AWS account**.

2. Follow the online instructions.

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

Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad. Note your AWS account number because you will need it later.

Create an IAM Admin Group and User

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. 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 the account with your 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. For more information, see Getting Started with AWS Artifact (p. 5).

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

Getting Started with AWS Artifact

AWS Artifact offers a number of documents for downloading and allows 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.

This Getting Started tutorial shows you how to set up permissions to download reports or manage agreements by completing the following steps:

1. Step 1: Create an Administrators Group and Add an IAM User
2. Step 2: Download a Report and Manage an Agreement

Step 1: Create an Administrators Group and Add an IAM User

In this step, you create an Administrators group, create an IAM user for yourself, and add your IAM user to the group. Creating an IAM group allows you to attach the permissions to a group instead of an individual user, and you can grant the same permission to other users by adding them to the group.

To create an IAM user for yourself and add the user to an Administrators group

1. Use your AWS account email address and password to sign in as the *AWS account root user* to the IAM console at https://console.aws.amazon.com/iam/.

   Note
   We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.
2. In the navigation pane of the console, choose **Users**, and then choose **Add user**.
3. For **User name**, type **`Administrator`**.
4. Select the check box next to **AWS Management Console access**, select **Custom password**, and then type the new user's password in the text box. You can optionally select **Require password reset** to force the user to create a new password the next time the user signs in.
5. Choose **Next: Permissions**.
6. On the **Set permissions** page, choose **Add user to group**.
7. Choose **Create group**.
8. In the **Create group** dialog box, for **Group name** type **`Administrators`**.
9. For **Filter policies**, select the check box for **AWS managed - job function**.
10. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.
11. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
12. Choose **Next: Tags** to add metadata to the user by attaching tags as key-value pairs.
13. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users, and to give your users access to your AWS account resources. To learn about using policies to restrict users' permissions to specific AWS resources, go to Access Management and Example Policies.

> **Note**
> For information on IAM policies that are specific to AWS Artifact, see Controlling Access (p. 12).

You can repeat the preceding steps one through six and then choose the **Administrators** group from the list to grant administrator permissions to other IAM users.

Step 2: Download a Report and Manage an Agreement

Now that you have set up your IAM users and policies, you can download a document by following the procedure in Downloading Reports in AWS Artifact. You can also manage your AWS agreements. For more information, see Managing Your Agreements in AWS Artifact.

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 sign a nondisclosure agreement (NDA) before you can download them.

To download a report, you must have the appropriate permissions. For more information about permissions, see Controlling Access (p. 5).

To download a document

1. Sign in to the AWS Management Console and open the AWS Artifact console at https://console.aws.amazon.com/artifact/.
2. On the **AWS Artifact** dashboard, choose **Reports**.
3. Locate the report, and then choose **Get this artifact**.
4. Read the **Terms and conditions** for the document. You might be asked to sign a nondisclosure agreement (NDA) to download the document.

   Note
   The NDA is a legally binding contract. We recommend that you read it closely.
5. After you have read the **Terms and Conditions**, select the check box at the bottom of the page and then choose **Accept and download**. AWS Artifact generates your file and opens it in another window.
6. In the document window choose **Save File** or **Open with Adobe Acrobat Reader**, and then choose **OK**. Your document is downloaded to the specified location on your computer or opened in Adobe Reader.

Getting Permissions For Additional Reports

When you sign up for AWS Artifact, your account is automatically granted permissions to download some reports. If you need to request access to another listed report, use the provided form to request access from AWS.

Managing Your 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 Agreements to terminate the agreement.

Managing an Agreement for a Single Account

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

If you're an administrator of an account, you can give 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 about these permissions, see Create an IAM Policy (p. 12).

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

To accept an agreement with AWS

1. Sign in to the AWS Management Console and 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 that you want.
5. Choose **Download and review**.

6. In the **Terms and conditions** dialog box, choose **Accept and download**.

   Note
   The NDA is a legally binding contract. We recommend that you read it closely.
7. Review the agreement and then select the check boxes to indicate that you agree with the content.
8. Choose **Accept** to accept the agreement for just 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. To terminate an agreement, IAM and federated users must have the following permissions:

```
artifact:TerminateAgreement
```

For more information about these permissions, see Create an IAM Policy (p. 12).

Note
If you didn't use the AWS Artifact console to accept an agreement, you can't use the console to terminate the agreement. For more information, see Managing an Existing Offline Agreement (p. 11).

To terminate your online agreement with AWS

1. Sign in to the AWS Management Console and 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. For the agreement that you want to terminate, choose **Terminate agreement for this account**.
5. Choose the **Terminate** section.
6. Select all check boxes to indicate that you agree to terminate the agreement.
7. Choose the **Terminate** button. When prompted, choose it again.

Managing an Agreement for Multiple Accounts

If you are the owner of the master 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 master account with the correct AWS Artifact permissions to accept or terminate organization agreements. Users of member accounts with `describeOrganizations` 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 AWS Organizations.

Notes

- 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.
- If a member account is removed from an organization, that member account will no longer be covered by organization agreements. Master 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 about AWS Organizations and master accounts, see Managing the AWS Accounts in Your Organization. For more information about setting up an administrator account for AWS Artifact, see Step 1: Create an Administrators Group and Add an IAM User (p. 5).

Accepting an Agreement for Your Organization

You can accept an agreement on behalf of all member accounts in your organization in AWS Organizations. To accept an agreement, the owner of the master account must have the following permissions:

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateRole
iam:AttachRolePolicy
```

For more information about these permissions, see Create an IAM Policy (p. 12).

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

To accept an agreement for an organization

1. Sign in to the AWS Management Console and 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 that you want.
5. Choose **Download and review**.
6. In the **Terms and conditions** dialog box, choose **Accept and download**.

   Note
   The NDA is a legally binding contract. We recommend that you read it closely.
7. Review the agreement and then select the check boxes to indicate that you agree with the content.
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. To terminate an agreement, the owner of the master account must have the following permissions:

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

```
iam:CreateRole
iam:AttachRolePolicy
```

For more information about creating policies, see Create an IAM Policy (p. 12).

> **Note**
> If you didn't use the AWS Artifact console to accept an agreement, you can't use the console to terminate the agreement.
> For more information, see Managing an Existing Offline Agreement (p. 11).

To terminate your online organization agreement with AWS

1. Sign in to the AWS Management Console and 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. For the agreement that you want to terminate, choose **Terminate agreement for this account**.
5. Choose the **Terminate** section.
6. Select all check boxes to indicate that you agree to terminate the agreement.
7. Choose the **Terminate** button. When prompted, choose it again.

Managing an Existing Offline Agreement

Before you can view your accepted agreements for the first time, including the agreements that you accepted offline, follow the Getting Started with AWS Artifact (p. 5) process. After you go through all of the Getting Started steps, you can use the AWS Artifact console to view your offline agreements.

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 master 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:CreateRole
iam:AttachRolePolicy
```

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 about creating policies, see Create an IAM Policy (p. 12).

Controlling Access

Your administrative account has all of the permissions needed to manage agreements, but different documents and agreements might require you to delegate permissions differently for various user accounts. You delegate permissions by using IAM policies.

To grant non-administrative access, you must create a policy, attach the policy to a group, and add IAM users to the group.

1. Create an IAM Policy
2. Create an IAM Group
3. Create an IAM User and Add Them to a Group

Create an IAM Policy

Create a permissions policy that grants permissions to IAM users. The permissions allow the users to access AWS Artifact reports and accept and download agreements on behalf of either a single account or an organization. The following tables show the permissions that you can assign to IAM users based on the level of access that they need.

- Report Permissions
- Agreement Permissions
- Common AWS Artifact IAM Policies
- To create an IAM policy

Report Permissions

Permission Name	Permissions Granted	Example IAM Policy
`Get`	Grants the IAM user permission to download all reports that are accessible by the root account.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "artifact:Get" ], "Resource": [ "arn:aws:artifact:::report-package/*" ] } ] }`

Agreement Permissions

Permission Name	Permissions Granted	Example IAM Policy
`DownloadAgreement`	Grants the IAM user permission to download all agreements that are accessible by the root account. IAM users must have this permission to accept agreements.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "artifact:DownloadAgreement" ], "Resource": [ "*" ] } ] }`
`AcceptAgreement`	Grants the IAM user permission to accept an agreement on behalf of the root account. IAM users must also have permission to download agreements in order to accept an agreement.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "artifact:AcceptAgreement" ], "Resource": [ "*" ] } ] }`
`TerminateAgreement`	Grants the IAM user permission to terminate an agreement on behalf of the root account.	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "artifact:TerminateAgreement" ], "Resource": [ "*" ] } ] }`
`DescribeOrganization`	Grants the IAM user permission to retrieve information about the AWS Organizations organization that the user's account belongs to. Both master and member accounts need the `DescribeOrganizations`	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "organizations:DescribeOrganization",`

Permission Name	Permissions Granted	Example IAM Policy

	permission to view or use organization agreements.	<pre>],
		            "Resource": "*"
		        }
		    ]
		}</pre>

• `ListRoles`
• `CreateRole`
• `AttachRolePolicy`
	Grants the IAM user permission to create the IAM role that AWS Artifact uses to integrate with AWS Organizations.
	
	Your organization's master account must have these permissions to get started with organizational agreements.
		<pre>{
		    "Version": "2012-10-17",
		    "Statement": [
		        {
		            "Effect": "Allow",
		            "Action":
		 "iam:ListRoles",
		            "Resource":
		 "arn:aws:iam::*:role/*"
		        },
		        {
		            "Effect": "Allow",
		            "Action":
		 "iam:CreateRole",
		            "Resource":
		 "arn:aws:iam::*:role/service-role/
		AWSArtifactAccountSync"
		        },
		        {
		            "Effect": "Allow",
		            "Action":
		 "iam:AttachRolePolicy",
		            "Resource":
		 "arn:aws:iam::*:role/service-role/
		AWSArtifactAccountSync",
		            "Condition": {
		                "ArnEquals": {
		                    "iam:PolicyARN":
		 "arn:aws:iam::aws:policy/service-
		role/AWSArtifactAccountSync"
		                }
		            }
		        }
		    ]
		}</pre>

Permission Name	Permissions Granted	Example IAM Policy

• `EnableAWSServiceAccess`
• `ListAWSServiceAccessForOrganization`
	Grants the IAM user permission to grant AWS Artifact the permissions to use AWS Organizations. For more information about AWS Organizations, see Managing Your Agreements in AWS Artifact.
	
	Your organization's master account must have these permissions to get started with organizational agreements.
		<pre>{
		    "Version": "2012-10-17",
		    "Statement": [
		        {
		            "Effect": "Allow",
		            "Action": [
		
		"organizations:EnableAWSServiceAccess",
		
		"organizations:DescribeOrganization",
		
		"organizations:ListAWSServiceAccessForOrganizatio
		            ],
		            "Resource": "*"
		        }
		    ]
		}</pre>

Here are policies for seven of the most common use cases.

Common AWS Artifact IAM Policies

Use case	Permission names	Example policy

Full access to download reports and manage agreements	`artifact:Get`
	
	`artifact:AcceptAgreement`
	
	`artifact:DownloadAgreement`
	
	`artifact:TerminateAgreement`
	
	`organizations:DescribeOrganization`
	
	`organizations:EnableAWSServiceAccess`
	
	`organizations:ListAccounts`
	
	`organizations:ListAWSServiceAccessForOrganization`
	
	`iam:CreateRole`
	
	`iam:AttachRolePolicy`
	
	`iam:ListRoles`
		<pre>{
		    "Version": "2012-10-17",
		    "Statement": [
		        {
		            "Effect":
		"Allow",
		            "Action": [
		
		"artifact:Get",
		
		"artifact:AcceptAgreement",
		
		"artifact:DownloadAgreement",
		
		"artifact:TerminateAgreement"
		            ],
		            "Resource": [
		
		"arn:aws:artifact::*:customer-
		agreement/*",
		
		"arn:aws:artifact:::agreement/
		*",
		
		"arn:aws:artifact:::report-
		package/*"
		            ]
		        },
		        {
		            "Effect":
		"Allow",
		            "Action":
		"iam:ListRoles",</pre>

Use case	Permission names	Example policy
		"Resource": "arn:aws:iam::*:role/*" }, { "Effect": "Allow", "Action": "iam:CreateRole", "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync" }, { "Effect": "Allow", "Action": "iam:AttachRolePolicy", "Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync", "Condition": { "ArnEquals": { "iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync" } } }, { "Effect": "Allow", "Action": ["organizations:DescribeOrganization", "organizations:EnableAWSServiceAccess", "organizations:ListAccounts", "organizations:ListAWSServiceAccessForOr], "Resource": "*" }] }

Use case	Permission names	Example policy

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

Use case	Permission names	Example policy

Permissions to get started with and manage organizational agreements
 	
Master account only
	artifact:AcceptAgreement
	
	artifact:DownloadAgreement
	
	artifact:TerminateAgreement
	
	organizations:DescribeOrganization
	
	organizations:EnableAWSServiceAccess
	
	organizations:ListAccounts
	
	organizations:ListAWSServiceAccessForOrganization
	
	iam:CreateRole
	
	iam:AttachRolePolicy
	
	iam:ListRoles
		{
		"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:CreateRole",
		"Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync"
		},
		{
		"Effect": "Allow",
		"Action": "iam:AttachRolePolicy",
		"Resource": "arn:aws:iam::*:role/service-role/AWSArtifactAccountSync",
		"Condition": {
		"ArnEquals": {
		"iam:PolicyARN": "arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync"
		}
		}
		},
		{

Use case	Permission names	Example policy
		"Effect": "Allow", "Action": ["organizations:DescribeOrganization", "organizations:EnableAWSServiceAccess", "organizations:ListAccounts", "organizations:ListAWSServiceAccessForOr], "Resource": "*" }] }

Permissions to manage organizational agreements
 	
Master account only. You must set up organizational agreements beforehand.
	`artifact:AcceptAgreement`
	
	`artifact:DownloadAgreement`
	
	`artifact:TerminateAgreement`
	
	`organizations:DescribeOrganization`
		{ "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": "*" }] }

Use case	Permission names	Example policy

Permissions to view organizational agreements	`artifact:DownloadAgreement`
	
	`organizations:DescribeOrganization`
		{
		"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": "*"
		}
		]
		}

Permissions to view and download agreements	`artifact:DownloadAgreement`	{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Action": [
		"artifact:DownloadAgreement"
		],
		"Resource": [
		"arn:aws:artifact::*:customer-agreement/*",
		"arn:aws:artifact:::agreement/*"
		]
		}
		]
		}

Use case	Permission names	Example policy

Permissions for a user to manage the agreements of a single account	`artifact:AcceptAgreement`
	
	`artifact:DownloadAgreement`
	
	`artifact:TerminateAgreement`
		{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Action": [
		"artifact:AcceptAgreement",
		"artifact:TerminateAgreement",
		"artifact:DownloadAgreement"
		],
		"Resource": [
		"arn:aws:artifact::*:customer-agreement/*",
		"arn:aws:artifact:::agreement/*"
		]
		}
		]
		}

To create an IAM policy

Use the following procedure to create an IAM policy. You can use your own, or you can use one of the policies from the previous tables.

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Policies**.
3. Choose **Create Policy**.
4. Choose **Create Your Own Policy**.
5. For **Policy Name**, type a unique name that helps you to remember what your policy is intended to do.
6. For **Description**, type a description for your policy.
7. For **Policy Document**, copy and paste one of the policy documents from the Report Permissions (p. 12), Agreement Permissions (p. 13), or Common AWS Artifact IAM Policies (p. 15) tables, or copy and paste the following policy to grant access to to just the AWS PCI, SOC, and ISO reports in AWS Artifact:

```
{
    "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/
*"
            ]
        }
    ]
}
```

To remove permissions for a specific type of report, remove the line with that report type. For example, to remove the SOC reports, remove the following line:

```
"arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
```

8. Choose **Validate Policy**.
9. Choose **Create Policy**.

Now that you have created your policy, you can attach the policy to a group.

Create an IAM Group

In the preceding procedure, you created a permissions policy. You can attach the policy to a group and add other IAM users to the group at any time.

To create an IAM group and attach your policy

1. Use your AWS account email address and password to sign in as the *AWS account root user* to the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the console, choose **Groups** and then choose **Create New Group**.
3. For **Group Name**, type a name for your IAM group and then choose **Next Step**.
4. In the search box, type the name of the policy that you created.
5. In the policy list, select the check box for your policy. Then choose **Next Step**.
6. Review the group name and policies. When you are ready to proceed, choose **Create Group**.

Now that you have created your group and attached your policy to it, you can add a user to the group.

Create an IAM User and Add Them to a Group

In the preceding procedure, you created an IAM policy, created a group, and attached the policy to the group. You can add IAM users to the group at any time.

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

1. Use your AWS account email address and password to sign in as the *AWS account root user* to the IAM console at https://console.aws.amazon.com/iam/.

   Note
   We strongly recommend that you adhere to the best practice of using the **`Administrator`** IAM user below and securely lock away the root user credentials. Sign in as the root user only to perform a few account and service management tasks.
2. In the navigation pane of the console, choose **Users** and then choose **Add user**.

3. For **User name**, type the name for your user.
4. Select the check box next to **AWS Management Console access**, select **Custom password**, and type the new user's password in the text box. You can optionally select **Require password reset** to force the user to create a new password the next time the user signs in.
5. Choose **Next: Permissions**.
6. On the **Set permissions for user** page, choose **Add user to group**.
7. In the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
8. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

Now that you have created your group, attached your policy to it, and added a user to the group, you can add more users or groups with different permissions using the same procedures.

Document History for AWS Artifact

The following table describes the documentation for this release of AWS Artifact.

- **Latest documentation update:** June 5th, 2018

Change	Description	Date
AWS Organizations agreements	Added documentation for managing agreements for an organization.	June 20 , 2018
Agreements	Added documentation for managing AWS Artifact agreements.	June 13, 2017
Release of the documentation	The first release of the documentation. Includes details for setting up, getting started, and downloading a document.	November 30, 2016